0. Version and certification validity notes

0.a. This gamma (0.4) publication of the UK digital identity and attributes trust framework ('trust framework') comes into force on 1 July 2025. New certifications or recertifications can be made against this publication after this date.

0.b. All certifications against the alpha (0.2) version of the trust framework expired on 31 August 2024. Certifications against the beta (0.3) version of the trust framework will remain valid until 31 March 2026 or one of the following conditions is met:

- a service uplifts to the gamma (0.4) publication (including through an annual surveillance audit); or
- the service's beta (0.3) certification expires.

0.c. While we did not intend to make any changes to the content of this document between its pre-release and this final publication, except for alterations within this section, minimal changes have been necessary to support certification. These changes are explained in the following table:

Section/Rule	Change
1.2.a.	Removed a misleading hyperlink to 'data protection legislation', which is defined more accurately in the glossary
4.4.c.	Removed the word 'pilot' now supplementary codes have been recognised by the UK Accreditation Service
Illustrative example 1	Replaced reference to 'an identity service provider' with 'a digital verification service'. Also removed reference to the 'pilot' supplementary code now supplementary codes have been recognised by the UK Accreditation Service
10.2.c.	Replaced an imprecise hyperlink to the Web Content Accessibility Guidelines 2.2 with a more accurate web address
12.4.a.	Replaced an out-of-date reference and hyperlink to 'Government Internal Audit Agency's standards', which has been withdrawn, with a link to the updated 'Government Functional Standard GovS 009: Internal Audit'. Also replaced an out-of-date hyperlink to 'Guidance from the Chartered Institute of Management Accountants' with an updated web address.
Whole document, especially 12.7.	Replaced a series of out-of-date hyperlinks to various guidance hosted by the Information Commissioner's Office with updated web addresses

Section/Rule	Change
12.7.2.	Replaced an incorrect reference and hyperlink to the Information Commissioner's Office's guidance on 'privacy by design and default' with 'data protection by design and default'
Illustrative example 9	Removed reference to the 'pilot' supplementary code now supplementary codes have been recognised by the UK Accreditation Service
12.7.5.a.	Replaced out-of-date references and hyperlinks to draft guidance on anonymisation from the Information Commissioner's Office with the final, published version

Part 1 - Background and context

1. Introduction

1.a. This is the gamma (0.4) publication of the UK digital identity and attributes trust framework. The trust framework is a set of rules for an organisation to follow if they want to have their service certified as a trustworthy digital verification service (DVS). A DVS is a service that enables people to digitally prove who they are, information about themselves or their eligibility to do something. The trust framework aims to make it easier and more secure for people to use these services.

1.b. The trust framework is based on the government's digital identity principles outlined in the response to the Call for Evidence on digital identity. The principles are:

1. **Privacy**. When personal data is accessed, citizens will have confidence that there are measures in place to ensure confidentiality and privacy. Where possible, citizens select what personal data is shared. Providers will have privacy standards to uphold and will need to prove their ongoing compliance.
2. **Transparency**. Citizens must be able to understand by who, why and when their identity and attribute data is used when using digital verification services.
3. **Inclusivity**. Those who want or need a digital identity should be able to obtain one.
4. **Interoperability**. Setting technical and operating standards for use across the UK's economy will help to enable international and domestic interoperability.
5. **Proportionality**. Citizens' needs and other considerations such as privacy and security will be balanced so digital verification services can be used with confidence across the economy.
6. **Good governance**. Standards will be linked to government policy and law. Governance of the digital identity and attributes ecosystem will be clear, coherent and align with the government's wider strategic approach to digital regulation.

1.c. The trust framework is maintained by the Office for Digital Identities and Attributes (OfDIA), part of the Department for Science, Innovation and Technology (DSIT).

1.1. What the trust framework does

1.1.a. The trust framework will help people use and reuse trustworthy digital identities and attributes, with people and organisations across the United Kingdom and internationally. It is intended to accelerate innovation, investment and uptake, while ensuring that services are safely developed and deployed for the benefit of all who wish to use them.

1.1.b. The trust framework draws mainly on existing standards, guidance, best practice and legislation. DVS providers can have their services independently certified against these rules to prove they meet the high standards set out in the trust framework.

1.1.c. In this way, the trust framework and its associated certification process is designed to address a key barrier to the use of digital verification services: that one organisation does not know how another creates digital identities or attributes. Establishing consistent language and requirements will help organisations and people interact and build trust that the information they receive from one another is accurate and reliable.

1.2. What the trust framework does not do

1.2.a. This document does not:

- supersede the requirements in any other contracts, policies or legislation that organisations already need to meet, including data protection legislation;
- explain the legislative or governance arrangements DSIT has established to support digital verification services. This information is available on GOV.UK;
- provide a technical architecture for digital identity or attribute products;
- prevent providers from pursuing even higher standards and levels of innovation, where such actions align with the principles of the trust framework and benefit users;
- set commercial arrangements for organisations; or
- set out the design for a centralised or mandatory national digital identity system.

2. Feedback received and updates

2.a. The trust framework is being developed iteratively. This allows for testing to ensure that trust framework rules are appropriate, proportionate and deliver on the government's digital identity principles. It will continue to be updated as changes are needed and the market develops.

2.1. Policy testing process

2.1.a. Following the beta (0.3) publication of the trust framework in June 2022, DSIT began an extensive policy testing process. This included consultation with the Information Commissioner's Office (ICO), sandbox testing with providers, a public dialogue on trust in digital identity services, regular engagement with over 250 stakeholders across industry, civil society, and the public sector, and a number of written surveys and working groups.

2.1.b. The objectives of policy testing were to:

- assess whether trust framework rules are fit for purpose and where they should be improved;
- understand the level of interest from organisations to become certified against the trust framework;

- understand public attitudes towards digital identities; and
- identify and address barriers to adoption of secure digital verification services across the UK economy.

2.2. Changes made for the gamma publication

2.2.1. New certifiable roles

2.2.1.a. The beta publication of the trust framework outlined three broad role types that providers could be certified as: identity, attribute, and orchestration service providers. During policy testing, some organisations expressed concern that their services were not adequately captured by these role types. In particular, digital wallet providers, providers of reusable services and providers of specific parts of the identity checking or authentication processes found it difficult to identify what trust framework rules they needed to meet.

2.2.1.b. To address this feedback, we have added two new roles to this publication:

- Holder service provider: A holder service provider creates a user-facing device, service, software or app that allows a user to collect, store, view, manage or share identity and/or attribute information and reuse it in multiple scenarios over time. For example, a digital wallet or personal data store.
- Component service provider: A component service provider specialises in designing and building components that can be used during part(s) of the identity proofing, verification or authentication process, but does not offer a complete identity, attribute or holder service. For example, they may specialise in providing biometrics 'liveness' checks that can be used by an identity service provider.

2.2.1.c. It was possible for providers of all these services to be certified against the beta publication of the trust framework. But defining these new roles makes it easier for these types of services to engage with the trust framework with clearer routes to certification. More details are available in section 4.1. on certifiable roles.

2.2.2. Holder service accounts

2.2.2.a. In the beta publication of the trust framework, identity or attribute service providers offering reusable services had responsibilities to manage user accounts. If they wish to be certified under this publication, providers offering reusable identity and/or attribute services will also need to be certified as holder service providers. Requirements around managing user accounts have accordingly moved to this new role. For example, holder service providers seeking certification will need to demonstrate that they can make changes to a user's holder service account and close it when needed.

2.2.2.b. Feedback from industry stakeholders suggested reusable identity providers were uncertain about how to meet the requirements related to closing users' accounts. This publication clarifies rules related to account closures, and introduces a new requirement to reverify inactive identities held in a user's holder service account to help reduce fraud. More details are available in section 12.5.4. on responding to fraud.

2.2.3. Inclusion

2.2.3.a. The government is committed to ensuring that anyone who chooses to use a digital identity can do so. We are continually working to strengthen the evidence base on inclusion to inform future publications of the trust framework and other potential policy interventions.

2.2.3.b. Specifically, we have made changes to the inclusion monitoring reports that providers must submit annually to OfDIA. We have added more detailed questions on a broader range of topics and standardised the response format to improve the quality and range of data collected.

