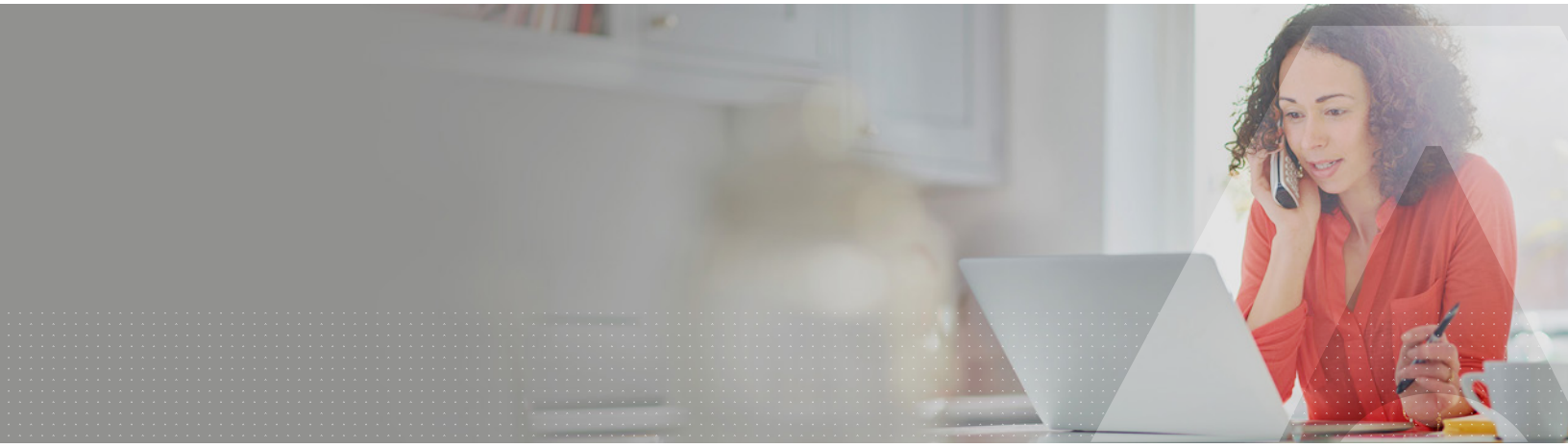
cpl.thalesgroup.com

THALES
Building a future we can all trust

UK National Cyber Strategy (GCHQ) Guidelines for Strong Identity Authentication



Advances in technology combined with decreasing costs have made the world more connected than ever, driving extraordinary opportunity, innovation, and progress. The proliferation of cyberspace is changing the way we live, work, and communicate, and is transforming the critical systems we rely on in areas such as finance, energy, food distribution, healthcare and transport.

The scale and speed of this change is also creating unprecedented complexity, instability and risk. We have witnessed cyber-attacks on hospitals and oil pipelines, schools and businesses, some brought to a standstill by ransomware.

The UK National Cyber Strategy 2022

In December 2021, the UK Government published the National Cyber Strategy 2022[1], which envisions that "the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace." One of the goals of the Strategy is "a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats.

The outcomes of the Strategy are grouped in five pillars:

- **Pillar 1**: Strengthening the UK cyber ecosystem, investing in people and skills and deepening the partnership between government, academia, and industry.
- **Pillar 2**: Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximize the economic benefits of digital technology.
- **Pillar 3**: Taking the lead in the technologies vital to cyber power.
- **Pillar 4**: Advancing UK global leadership and influence for a more secure, prosperous and open international order.
- **Pillar 5**: Detecting, disrupting, and deterring adversaries to enhance UK security in and through cyberspace.

Identity authentication is core to cyber resilience

Cybersecurity and resilience are foundational to taking full advantage of the transformational potential of digital technologies. Pillar 2 of the Strategy places emphasis, among others, on making "the internet automatically safer, preventing attacks, building in basic protections to benefit all UK businesses, organizations and citizens," and "embedding cyber security as a core part of good business."

The Strategy recognizes that "some attacks will happen", therefore businesses must "be resilient enough to minimize their impact and

1 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#contents

be able to recover." To improve the resiliency of the UK digital economy, the Government is planning to help "individuals and small businesses and organizations with basic actions to improve cyber security."

Pillar 3 of the Strategy further elaborates on the objectives of Pillar 2 and explains that a variety of existing and emerging technologies "will be critical to the UK's cyber power." Identity and access management is highlighted as one of the technologies that the UK Government needs to prioritize to secure the UK economy.

The guidelines published by UK's National Cyber Security Centre (NCSC) provide clarifications on how organizations can protect themselves in cyberspace, specifying that businesses should "develop appropriate identity and access management policies and processes," and "consider multi-factor authentication for all user accounts.[2]"

The guidance on zero trust architecture[3] goes a step further, mentioning that "it is important that strong authentication doesn't hinder the usability of a service." NCSC recommends that businesses should "choose authentication methods that are proportionate to the risk and support the ways in which people naturally work." Finally, the guidance suggest that businesses should "offer people a choice of factors to self-authenticate, as no single method will suit everyone (or all environments or devices)."

To this end, there are several authentication methods and technologies, which meet the NCSC guidance. The key to good implementation is to "choose an authentication method that is proportionate to the risk and supports the ways in which people naturally work."

Below is an overview of these methods.

Survey of MFA Methods

Although MFA generally protects against common methods of gaining unauthorized account access, not all multi-factor authentication methods can protect against sophisticated phishing attacks. Indeed, both the EU Cybersecurity Agency (ENISA)[4] and the US National Institute of Science and Technology (NIST)[5] advise against the use of authentication methods that rely on memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, and one-time-passwords (OTP).

