# Passkeys: they're not perfect but they're getting better

**Passkeys are the future of authentication, offering enhanced security and convenience over passwords, but widespread adoption faces challenges that the NCSC is working to resolve.**

Ollie Whitehouse, David C, James L

Now we're in 2025, a lot more services are offering passkeys as a replacement for passwords and the NCSC believes they are the future of modern authentication. However, there are still some significant bumps in the road ahead. Here we set out the case for mass adoption of passkeys and outline the remaining issues which are hindering their widespread implementation. The NCSC will work alongside industry to help resolve these problems and help to get passkeys over the line.

---

## What's wrong with passwords – why do we need passkeys?

Most cyber harms that affect citizens occur through abuse of legitimate credentials. That is, attackers have obtained the victim's password somehow – whether by phishing or exploiting the fact the passwords are weak or have been reused.

Passwords are just not a good way to authenticate users on the modern internet (and arguably weren't suitable back in the 1970s when the internet was used by just a few academics). Adding a strong – phishing-resistant – second factor to passwords definitely helps, but not everyone does this and not every type of Multi-Factor Authentication (MFA) is strong.

---

## So if not passwords, then what?

Passkeys have recently come to prominence as the world's best option for going passwordless – finally replacing account passwords with something better. If you haven't come across passkeys, take a look at our other blog on the promise of passkeys. The short story is that passkeys solve the main security problems we have with passwords.

Passkeys:

- are generated securely and so can't be guessed
- can't be phished
- are unique for each website you use, so if one website is compromised it doesn't put your other logins at risk

Passkeys manage what was previously thought impossible. As well as being far more secure, they're also quicker, easier and more convenient for users. For example, Microsoft has seen that on average passkey sign-ins to their services take only 8 seconds, compared with 69 seconds to sign in using a traditional password and second factor.

As a solution that's designed to be easier for users **and** more secure, you might expect passkeys to be the NCSC's default recommendation for websites authenticating their customers. But if you check out our guidance: MFA for your corporate online services and Authentication methods: Choosing the right type, you'll see we're currently still having to recommend options that include a password and something extra to secure it.

We welcome the year-on-year improvements in passkey technologies but the remaining problems with them means we aren't ready to recommend them for mass adoption across all services yet. The NCSC wants to see an acceleration in progress and collaboration, so that we can confidently recommend this technology as the most secure and usable form of online authentication.

---

## What then are the remaining problems with passkeys?

There's plenty of media evidence pointing to the challenges to passkey adoption. This includes:

### Inconsistent support and experiences

Due to the history of their development, there are currently multiple 'flavours' of passkey available that providers and users need to understand how to manage. These range from device-bound and physical token passkeys (that never leave the device) to 'synced' passkeys (where a device's Credential Manager backs up and synchronises passkeys across the user's other devices).

This complicates things for websites which want to offer effective passkey support but also want to know how the passkey is being handled by the user's device to keep their accounts safe. This can also lead to confusing or frustrating experiences for passkey users who just want the authentication to work, without having to worry about the nuances of underlying technology. For example, some websites support synced passkeys, while others still only support device-bound passkeys.

Industry groups (including the FIDO Alliance and W3C) are working on standards, guides and tools to improve this situation for developers and users, but it will take time for these to be adopted consistently across the range of apps and websites available today. The NCSC strongly encourages providers and developers to engage with these groups and accelerate their adoption of these consistent standards when they're released.

### Device loss scenarios

Users are largely unsure about the implications for their passkeys if they lose or break their device, as it seems their device holds the  entire capability to authenticate. To trust passkeys as a replacement for the password, users need to be prepared and know what to do in the event of losing one – or all – of their devices.

Backing up and synchronising passkeys with a Credential Manager makes it easier to recover access to them compared to other existing second factor options. However, this relies on the user having prepared their Credential Manager account for recovery. Users need help in understanding and

implementing the right steps so they can feel ready to go passwordless and use passkeys without extra worry and hassle.

### Migration issues

Passkeys are 'long life' because users can't forget them or create one that is weak, so if they're done well there should be no need to reset or update them. As a result, there's an increased likelihood that at some point a user will want to move their passkeys to the Credential Manager of a different vendor or platform. This is currently challenging to do, but FIDO and vendors are actively working to address this issue and we wait to see support for this take hold across the market.