This revised approach has been validated via a pilot to help ensure a more accurate picture of inclusion across the market. More details are available in section 10.1.2. on inclusion monitoring.

2.2.4. Incidents and complaints

2.2.4.a. During policy testing, we received feedback that the rules for incidents and complaints in the beta publication were suitable for industry's requirements. However, the public dialogue found that users wanted further assurances that they will be able to access support if something goes wrong, and timely action will be taken to resolve issues.

2.2.4.b. To address this feedback, we have taken steps requiring providers to have incidents and complaints processes that are easily accessible to users. We have added a new requirement for providers to publish contact details so users can reach the appropriate support, and suggested that providers publish information about their handling timelines and escalation processes. Providers will also need to respond to requests for information from OfDIA to support our continued monitoring of how complaints are handled in the market.

2.2.5. Fraud

2.2.5.a. Ensuring that digital verification services are safe and mitigate against fraud is vital for the safety of citizens and businesses, and for building trust in the digital identity and attributes market. The particular counter-fraud processes that organisations must follow will depend on their sector and any corresponding regulations, legislation or guidance. However, the trust framework also plays an important role in setting out fraud management requirements for the whole digital identity and attributes market.

2.2.5.b. During policy testing, we received feedback that the rules on fraud management should be more detailed. We have therefore introduced new requirements around regular fraud audits, whistleblowing policies, data transparency, sharing information and greater cooperation with relying parties. These changes strengthen fraud controls, make information sharing more accessible, keep users informed of how their data is used and will improve relationships between providers and relying parties.

2.2.5.c. The fraud landscape is evolving at pace and fraud management requirements in the trust framework will be frequently reviewed to ensure they stay relevant and robust.

2.2.6. Identity repair

2.2.6.a. Identity repair refers to an individual being able to use their rightful identity after becoming a victim of identity theft. The beta publication introduced rules related to identity repair, but during policy testing we heard that these did not go far enough to support users.

2.2.6.b. In response to this feedback, we have made the identity repair rules in section 12.5.5. more prominent and placed a greater focus on user support.

2.2.7. Privacy and data protection

2.2.7.a. The public dialogue found the public wants certified services to prioritise transparency, safety and data security. The trust framework already highlights data protection requirements that providers must legally meet, regardless of their role, as well as industry best practice around data protection that is a requirement for certification.

2.2.7.b. This publication includes further updates to privacy and data protection rules, particularly in relation to data storage, users' rights and automated decision-making, following feedback from the ICO. We have also clarified rules relating to providers' privacy policies, with more details available in section 12.7.1. on the principle of 'transparency'.

2.2.7.c. To create trust and protect citizens, users need to understand what will happen if they choose to share their identity and attribute data. Under data protection legislation, providers must already determine their lawful basis for processing users' personal data. This publication includes a separate, clarified requirement for providers who are in direct contact with users to obtain positive confirmation that they have understood how their data will be shared or disclosed (the beta publication called this gaining 'user agreement'). This clarification was made following providers telling us there was uncertainty about the relationship between 'user agreement' and their own assessment of their lawful bases of user data processing.

2.2.7.d. Finally, we have clarified that rules prohibiting third-party marketing to users applies specifically to the use of identity and attribute data in these activities.

2.2.8. Biometrics

2.2.8.a. Biometric technologies can offer greater accuracy and security for digital verification services. However, to ensure that all users of digital identities can benefit from these features, biometric technologies need to be inclusive, accessible and appropriately tested to ensure they work for a wide range of users.

2.2.8.b. Following feedback from industry and civil society, we have added requirements and guidance on using biometrics in certified services. This includes requirements for any biometric technology to have consistent performance rates across demographics, and for providers to be transparent about their technology's performance. We have also added detail on the types of testing providers must undertake. Additionally, we now require providers who offer both biometric and non-biometric checks to offer both options simultaneously. More details are available in section 12.8. on using biometrics.

2.2.9. Relying party flow down terms

2.2.9.a. Relying parties do not need to be certified against the trust framework in order to consume digital identities and attributes from certified services. However, it is vital that they do not undermine the principles of the trust framework. The beta publication consequently introduced flow down terms, designed to encourage relying parties to follow good practice while allowing the market to innovate.

2.2.9.b. The responses to flow down terms were mixed. Some stakeholders expressed that more should be done to ensure flow down terms are enforced, while others told us flow down terms are burdensome. The government has committed to enabling secure and trusted digital verification services, and a crucial part of that is engaging relying parties in good practice. Flow down terms offer protections and reassurance to users that their data is safe and being handled by trustworthy organisations. In this publication, we have updated flow down terms to clarify their importance and their relationship with certification.

2.2.10. The register of certified services

2.2.10.a. Providers that successfully get services certified against the trust framework can apply to appear on the register of certified digital identity and attribute services, a public list that OfDIA maintains. More details can be found on GOV.UK.

2.2.10.b. To reflect this opportunity and manage associated risks, this publication includes new rules governing a service's presence on the register of certified services in section 13.

2.2.11. Business probity rules

2.2.11.a. To ensure we are upholding the highest standards across the trust framework ecosystem, we have added rules relating to business probity in section 11.1. These make explicit that providers must pass checks (already being undertaken during the beta certification process) to ensure a provider's legitimacy to conduct business in the UK. Once a service is certified, these

rules now also require providers to keep OfDIA informed about significant changes to their business, such as mergers and acquisitions.

2.2.12. Schemes

2.2.12.a. The beta publication set out some early thinking on schemes, and committed DSIT to testing governance options. Following further policy development, we have removed all references to 'schemes' in the trust framework from this publication.

2.2.12.c. Instead, where there are additional sector or use case-specific needs which the trust framework does not address, we will look to create 'supplementary codes.' As with the trust framework itself, supplementary codes will be owned and run by OfDIA, prepared through stakeholder engagement and certified against by approved CABs. Services will have to be certified against the trust framework to be certified against any supplementary codes. Further information on supplementary codes can be found in section 4.4.

2.2.13. Auditable language changes

2.2.13.a. To support certification and auditing against the trust framework, we have changed the structure of this publication. As the market is more mature, much of the context-setting information included in the beta version has been relocated and is available on GOV.UK.

2.2.13.b. We have also collated the certifiable rules into two dedicated sections. Part 2 covers rules for individual providers by role, while Part 3 details rules for all service providers. Within these sections, we have tightened requirements where possible, distinguishing between rules providers must follow to be certified and more general practices they could find useful to consider. Finally, we have numbered subheadings and lettered paragraphs throughout the document to make it easier to refer to specific requirements.

3. Terms and definitions

3.a. Please see the glossary for a full list of terms and definitions.

3.1. Digital identities and attributes

3.1.a. In the context of the trust framework, a digital identity is a digital representation of a person acting as an individual or as a representative of an organisation. It enables them to prove who they are during interactions and transactions. It is also a way for organisations or users to check that other users are who they say they are. Digital identities can be used online or in person, and may be created for single point-in-time use or be reusable.

3.1.b. Attributes are individual pieces of information that describe something about a person, like their age, or an organisation, like their VAT number. A combination of attributes can be used to create a digital identity, and help people prove that they are who they say they are. But attributes can also help prove a user is eligible or entitled to do something, such as buying age-restricted goods. In these circumstances, it often is not necessary to know the user's full identity before they can complete an interaction, and attributes can be used on their own. In other situations, this proof could be added to an existing digital identity.

3.2. Other terms used in this document

3.2.a. We use 'provider' to refer to an organisation that offers digital verification services under the trust framework. Where a provider has had their service or product certified against the trust framework, we refer to it as a 'certified service' or 'service'.

3.2.b. We use ‘the register’ to refer to the register of digital identity and attribute services, a public list of providers offering certified services. Where a provider has a certified service listed in the register, we refer to them as a ‘registered provider’ and their service as a ‘registered service’.

3.2.c. We use ‘you’ and ‘your service’ in this document to direct a provider to the specific rules their organisation and service(s) must follow, and the recommendations they can follow, in order to be certified against the trust framework.

3.2.d. The word ‘must’ is used for any rules that a provider has to prove they have met in order for their service to be certified.

3.2.e. The words ‘can’, ‘may’ or ‘could’ are used to draw providers’ attention to optional standards and guidance they may wish to consider depending on their circumstances. However, these will not be requirements for certification.