GCHQ's position on phishing resistant MFA can be seen in a recent joint security advisory, which was signed by the cybersecurity authorities of the United States, Canada, New Zealand, the Netherlands, and the United Kingdom[6]. The advisory strongly advises to "implement MFA," and suggests that organizations should "require phishing-resistant MFA (such as security keys or PIV cards) for critical services."

SMS-based OTP

Security experts consider SMS authentication to be vulnerable to SIM swapping attacks and interception over public networks. When an authentication code is sent via SMS to a mobile device, we must be confident that the message reaches the intended recipient. However, research has demonstrated the increasing success of redirecting or intercepting SMS messages without requiring cost or time. Despite this, SMS authentication combined with additional protections such as contextual authentication is still quite broadly used in consumer settings because of its convenience.

Authentication using Public Switched Telephone Networks

Use of public phone networks is considered insecure due to the risk of device infection or SIM swapping, code interception, authentication spamming and other risks associated with social engineering.

Push OTP

Much attention has focused on OTP Push authentication, which has been widely deployed in enterprise and employee authentication use cases, for its convenience. Although not phishing-resistant, NIST and other security agencies consider it to offer higher security than SMS/PSTN authentication. At the same time, because this method is so widely deployed and offers a good level of security for numerous situations, it will most likely continue to be broadly used.

Optimizing secure access with appropriate authentication

Although phishing-resistant authentication is strongly recommended for its superior security, any authentication method should be used in accordance with the principle of proportionality, as highlighted in the NCSC guidelines. The most widely available phishing resistant methods today are FIDO2 security keys or physical PKI smart cards. Practical considerations relating to hardware management and provisioning, as well as operational constraints, may limit organizations' ability to deploy them for all use cases.

In addition, many organizations have already implemented OTP hardware or OTP Push authentication. For these enterprises, the prospect of ripping and replacing existing implementations can be daunting. A key question is how organizations can achieve the 'principle of proportionality' in their access security strategy?

PUSH OTP, although not phishing-resistant, can be used for some applications and users, depending on the user profile, the context, and the sensitivity of the data. In addition, when implementing PUSH OTP, or phone-based authenticator apps, there are ways to harden security by:

2 https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management

3 https://www.ncsc.gov.uk/collection/zero-trust-architecture/authenticate-and-authorise

4 https://www.enisa.europa.eu/news/enisa-news/joint-publication-boosting-your-organisations-cyber-resilience

5 https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

6 https://www.cisa.gov/uscert/ncas/alerts/aa22-137a

- Combining PUSH OTP with conditional and contextual authentication. If a login context is considered as high risk, the user could be required to provide additional methods of authentication.
- Combining PUSH OTP with device-native biometrics can demonstrate that an individual intended to authenticate with a specific device.
- Ensuring the integrity of the authentication through risk monitoring, end-point security and anomaly detection.

Ideally, organizations should be able to implement a range of authentication methods, including phishing resistant FIDO2 devices or smart cards. However, in many cases, a single type of authentication will not be able to address IT complexity and diverse user populations. For example:

- Not all applications can support FIDO authentication. Alternative methods of authentication would therefore be needed to enable secure access.
- Some environments, such as factory floors or laboratories, are mobile-free areas. Users logging onto systems under these circumstances would need to use an authentication method that does not rely on mobile phones.

Addressing the UK Cyber Strategy 2022 objectives with Thales OneWelcome IAM solutions

OneWelcome provides an end-to-end access management and authentication platform that meets the cybersecurity and cyber resilience goals and objectives of the UK National Cyber Strategy 2022.

With the OneWelcome Identity Platform, organizations and agencies get a centralized risk-based access platform, which supports a broad range of strong MFA and risk-based authentication to protect all services, apps and environments whether hosted, on-premises or in the cloud.

The OneWelcome Identity Platform is an enterprise-wide identity system that supports a broad range of authentication methods, including:

- **FIDO2 devices**
- **Virtual PKI smart card**
- **PKI smart cards and USB authenticators**
- **Two factor Push OTP in combination with biometric, contextual and risk based authentication**
- **Two factor OTP hardware authenticators**
- **Contextual / adaptive authentication**
- **Risk-based authentication**

The following table maps the GCHQ and NCSC guidelines with the OneWelcome solution offering.

GCHQ and NCSC Guidelines	OneWelcome Solution
High assurance identity and access management technology	OneWelcome Identity Platform offers a broad range of identity and access management features to support all use cases and meet the principle of proportionality
Deployment of multi-factor authentication for all user accounts	A broad range of multi-factor authentication options are proportionate to the risk and supports the ways in which people naturally work
Control third-party access to corporate networks and systems	Access and risk based policies enforce the right level of security and authentication method
Choose authentication methods that are proportionate to the risk	Policy and risk-based access and a broad range of authentication methods allow organizations to enforce the right authentication methods for the right level of risk
Offer a choice of factors to authenticate	A broad range of multi-factor authentication options which can support all remote access use cases

Conclusion

The UK National Cyber Strategy 2022 reflects the growing emphasis on access security and multi-factor authentication as foundational to reducing the threat of data breaches and malicious access to sensitive resources.

The NCSC guidelines calling for organizations to achieve zero trust security by deploying strong authentication that does not hinder experience, can be fully met by the OneWelcome Identity Platform, which offers integrated access management, and a broad range of multi-factor, adaptive and contextual identity validation methods, which support diverse user types and applications.

To learn more about how OneWelcome access management and MFA solutions, go to our dedicated website.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us