### Account recovery processes

For passkey-protected accounts, potential attackers are now more likely to focus on finding weaknesses in account recovery and reset requests – whether by email, phone or chat – and pivot to phishing for recovery keys. These processes need to be sufficiently hardened by providers to prevent trivial abuse by these attackers and to maintain the security benefits of using passkeys. Users also need to be educated on how to spot and report abuse of these processes before their accounts are compromised. This problem is not unique to passkeys, but as passkeys begin to successfully frustrate attackers on a large scale, it's likely that attackers will increasingly shift their focus to these methods.

### Platform differences

Different platforms use different terms to describe the process of passkey logins, which can confuse users and put them off using passkeys. Vendors will need to work together and with the FIDO Alliance to agree on consistent, accessible language and avoid working in silos. This will help users have confidence in what they are using across their digital lives.

### Suitability for all scenarios

Using passkeys assumes that the user has exclusive, private access to an account or device for preparing and accessing the Credential Manager holding their passkeys. However, this is not always the case, such as in households where multiple people use the same phone or tablet, for individuals who don't have

their own modern device and primarily access the internet at places like libraries, and for people for whom biometrics don't work well. Platform providers need to ensure that all users have a personal and private means of accessing their Credential Manager.

---

## Further problems for apps that want to use passkeys

There are additional problems for apps and websites that would like to offer passkeys as a way to sign in (known as 'relying parties') such as:

#### Implementation complexity

It's challenging to offer passkeys to users for services that currently use multiple domains for authentication (such as *account.example.co.uk* and *account.example.com*) and users might need multiple passkeys to sign in to what appears to be the same service. The FIDO Alliance and the industry is working on this problem but it isn't yet effectively accepted and established.

#### Inconsistent use

There's no consensus on when passkeys should be used in a sign-in journey or how much assurance each 'flavour' of passkey provides. As a result, some websites choose to ask for a passkey and an additional factor, while others allow passkey-only sign-ins.

#### Uncertainty around multi-factor status

Website owners and regulators haven't yet reached a consensus on whether all 'flavours' of passkey count as 'multi-factor' (or equivalent) when the user is verified, typically with local-device biometrics or a PIN.

#### Uncertainty around syncing and sharing

For the most critical and sensitive accounts where verifiable user identity is required – for example bank accounts or those connected with power of attorney – there's also uncertainty about whether passkeys which can be synced

and shared are secure enough on their own. Work is still ongoing to agree and define methods of resolving this.

---

## What is the NCSC doing about passkeys?

We'd like passkeys to be our default authentication recommendation and for passkeys to be widely deployed. To enable that, the NCSC is doing the following:

- Working with FIDO and vendors on the above challenges.
- Encouraging UK organisations to make passkeys available as an option to users.
- Exploring where the UK government can lead by example, such as by giving citizens the option to use passkeys to access central government services with GOV.UK One Login.
- Reviewing the regulatory environment and updating rules and standards (such as GPG 44) that underpin how UK organisations offer services to customers to ensure that sites are able to offer passkeys.
- Encouraging organisations – once the technology and underpinning standards mature – to offer passkeys as default for their customers and citizen users.

> In summary, the NCSC believes passkeys are the future of online authentication – for a business authenticating its customers, or a government service authenticating its citizens – and we're working to make this a reality as soon as possible. But achieving this vision needs an intensified effort from all parties and greater collaboration to cohere the vision and prevent it fragmenting to the extent that users disengage.

---

## Should you be using passkeys now?

If you own a service that needs to authenticate users then – ideally – yes, but you'll need to consider whether you can mitigate the challenges for your userbase first.

If you're a user who has read this far, then almost definitely yes!

Passkeys protect you from the most widespread attacks that lead to abuse of legitimate credentials, and modern devices make them as effortless to use as passwords. But as we've highlighted, there are still some challenges to getting them fully adopted across all services. The NCSC will be working with vendors, websites that authenticate users and users themselves to resolve these problems.

Please get in touch with us if you'd like to give feedback, comment or ask a question.

**Ollie Whitehouse**
**NCSC Chief Technical Officer**

**David C**
**Technical Director for Platforms Research**

**James L**
**Senior Security Researcher**

**WRITTEN BY**

Ollie Whitehouse
Chief Technology Officer (CTO), NCSC

**WRITTEN BY**

David C
NCSC Technical Director for Platforms Research

**WRITTEN BY**

James L
Senior Security Researcher

**PUBLISHED**

15 January 2025

**WRITTEN FOR**

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

**PART OF BLOG**

Inside the NCSC