3.2.f. We use ‘relying party’ to refer to an organisation that uses (or ‘consumes’) digital verification products or services. In the context of the trust framework, we assume they are consuming digital identities and attributes from certified services.

3.2.g. We use ‘participant’ as a collective term to refer to all organisations that interact with the trust framework and take part in the wider digital identity and attributes market. This includes certified services and relying parties.

3.2.h. We use ‘supplementary code’ to refer to additional rules that providers can certify against, alongside the trust framework, to demonstrate that they meet the requirements of a particular sector or use case.

3.2.i. We use ‘user’ to refer to a person who uses digital verification services. This can include individuals with delegated authority to act on behalf of somebody else, such as carers or parents.

4. How organisations participate in the trust framework

4.a. How you choose to participate in the trust framework will determine whether your service(s) needs to become certified and, if so, which trust framework rules are relevant. It is possible for your organisation and/or your service(s) to fulfil multiple roles under the trust framework. If so, you will need to follow the rules for each role. More information is available in section 4.1. on certifiable roles.

4.b. DVS providers who wish to participate in the trust framework must get their service certified against trust framework rules by an approved trust framework conformity assessment body (CAB). CABs must be accredited to ISO 17065 by the UK Accreditation Service (UKAS) and approved by OfDIA to certify a service against trust framework rules.

4.c. In cases where trust framework rules have been breached, an investigation of a certified service’s compliance with the trust framework will be launched by the CAB the provider has contracted with for certification.

4.d. Other participants do not require certification against the trust framework to adopt digital identities, but they may choose to engage with certified services as part of their business operations. More information is available in section 4.2. on market participants.

4.1. Roles with certifiable services

4.1.a. Providers that wish to have their service certified against the trust framework's rules must perform at least one of the following roles:

- identity service provider
- attribute service provider
- holder service provider
- orchestration service provider
- component service provider

4.1.b. To be certified, a CAB will need to check that a service follows all the rules for the role(s) it performs. A service may be able to perform more than one of these roles, which are associated with different capabilities, as the table below summarises:

Service capabilities	Identity service provider	Attribute service provider	Holder service provider	Orchestration service provider	Component service provider
Proves and/or verifies identities	✓				
Collects, creates or checks attributes		✓			
Holds identities and/or attributes over time			✓		
Orchestrates interactions between participants				✓	
Provides specific part(s) of the identity proofing, verification or authentication processes					✓

Figure 1

4.1.c. The rules for providers are 'outcome based'. By following them, services will achieve certain goals. The rules do not require the use of specific technologies or processes, but direct services to follow open technical standards where possible to strengthen interoperability between participants.

This means providers of certified services will be able to innovate and develop products and services to better support users, without being restricted to using certain technologies.

4.1.d. Once certified, a certificate is valid for three years, unless it is suspended or revoked. A certificate applies only to the certified service and cannot be used to imply that any other service or an organisation as a whole is certified. The certified service will be subject to regular auditing during that period and must be re-certified prior to its certificate expiring in order to maintain its certified status. OfDIA may require providers of certified services to uplift to a more recent publication of the trust framework less than three years after a previous certificate has been issued in order to maintain certification. More information about the certification process is available from the CABs.

4.1.e. Certified services may apply to be listed in the public register of digital identity and attribute services. More information is available in section 13.

4.1.1. Identity service provider

4.1.1.a. An identity service provider proves and verifies a user's identity for one-off use at a single point in time. It can provide services across a range of relationships between users, businesses and government, but will generally work directly with relying parties.

4.1.1.b. An identity service provider can specialise in proving and verifying users' identities, or offer identity proofing and verification alongside other services – an example of this might be a bank, solicitor, library or postal organisation.

4.1.1.c. An identity service provider does not need to do all parts of the identity proofing and verification process itself, but it is responsible for the overall process and its outcome. For example, it may contract with one or more component service providers or other third parties that specialise in providing specific part(s) of the process.

4.1.1.d. If a provider is creating, quality-checking or sharing attributes as part of their service it is also an attribute service provider.

4.1.1.e. If a provider holds and/or supports the reuse of a digital identity, it is also a holder service provider.

4.1.2. Attribute service provider

4.1.2.a. An attribute service provider collects, creates, checks or shares pieces of information that describe something about a user. It can provide services across a range of relationships between users, businesses and government.

4.1.2.b. An attribute service provider can share users' attributes with relying parties, identity service providers and holder service providers if they confirm a user's understanding. It is also able to assess the quality of the attributes it collects, creates, checks or shares in order to support relying parties.

4.1.2.c. An organisation does not need to do all parts of the attribute collection, creation, checking or sharing processes. It may wish to contract with one or more component service providers or other third parties that specialise in providing a specific part(s) of the process.

4.1.2.d. The trust framework describes how attribute service providers fall into sub-roles, including:

- attribute issuers from the public sector – organisations providing attributes found in documents or databases such as passports, driving licences, birth certificates, and some kinds of digital credentials; and
- attribute issuers from the private sector – organisations providing attributes such as a mobile number, bank account balance, credit score, and mortgage.

4.1.2.e. If a provider holds and/or supports the reuse of attributes for a user, it is also a holder service provider.

4.1.3. Holder service provider

4.1.3.a. A holder service provider creates a user-facing device, service, software or app that allows a user to collect, store, view, manage or share identity and/or attribute information. It securely holds and shares this information, and ensures it is not illegitimately changed, but cannot create new information itself. The user can control what information their holder service stores, when it can be shared, and who it is shared with.

4.1.3.b. Users can keep many different things in their holder service. One form of holder service, called a 'digital wallet', is commonly used on mobile phones to hold things such as payment card details or tickets. Other forms of holder services could include:

- reusable digital identities and attributes;
- a personal data store;
- a personal data vault; or
- a pod provider.

4.1.3.c. Holder services include an 'account' functionality. This is a user interface that allows a user to consistently access and manage information held in their holder service. It also allows a provider to directly support and remotely manage a user's holder service, for instance to facilitate identity recovery processes and respond to fraud incidents.

4.1.3.d. Relying parties can connect directly with a holder service to get information about a user, or there can be another party involved to help with the exchange of information.

4.1.3.e. If a provider wants to prove and verify an identity, in addition to holding it for later reuse, it is also an identity service provider.

4.1.3.f. If a provider wants to create new attributes based on information held in a holder service, including deriving attributes, it is also an attribute service provider.

4.1.4. Orchestration service provider

4.1.4.a. An orchestration service provider makes sure data can be securely shared between participants through the provision of their technology infrastructure. It is not user-facing.

4.1.4.b. The trust framework describes how orchestration service providers fall into sub-roles, including:

- identity and attribute broker service providers;
- identity and attribute hub service providers;
- identity access management service providers; and
- distributed ledger service providers.

4.1.4.c. The technical options for orchestrating identities and attributes are broad and open to innovation. The trust framework sets out the outcomes for orchestration service providers.

4.1.5. Component service provider

4.1.5.a. A component service provider specialises in designing and building components that can be used during part(s) of the identity proofing, verification or authentication processes. Identity, attribute or holder service providers can contract with one or more component service providers to provide specific part(s) of their service.

4.1.5.b. For example, component service providers could develop hardware and/or software to:

- provide identity evidence (e.g. facilitate a vouch);
- validate identity evidence (e.g. mobile account validation);
- check identity evidence is genuine (e.g. passport chip reading);
- provide identity fraud services (e.g. fraud database checking);
- provide biometrics verification (e.g. face biometrics); or
- provide non-biometric or biometric authentication (e.g. fingerprint biometrics on a mobile device).

4.2. Other participants in the market

4.2.1. Relying party

4.2.1.a. A relying party is an organisation such as an airline, bank or retailer that might not check users' identities and/or attributes themselves, but instead relies on a digital verification service.

4.2.1.b. For example, a relying party might need to make sure a user is who they say they are before letting them do something. To do this, the relying party can ask an identity service provider to prove a user's identity. A relying party might also need to check if a user is eligible to do something. It can do this by requesting attributes, or information about attributes, from an attribute service provider.

4.2.1.c. Relying parties do not need to be certified against the trust framework, but they will be subject to flow down terms from any certified services they have a relationship with to ensure the security of the supply chain.

4.2.1.d. In the context of the trust framework, a relying party is an organisation that receives, interprets and – depending on the use case – stores information received from certified services. Organisations which provide additional functions related to the information received, for instance binding it to an individual, will likely also be playing another role under the trust framework alongside being a relying party and may wish to be certified.

4.2.1.e. A digital verification service may only play a small part in a relying party's wider interactions with a user. For example, a bank may rely on a certified service as part of their onboarding process to verify a user's identity. In this instance, it would be misleading for the bank to claim that their entire onboarding process was certified against the trust framework on the basis that a certified service is used for identity verification only. More detail on providers' responsibilities can be found in section 11.1.b. on misrepresentation.

4.3. Relationships within the market

4.3.a. It is up to individual organisations to determine commercial relationships and decide who to work with. However, certified services will derive significant assurance, interoperability and user

protection advantages from working with other certified services. Relying parties will also derive significant user protection, reliability and security benefits from working with certified services (subject to business need and any regulatory requirements).

4.3.b. During certification, providers will be required to inform CABs which organisations they work with and rely on when providing services that are within the scope of the trust framework. This will help CABs to assess whether appropriate protections are in place throughout a supply chain and evaluate possible risks to other participants. For instance, numerous providers relying on one fraud monitoring service could create a single point of failure in the digital identity and attributes market. CABs will then anonymise and aggregate this information before submitting it to OfDIA who will use it to assess the market, including any emerging risks.

4.3.c. The following are examples of some possible relationships within the market. Please note these are not exhaustive and are for illustrative purposes only.

Figure 2

Figure 3

4.4. Supplementary codes

4.4.a. The trust framework's rules set a baseline for good digital verification services across the UK economy. Individual sectors or use cases may have additional requirements that exceed those in the trust framework, for instance to meet specific legislative or regulatory obligations. To make it easy for businesses to know how they can use digital verification services to meet these requirements, they can be translated into additional rules that providers can certify against as part of the trust framework certification scheme. This set of additional certifiable rules is known as a supplementary code.

4.4.b. OfDIA is responsible for the creation and maintenance of supplementary codes, and for facilitating providers' certification against them. OfDIA has determined four key principles it will follow to create new supplementary codes:

- like the main trust framework, supplementary codes must be based on consultation with appropriate persons, including regulators;
- like the main trust framework, supplementary codes will be version controlled and developed iteratively;
- the rules of a supplementary code must strengthen rather than undermine, the trust framework's rules; and
- the rules of a supplementary code must fulfil a market and user need.

4.4.c. There are three supplementary codes at the time of this publication. They describe rules for providers conducting digital right to work, right to rent and Disclosure and Barring Service checks. Further information on these supplementary codes can be found on GOV.UK.

Illustrative example 1
A company is hiring a new employee, and they need to conduct a right to work check. The Home Office allows right to work checks on British and Irish citizens to be conducted using a digital verification service, but the check needs to be done in a certain way. These extra requirements have been translated into a supplementary code.

The company works with a digital verification service that is certified against both the trust framework and the supplementary code for digital right to work checks. The provider conducts the check on the company's behalf, confirms the result to the company and, if the check is successful, shares a photo of the employee.

Once the company has conducted a likeness test against that photo, they are able to onboard the employee with confidence that the right to work check has been completed in a compliant way.

Part 2 - Rules for providers by role

5. Rules for identity service providers

5.a. Identity service providers must follow these rules, those in section 10. and Part 3.

5.1. Creating a digital identity

5.1.a. You must use the guidance on how to prove and verify someone's identity as a methodology to explain your service. This is known as 'Good Practice Guide' (GPG) 45. You must demonstrate how each aspect of your service maps onto GPG 45, for instance by detailing the kinds of evidence and checking methods your service can use to reach a 'medium' level of confidence.

5.1.b. You must also be able to share this information with relying parties and other services you work with, if it is requested. This must include the relevant GPG 45 strength, validity, activity history, identity fraud and/or verification scores that your service can achieve, as well as how your service can combine them to reach different profiles and levels of confidence.

5.1.c. If your service uses components from third parties, you must accurately describe how each component maps onto the relevant part of GPG 45. Using components sourced from certified component service providers may make it easier to demonstrate this.

5.1.d. If you work directly with relying parties, you must agree the level(s) of confidence or profile(s) that are suited to their needs and meet any contractual obligations that arise as a result.

5.2. Accepting expired documents

5.2.a. Although in-date documents must be used when available, in some circumstances you may accept documents after they have expired. There is no obligation to accept expired documents, but if you do choose to accept them, you must:

- demonstrate consideration of any legislation or guidance that may be relevant to a specific sector or use case; and
- only accept passports up to a maximum of 12 months after they have expired.

5.2.b. You could apply additional restrictions to your acceptance of expired documents. For example, you may choose to only accept expired passports with near-field communication (NFC) chips issued by specific countries, or for a maximum of 6 months. You could decide to set restrictions yourself, or they could be determined by other organisations you work with, such as a relying party.

6. Rules for attribute service providers

6.a. Attribute service providers must follow these rules, those in section 10. and Part 3.

6.1. Creating attributes

6.1.a. You must follow the guidance on how to create attributes. It could also be helpful to refer to the guidance on understanding attributes.

6.1.b. When creating an attribute, you must be able to reliably link it to an individual or organisation. This could involve binding the attribute using an 'identifying attribute' to make the connection. An identifying attribute, or 'identifier', is a unique attribute or combination of attributes that you can use to identify a person or organisation. Alternatively, this could involve embedding sufficient information in the attribute to allow a relying party or service you work with to ascertain to whom or what the attribute relates.

Illustrative example 2
When someone starts a new job, they are given a unique employee number which is an identifying attribute. This links the person to their job title (another attribute).

The HR department uses the identifying attribute to link the employee's other attributes to the employee. Their other attributes include their salary and how many hours they work a week.

For example, a company has two employees named Daniel Jones. When the HR department gets a phone call from one of them, the HR representative asks for their employee number. This helps them know which Daniel Jones they are talking to.

6.1.1. Sharing attributes

6.1.1.a. Before you share or allow checks against an attribute, you must check:

- when the attribute was last updated;
- whether you will share it in a way that meets the privacy and data protection rules in section 12.7.; and
- if the person or organisation requesting it has the right to see it.

6.2. Assessing attribute quality

6.2.a. You must have a way of assessing the quality of attributes that you create or share. You could follow the guidance on how to score attributes or you could follow your own processes.

6.2.b. You must also be able to share this information with relying parties and other services you work with, if it is requested. Relying parties and other services you work with can use your assessment to decide which attributes meet their needs.

7. Rules for holder service providers

7.a. Holder service providers must follow these rules, those in section 10. and Part 3.

7.1. Holding identities and attributes

7.1.a. Your service must store information securely and ensure it is not illegitimately accessed or changed. You must prevent any unauthorised persons from accessing a user's holder service account by following the guidance on using authenticators to protect an online service. This is also known as Good Practice Guide (GPG) 44.

7.1.b. Your service must make clear to relying parties and users whether:

- an identity or attribute you hold comes from a certified or uncertified service, except where it comes from a UK government source; and
- an attribute you hold has been linked to a person or organisation. This is called binding, and could follow the guidance on how to bind an attribute. If you do not follow this guidance, you must demonstrate how attributes are linked to a person or organisation so that the person or organisation checking them can tell to whom the attribute relates.

Illustrative example 3
George is travelling on holiday abroad with her child. She holds both of their boarding passes as attributes in her digital wallet.

The wallet has been certified as a holder service and is protected by an appropriate form of biometric authentication.

Airline staff request their boarding passes at the gate. George has to scan her face in the app before it will allow her to present the boarding pass. This ensures that only George can access the information stored in her holder service. George's child would not be able to access their boarding pass without her.

7.2. Reusing a verified digital identity or attribute in a holder service

7.2.a. If you are an identity or attribute service provider and want to allow a user to repeatedly assert information about themselves that you have verified, you must store the digital identity and/or attributes in a holder service. Your service must follow the rules in section 12.7.3. on confirming a user's understanding before you use their data to do this.

7.2.b. You must also be able to show a user what level(s) of confidence and identity profile(s) their identity meets under GPG 45, in an easily accessible way, if this information is available to you.

Illustrative example 4
Hayley has already verified her identity to a medium level of confidence with a high street bank to sign up to their online banking app.

Following the trust framework, the bank used the details provided by Hayley during the sign-up process to create a verified digital identity. Hayley can store this identity in the bank's holder service, and the bank makes it easy for Hayley to check which level of confidence under GPG 45 her identity reaches.

Hayley can then use this service in the future to prove her identity and share attributes without verifying her identity from scratch.

Illustrative example 5
In the future, Patrick may be able to electronically sign a lease agreement to rent a new flat using a Qualified Certificate (QC). A qualified trust service provider (QTSP) will have bound his proven and verified identity to this Qualified Certificate.

Because QTSPs would follow GPG 45 when creating the QC used to make the Qualified e-Signature, a holder service provider could rely on the identity verification process that was used by the QTSP. With Patrick's permission, this certificate containing his digital identity could be held in a certified holder service so Patrick can present it again in the future.

7.3. Managing a user's holder service account

7.3.a. You must have processes to revoke, suspend, close, recover and make changes to a user's holder service account. This includes supporting the appropriate identity and/or attribute services, which could be another service you provide, to make legitimate changes to information held in a user's holder service account. For example, if a verifiable credential is altered or revoked by its issuer, you must be able to reflect these changes in the user's holder service account.

7.3.b. You must close a holder service account if:

- the user wants to close it;
- you have evidence it was created fraudulently, including using a synthetic identity; or
- you become aware of the user's death. You could follow the guidance on delegated authority to manage requests related to their account, for example to manage settling estates.

7.3.c. You must have processes in place to take action against a user who does not follow the terms of use they agreed to. These must include a process for closing their holder service account and preventing access to your service if the issue cannot be resolved.

7.3.d. If an identity in a user's holder service account has been inactive for 14 months, the user must be reverified before the inactive identity can be used or shared again.

7.3.1. Notifying a user of changes to their holder service account
7.3.1.a. You must have a process in place to notify the user of any changes to their holder service account as well as any identities and attributes held within it. This includes any legitimate changes made by the identity or attribute service that issued it. You must also have a process in place to notify the user if you have received a request to close their holder service account. These processes must be multi-channel and not undermine any requirements covering risk management (section 11.7.), fraud management (section 12.4.) and responding to incidents (section 12.5.).

7.3.1.b. You must provide users with means to respond to these notifications, for instance by querying the change or closure.

7.3.1.c. If a user wants to change the contact details associated with their holder service account, you must authenticate the user before allowing them to make these changes.

8. Rules for orchestration service providers

8.a. Orchestration service providers must follow the rules in Part 3. There are currently no rules specific to orchestration service providers.

9. Rules for component service providers

9.a. Component service providers must follow these rules and those in Part 3.

9.b. If you provide other certified services with component part(s), you must support those services to fulfil their requirements under section 10.

9.1. Providing components of GPG 45 or GPG 44

9.1.a. Some component service providers may provide part(s) of the identity proofing, verification or authentication processes outlined in GPG 45 or GPG 44.

9.1.1. GPG 45 components

9.1.1.a. If you provide part(s) of the GPG 45 proofing and/or verification process, then you must follow the rules for identity service providers in sections 5.1. and 5.2.

9.1.1.b. Where GPG 45 identity checks that you carry out fail, you must be able to share information about why with a relying party or other service you work with using clearly defined and coded failure modes.

9.1.2. GPG 44 components

9.1.2.a. If you provide part(s) of the GPG 44 authentication process, then you must demonstrate how each aspect of your service maps onto GPG 44, for instance by detailing how authenticators are created, managed and captured by your component.

9.1.2.b. You must also be able to share this information with relying parties and other services you work with, if it is requested. This must include the specific quality levels of any authenticators your service can provide, as well as how your service can reach different levels of protection.

9.1.2.c. Where a GPG 44 authentication process that you carry out fails, you must be able to share information about why with a relying party or other service you work with using clearly defined and coded failure modes.

10. Rules for all identity, attribute and holder service providers

10.1. Making your products and services inclusive

10.1.a. Making your products and services inclusive means as many people as possible can use them, no matter who they are. This includes people who do not have traditional identity documents, such as passports, or who may find it difficult to verify their identity to access services online. However, there are reasons someone might be legitimately excluded. For example, for certain products and services that cannot be legally accessed until the age of 18, it is fair to restrict service access on account of someone's age.

10.1.b. You must comply with the Equality Act (2010), or equivalent legislation in Northern Ireland, when considering how to make sure no one is excluded because of their 'protected characteristics'. Public sector organisations or non-public sector organisations carrying out public functions must also meet the public sector equality duty (PSED) detailed in the Equality Act (2010).

10.1.1. How to make your product or service more inclusive

10.1.1.a. There are many reasons why a user may be unintentionally or unnecessarily excluded from using a product or service. Common reasons include users being asked to provide specific evidence as proof of their identity, or services relying on specific databases to check users' information.

Illustrative example 6
A service that only accepts a UK passport as proof of someone's identity will exclude users who do not have, cannot find or cannot afford a UK passport.

Illustrative example 7
A service that only checks users' information against a credit reference agency database will stop users who do not have a credit history from creating a digital identity. This could exclude users because of their age or income.

10.1.1.b. You could improve the inclusivity of your service by accepting a wide variety of identity and attribute evidence, provided it can still combine to meet a relying party's required level of confidence. You could also choose to accept a declaration from someone that knows the user (known as a 'vouch') as evidence. If you accept vouches, you must follow the vouching guidance.

10.1.1.c. You might also exclude users if your service uses any software or hardware that has only been developed and tested with a specific user group. To improve the inclusivity of your service, you could ensure that all aspects of it have been performance tested with a variety of users from different demographics.

Illustrative example 8
A service might check users' identities using a facial recognition system that was tested with a small sample of users. As most of these users were white men, the system was not taught how to recognise users of other genders or ethnicities.

By choosing this system, the service will exclude some users from proving their identity because of the way they look.

10.1.2. Submitting an annual inclusion monitoring report
10.1.2.a. You must submit an inclusion monitoring report at least annually. The anonymised and aggregated results of these reports will provide an evidence base to inform policy development to support our inclusion aims.

10.1.2.b. The report will explore what avenues your service offers to acquire a digital identity and/or attributes. It will also collect information on what technology your service uses, what identity evidence is accepted by your service and include an opportunity for you to explain any inclusion measures you are planning to take in future. You are not required to collect information on users solely for the purposes of inclusion reporting.

10.1.2.c. Details on how to submit an inclusion monitoring report will be provided by your CAB directly.

10.1.3. Allowing users to retake a check
10.1.3.a. There are many reasons why an identity or attribute check might fail. If a user fails a check and there is no suspicion of fraud, you must have a process to allow the user to undergo an identity or attribute check again, with corrected data if applicable.

10.1.3.b. You may wish to determine whether the check failed due to:

- a transposition error – for example, dates might appear in different formats or names with punctuation might have been transposed differently; or
- a failure in technology – for example, there might be an issue with readings from the NFC chips in passports, resulting in a false-negative result.

10.1.3.c. If a check still fails, you could use alternative identity evidence and methods of identity verification, following GPG 45. You could:

- verify the user's identity using a different identity profile for the same level of confidence as when you first verified the user's identity;
- verify the user's identity using the same identity profile but alternative data sources; or
- verify the user's identity using the same identity profile but a different process.

10.1.3.d. If there is a suspicion of fraud, you must follow the rules in section 12.4. on fraud management.

10.2. Making your products and services accessible

10.2.a. If you are a public sector body, you must follow the accessibility requirements for public bodies.

10.2.b. If you are a public sector organisation that develops products or services for the public in Wales, you might be subject to Welsh Language Act (1993) or the Welsh Language (Wales) Measure (2011). You must check your legal obligations carefully. The Welsh Government has published a detailed Bilingual Technology Toolkit to help organisations provide a good user experience in both Welsh and English.

10.2.c. If you are a private sector organisation, you must also make sure your service is accessible. You could do this by following:

- Web Content Accessibility Guidelines (WCAG 2.2) to AA level; or
- The European Telecommunication Standards Institute (ETSI) standard for accessibility requirements EN 301 549 V3.2.1 (2021-03).

10.2.d. If you do not follow these guidelines or standards, you must evidence that your service fulfils the principles of POUR: that it is Perceivable, Operable, Understandable and Robust. More information is available via the World Wide Web Consortium.

10.2.e. You and/or the relying party or other service you work with could also offer users more than one way to use a product or service. For example, where feasible and appropriate to do so you could offer users the option of posting their identity evidence to you or carry out checks in-person to support users that are unable to use an online service.

Part 3 - Rules for all service providers

11. Operational requirements

11.1. Business probity

11.1.a. When doing anything related to the trust framework, you must not bring the trust framework into disrepute or damage its reputation, optics or trustworthiness. You must check your legal obligations carefully and not act unlawfully.

11.1.b. You must not misrepresent the certification status of services you offer, or allow others you work with to misrepresent their services through reliance on your certificate(s). For example, you must be clear which of the services you offer have been certified and which have not. Similarly, you must also not allow a third party to claim that they offer a certified end-to-end service solely because some aspects of it are delivered by your certified service. This does not preclude the third party from disclosing that a certified service forms part of their supply chain, particularly where the certified service is conducting specific activities in line with regulatory requirements.

11.1.c. You must prove that your organisation is a legitimate entity. You can demonstrate this by supplying evidence such as your Companies House registration number, Charities Commission registration number, Data Universal Numbering System (DUNs) number, Legal Entity Identifier (LEI) or other information that identifies your organisation as a registered entity in the UK or another jurisdiction.

11.1.d. You must also evidence that:

- your director(s), or equivalent depending on your legal status, does not have any restrictions or constraints inhibiting their ability to carry out their duties, such as outstanding bankruptcy proceedings or court summons;
- your organisation (and parent company if applicable), ultimate beneficial owners, director(s) and people with significant control, or equivalent depending on your legal status, do not appear on a UK Sanctions List;
- your organisation is not involved in any outstanding proceedings which could affect the provision of your digital verification service, such as patent disputes, court orders, or criminal or small claims court proceedings; and
- your organisation does not have any convictions or pending sanctions cases relating to corruption, bribery, money laundering, terrorism financing or fraud as defined in law such as the Money Laundering Regulations (2017), and the Fraud Act (2006).

11.1.e. You must declare to your CAB and OfDIA any ICO investigations into your organisation that are relevant to your service, and evidence how you have responded to their concerns in your service design.

11.1.f. If you undergo a merger or acquisition, including acquisition of a significant share of company shareholding or voting rights, you must evidence that you and the acquirer followed the notification regime in line with the National Security and Investment Act (2021). You must also evidence that you and the acquirer will continue to abide by the trust framework and any other conditions of your certification as a provider.

11.2. Responding to complaints and disputes

11.2.a. You must have documented processes for dealing with complaints and disputes. Disputes could involve your users or other participants in the trust framework.

11.2.b. You must publish easily accessible details about these processes, including the contact details your customers can use to contact you about a complaint or dispute. You could publish the timelines you expect to meet when dealing with complaints and disputes, and information about your escalation processes.

11.2.c. Your complaints and disputes procedures must take account of relevant regulatory channels. You must also retain appropriate records of any complaints or disputes and provide OfDIA or your CAB with information about complaints if requested.

11.3. Staff and resources

11.3.a. You must demonstrate that you have ways to:

- make sure your staff (including contractors) have the right experience, training (such as data protection training), competencies and qualifications needed to do their job;
- do background checks on your staff; and
- make sure any personal, cryptographic or sensitive information you keep can only be accessed by authorised staff.

11.3.b. You could evidence this by:

- following the ‘applicable skills and security awareness’ control in ISO/IEC 27001;

- following equivalent industry standards such as the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), or the National Institute of Standards and Technology (NIST) Cybersecurity Framework; and/or
- following BS 7858:2019 on screening individuals.

11.3.c. You must have a Senior Responsible Officer (SRO) in your organisation responsible for managing operational matters relating to your service. The SRO will be directly notified of any important changes to the trust framework, certification and other matters. You must:

- provide your CAB with accurate contact details for your SRO and keep these up-to-date (you can provide details for more than one person); and
- demonstrate that you have processes to appoint a new SRO if needed.

11.3.d. Your SRO must inform OfDIA and your CAB of any material changes to your organisation or service within 48 hours of those changes happening. This includes ceasing to provide the certified service or changes to:

- your service's technology;
- your directors, or equivalent;
- ultimate beneficial owners, or equivalent;
- people with significant control, or equivalent; and
- any information covered by the business probity rules in section 11.1.

11.4. Service and quality management

11.4.a. You must have service and quality management processes that cover all areas of your organisation that are applicable to the trust framework. Your service and quality management process could be set out in a collection of documents that describe your organisation's objectives and explain how you will achieve them.

11.4.b. For example, your objectives could include:

- investigating and fixing all faults within 2 hours – this refers to your service management; and
- making sure every member of staff completes 5 hours of security training every month – this refers to your quality management.

11.4.c. The trust framework does not mandate certification to any particular standards to meet your objectives. You could follow a recognised industry standard, such as ISO 9001, ISO/IEC 20000 or the Information Technology Information Library (ITIL)®. Depending on which sector you operate in, you could also follow Six Sigma™.

11.4.d. You must have policies or documentation that describe how you approach end-to-end service management in areas such as:

- service design;
- service transition; and
- service operation.

11.4.e. Your management system documentation must include the following information:

- how your management processes are organised;

- how you measure how well you have met your objectives;
- who in your organisation is responsible for meeting the objectives;
- how you carry out routine operational tasks;
- what standards you follow;
- what tools, funding, people and other resources you need;
- how you plan to improve the quality of your products or services on an ongoing basis (known as 'continuous improvement');
- how you deal with customer relationships; and
- how you resolve service disappointments.

11.5. Information management

11.5.a. Your organisation must have an information management system that follows industry standards, such as ISO/IEC 27001 and the ISO/IEC 27701 extension. If you do not follow these standards, you must still ensure your information management system meets the criteria detailed in this section.

11.5.b. An information management system is a collection of documents that explains:

- why your organisation needs to keep the information it keeps, covering both personal and non-personal data;
- how you create, organise and store information;
- who has access to the information;
- how information is classified;
- how you share information (including why it is shared, who it is shared with, how often it is shared, what format it is in and how it is protected);
- how long you retain and how you protect data; and
- how you archive information.

11.5.1. Archiving information

11.5.1.a. You must have an archiving policy that:

- meets any legislative or regulatory requirements that apply to your organisation; and
- follows any standards or best practice relevant to the industry or sector your organisation is part of.

11.5.1.b. It must also explain:

- how archived information is used to support your organisation's work;
- why your organisation needs continued access to archived information;
- the risks of not having access to archived information;
- how archiving information protects the interests and legal rights of your organisation and others you work with; and
- the relationship between this information and any other records, data or evidence you keep.

11.5.2. Disposal schedule

11.5.2.a. You must have a documented disposal schedule that records how you manage and delete information. It must show:

- that you have policies in place to meet any legislative or regulatory requirements about keeping and deleting information;
- what information was created but later deleted;
- what format the information is in (for example if it was physical or digital);
- where information is located; and
- how information is transferred for disposal, if this is relevant.

11.5.3. Data management

11.5.3.a. You must have a documented data management policy that explains how you create, obtain, hold, transform, share, protect, document, dispose of and preserve data. It must include:

- file naming conventions;
- how you create and manage metadata;
- how your organisation makes sure data is available when it is needed;
- how you know data is accurate and complete; and
- how you maintain and secure your data.

11.5.3.b. Your data management policy must cover the full data and metadata lifecycle. It must explain how architectures, policies, practices and procedures are implemented and maintained.

11.6. Information security

11.6.a. Information security incorporates cyber security as well as broader security considerations. You must have an information security management system that follows an industry standard, such as ISO/IEC 27001, and complies with requirements in UK data protection legislation. If you do not follow this standard, you must still ensure your information security management system meets the criteria detailed in this section. This must ensure your organisation can control and evaluate how you handle data when it is stored, transmitted or otherwise processed.

11.6.b. Your information security management system must be based on the principles of the 'CIA Triad':

- confidentiality (11.6.1.), which involves preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;
- integrity (11.6.2.), which involves guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity; and
- availability (11.6.3.), which involves ensuring timely and reliable access to and use of information.

11.6.c. At minimum, you must also have documents that cover the following to support your information security policy:

- technical controls;
- organisational controls; and
- physical security controls.

11.6.d. NCSC guidance on building and operating a secure online service can support you in the development of your information security management system.

11.6.e. You could also conform with and be certified against Cyber Essentials or Cyber Essentials Plus.

11.6.1. Confidentiality

11.6.1.a. You must make sure any information your organisation keeps can only be accessed by authorised users. For example, you could require that users need an authenticator (such as a password) to access the information.

11.6.1.b. You could also use an access-control list or role-based access control to protect information held by your organisation. If you do, they must specify:

- which people or systems can access your information;
- how they are granted access; and
- what they can do with your information.

11.6.1.c. This could be explained in your organisation's password control policy or access control policy.

11.6.1.d You must have a policy that classifies confidential information, describes who has access to what and ensures that there are appropriate levels of protection for confidential information. This could follow ISO 27001 Control objective A.8.2 Information Classification. At minimum this must detail:

- the types of information you are storing;
- how critical to business processes or service provision that information is;
- the risks of misuse or mishandling and the consequences of the data being lost or hacked; and
- the value of that data/information to your business or to a bad actor.

11.6.2. Integrity

11.6.2.a. You must have policies to maintain the integrity of any information your organisation holds. You might need to provide these and demonstrate compliance with them for legal reasons, for example if you suffer a breach. Your organisation must also have an information security policy that explains how you will:

- stop information from being modified, either by accident or on purpose (including how you will protect it against malicious acts);
- provide assurances that information is trustworthy and accurate;
- keep information in its 'correct state' – the format or reason for collecting the information must not change;
- restore information to its correct state if you suspect it has been tampered with;
- use secure communication protocols to help secure data in transit;
- how you perform data validation and verification;
- regular backups and recovery plans;
- how you maintain data versioning and timestamps;
- what audit trails and logs you keep and how you protect them; and

- what error handling mechanisms you have implemented.

11.6.3. Availability

11.6.3.a. You must have policies and procedures to make sure that any information your organisation keeps is consistently managed and only readily accessible by authorised users. At minimum, you will need:

- tools and processes that can cope with the amount of requests you expect to get; and
- a backup policy, in case you need to recover any information, which must explain your Recovery Time Objective.

11.6.3.b. You must explain how these work in your:

- data support and operations plan;
- policy and business/organisation continuity plan;
- disaster recovery plan; and
- information security policy.

11.6.3.c. You must avoid single points of failure, where any component such as a server or a network connection could result in your whole system stopping working. You could achieve this by implementing power supply management, load balancers and regular maintenance and monitoring. You could also implement redundant systems and network redundancy to enhance data availability.

11.6.4. Technical and security controls

11.6.4.a. You must have a document that explains what hardware and software you use to protect information, such as firewalls, intrusion detection systems and encryption techniques. It must also explain what software you use to monitor and control access to information.

11.6.4.b. You could follow NCSC guidance on Secure Design Principles and the NCSC Cyber Assessment Framework (CAF).

11.6.5. Organisational controls

11.6.5.a. You must have a document that explains how you will continue to meet security rules. For example, it could explain what information security training your staff will regularly have to complete. It must explain what roles are in your organisation and what parts of the information security process they are responsible for.

11.6.6. Physical security controls

11.6.6.a. You must have a document that explains what security controls protect the physical locations where the following things are kept:

- any information your organisation has; and
- any technology that helps you provide your products or services.

11.6.6.b. It could include how you:

- assessed the risks of hosting information in different locations;
- secure any data centres or locations you use that are operated by third parties; and
- protect information and technology when they are accessed from a remote location (i.e. outside of the usual place of work).

11.6.7. Security governance

11.6.7.a. You must take steps to ensure that your information security policy is followed at all times and that you have a way for managing security risks. This is also known as ‘security governance’.

11.6.7.b. You must:

- make a security plan based on security risks you have identified;
- have a process for investigating and responding to security risks;
- report security risks in a way that is proportionate to your organisation and product or service; and
- have a robust assurance and review process.

11.6.8. Using security measures to protect the information you collect
11.6.8.a. You must use technical and organisational safeguards to protect personal data. Your security measures must also guarantee the confidentiality and integrity of information. This means they need to reliably protect information from:

- loss or misuse;
- unauthorised use, access, modification or disclosure; and
- fraudulent use.

11.6.8.b. To do this, you must demonstrate that you:

- use robust safeguards (for example, pseudonymisation, anonymisation and encryption);
- use security measures that ensure confidentiality, integrity and availability;
- test your security measures regularly, using the same tests each time, and improve them whenever you can;
- can quickly restore access to personal data if there is a physical or technical incident; and
- know how you will tell people if there is a security breach, so they can protect themselves from potential identity theft.

11.6.8.c. You must also show how you meet these rules in your ongoing internal audits.

11.7. Risk Management

11.7.a. You must have a risk management framework that follows industry standards, such as:

- ISO/IEC 27005; or
- ISO 31000.

11.7.b. If the standard you follow is not one of the above, your risk management framework must still include guidance about how to:

- identify risks to your organisation, including where they can come from and the impact they could have;
- identify risks to your users, which could include phishing attacks, man in the middle attacks and imposter attacks;
- find out how likely it is that risks could materialise;

- measure how effective your current processes are at managing risks;
- compare any risks you have identified to the established risk criteria;
- monitor risks;
- report risks to your stakeholders;
- measure residual risk;
- write, implement and maintain your organisation's risk strategy; and
- protect your organisation from internal risks, including producing a whistleblowing policy and a bribery and corruption policy.

11.7.c. You could use NCSC guidance on cyber security-related risk management to develop your risk management framework.

11.7.d. You must set out and communicate the risks you will and will not take in pursuance of your organisational goals. This is often referred to as a statement of risk appetite and it will help those who are responsible for making risk management decisions understand where the risk management boundaries lie.

11.8. Keeping records

11.8.a. You must record what your service did to create, manage, share or consume a digital identity or attribute. You must do this in a way that meets the requirements in Article 30 of the UK GDPR.

11.8.b. You must keep your own copies of any records. You must dispose of these records when you no longer have any use for them.

11.8.c. When sharing identity or attribute information with a relying party or another service, you may need to make sure they get a copy of any records about that digital identity or attribute.

11.8.d. Before you start keeping records, you must have:

- clear rules for keeping, managing and disposing of them;
- a records management policy and a disposal statement; and
- a named person in your organisation who oversees records management.

11.8.e. You must have rules that cover your day-to-day records management. At minimum, these must cover:

- which records to keep;
- who keeps them;
- how to keep them, covering the formats and media you use; and
- when to dispose of them – this is usually covered in a disposal statement.

11.8.f. The rules for your organisation can be as detailed as you need them to be. These rules could be a part of your records management policy or maintained separately.

11.8.1. Records management policy

11.8.1.a. You must have an up-to-date and internally published records management policy. The policy must include:

- a commitment to managing records, including what is covered and why;
- the policy's objectives (for example, to help you meet standards or legal requirements);
- how the records management policy relates to your organisation's other policies, such as data security, complaints or fraud policies;
- the job roles in your organisation and what their records management responsibilities are; and
- specific plans for records that are particularly important or sensitive.

11.8.1.b. To help employees understand why it is important to follow the management rules and keep records correctly, you must demonstrate that it is easy for anyone in your organisation to find and use the policy.

11.8.1.c. You must demonstrate you have agreed the records management policy at a senior level. It could be part of your wider information management strategy.

11.8.2. Other record keeping responsibilities
11.8.2.a. You must also:

- have documented guidance on naming conventions;
- know how (and how often) you are going to check that your records are being managed according to your policy; and
- make sure that access to records is controlled and monitored.

11.8.3. Disposing of records
11.8.3.a. Your organisation must have clear, documented rules on how long to keep records for, in line with ICO guidance on retention policies, to assist in demonstrating compliance with the storage limitation principle set out in the UK GDPR. When you no longer need information, you must dispose of it in a safe and secure way. Before you decide whether to keep or dispose of a record, you must consider whether you may need it for:

- legal reasons;
- performance analysis;
- complaints and disputes responsibilities;
- fraud analysis; or
- audits or other investigations.

11.8.3.b. You might need to keep just part of the record. For example, a provider conducting age verification checks might retain that they have completed an age check for a user, but not retain the data used to complete that check.

11.8.4. Disposal statement
11.8.4.a. Your organisation must have a formal written disposal statement. It must include the types of record you handle and:

- how long you keep each type;
- how you dispose of each type; and
- your processes for archiving and destroying records.

11.8.5. What people in your organisation need to do

11.8.5.a. Anyone who handles records must follow the records management policy. This includes temporary staff and contractors. You must demonstrate that you have processes in place to ensure that everyone who works for your organisation knows:

- which information needs to be added to the record-keeping system;
- what your records management policy is; and
- what they must do to comply with data protection legislation and (if your organisation is a public authority) the Freedom of Information Act (2000) or where relevant, the Freedom of Information (Scotland) Act (2002). For more information, see the ICO guidance on freedom of information requests.

11.8.6. Accountability for records management

11.8.6.a. You must choose a named person with accountability for overseeing your records management. They are ultimately responsible for making sure your records are accurate, accessible and secure. They must:

- check your records are being managed according to the records management policy and disposal statement;
- make sure you meet your legal and regulatory requirements;
- set up or maintain your record-keeping systems;
- identify important or sensitive records that need specific management plans;
- set up a way to document who has accessed, added or changed a record; and
- act as a single point of contact for records management issues.

11.9. Withdrawing from the trust framework

11.9.a. In case you withdraw from the trust framework, you must demonstrate you have a transition plan and policies to:

- notify all users of your product or service;
- notify any relying parties that consume identities and/or attributes you have created; and
- notify your CAB and OfDIA.

11.9.b. In case you retire your product or service, you must also demonstrate you have a transition plan and documented processes to:

- provide users, other services you work with and relying parties with a reasonable period of time to migrate to other providers; and
- dispose of any data you hold in an appropriate way.

12. Service requirements

12.1. Making your products and services interoperable with others

12.1.1. Data schema

12.1.1.a. The trust framework data schema provides guidance for services and relying parties on how to organise and exchange information in a consistent way to enable interoperability. It describes the outcomes of different GPG 45 identity verification processes in a machine-readable format. To enable open and collaborative development, the data schema has been uploaded to GitHub.

12.1.1.b. You could use the data schema to help ensure your service is interoperable with other certified services and relying parties. It is recommended that the data schema is followed across the market to encourage interoperability between organisations, in the UK and internationally.

12.1.1.c. The data schema has been written to be consistent and not in conflict with different industry approaches for data exchange and technical standards, such as OpenID Connect and W3C's Verifiable Credentials data models.

12.1.2. Receiving messages from trust framework participants

12.1.2.a. If your service shares data with or receives data from other trust framework participants, you must be able to validate the integrity of messages you are receiving from those participants.

12.1.3. Sharing digital identities and attributes

12.1.3.a. When sharing a user's digital identity or attribute information with another service or relying party, you must provide enough information for them to be able to:

- identify the person; and/or
- decide if the person or organisation is eligible for something.

12.1.3.b. If the digital identity or attributes belong to a person, you could provide a:

- date of birth;
- first name;
- last name; or
- a unique identifier for the user, such as a user or account number.

12.1.3.c. To check if a person is eligible to do something, a relying party could also ask you for more information. This could include their:

- nationality;
- place of birth;
- previous name(s);
- email address;
- address;
- phone number;
- gender;
- occupation;
- income;
- citizen registration number (for people resident outside the UK or non-UK nationals);
- tax reference number;
- biometric information;
- passport number;
- qualifications;
- employment history;
- non-UK identity card number; or

- role in an organisation.

12.1.3.d. The relying party will need to decide if the information is sufficient for what they need. Knowing where the attribute comes from and how it has been checked could help them make this decision.

12.1.3.e. If the digital identity and attributes are linked to a UK or international business, your service may need to provide:

- its legal name; or
- a registered identifier, such as a Companies House number.

12.1.3.f. To check if an organisation is eligible to do something, a relying party could also ask you for more information. This could include:

- any email addresses associated with the business;
- any addresses associated with the business;
- the country of its incorporation;
- its VAT number;
- its turnover;
- its Legal Entity Identifier (LEI);
- its Standard Industrial Classification (SIC) code;
- its Economic Operators Registration and Identification (EORI) number;
- its Excise Authorisation Verification (SEED) number;
- its Data Universal Numbering System (DUNS) number; or
- its data protection registration number.

12.2. Checking if a user can act on behalf of an organisation or another person

12.2.a. Some users may be acting on behalf of an organisation or another person when they interact with you. This is known as ‘delegated authority’. There are a number of reasons why this might be appropriate, such as:

- the user might have been formally appointed using a lasting power of attorney (LPA) to look after someone else’s money and property;
- the user may be a parent or legal guardian acting on behalf of a child where the child is not old enough to access a service themselves; or
- the user might be appointed to act on behalf of an organisation. To do this they need to be able to:
    - assert proof of their identity;
    - have attributes that show the organisation exists; and
    - have this linked to the organisation that they are representing.

12.2.b. A user will only have delegated authority if they have been given permission to make decisions and complete tasks on behalf of the other person or organisation. A user may have delegated authority on a one-time basis, related to one specific task or service, or something more comprehensive. A user does not necessarily have delegated authority if they are helping someone do something. This could include:

- a user helping a friend who is not confident using a computer to fill in an online form; or
- anyone who offers ‘assisted digital support’ to users of a product or service.

12.2.c. You can choose whether to offer delegated authority as part of your service. If your service permits delegated authority of any type, you must follow the delegated authority guidance, including checking if the user has the necessary authority to act on someone else’s behalf, and demonstrate how you meet the guidance’s requirements. The details of their agreement with the other person might exist as an attribute.

12.2.d. If you are a holder service provider, you can allow a user to hold details about the identity or attributes of another person if they have authority to act on that person’s behalf.

12.3. Encryption and cryptography

12.3.a. The requirements in this section outline the minimum expectations for encryption and cryptographic controls and security measures. These are deliberately described as technology and vendor agnostic to cover numerous solutions. How you apply or implement these controls and methods is not prescribed as it is reasonable that the details of your specific implementation will be based on your technology choices.

12.3.b. You must carry out a thorough risk assessment of threats that could manifest for your service. In some cases, this will mean you need to exceed trust framework requirements, especially where there is a high risk due to the sensitivity of data.

12.3.c. You must implement cryptographic controls that follow industry standards and best practice for encryption and cryptographic techniques. These must ensure you can protect the confidentiality and integrity of electronic information in transit or at rest, and can mitigate against physical or logical threats.

12.3.d. You must have cryptographic controls that can authenticate the identities of both the sender and recipient to one another. The controls must protect against repudiation.

12.3.e. You must describe these controls and processes in an encryption and cryptographic controls policy document. You must also regularly test and update these controls.

12.3.f. Data on any type of media must be protected from theft.

12.3.g. You must protect your networks from typical hacking activities such as sniffing data packets across the network. You must also have a robust process to monitor network activity.

12.3.1. Encryption

12.3.1.a. When dealing with data at rest:

- all user-writable partitions on portable devices and portable storage media must be encrypted at the media-level (i.e. ‘Full Disk Encryption’);
- information held encrypted at rest must also be integrity protected;
- where multiple layers of encryption are available such as media-level and database field level, you must ensure each layer is applied proportionally to mitigate risks;
- the encryption software deployed on devices must restrict the number of authentication attempts within any given time interval; and
- encryption software deployed on devices must also have sufficient entropy as part of the authentication mechanism. Where passwords are used as the authentication mechanism

that password must be of sufficient length to match the password policy defined for the system.

12.3.1.b. When dealing with data in transit, encrypted communications channels must be protected using protocols, protocol suites and techniques in accordance with industry standards and best practices. You could use one of the following methods:

- at the application layer, using Transport Layer Security (TLS), ensuring this is the latest version;
- at the network layer, using Internet Protocol Security (IPsec); or
- following the NCSC guidance on using IPSec to protect data and consulting the most up-to-date cryptography profiles.

12.3.1.c. You could also consult the following NIST guidance:

- NIST SP 800-213A: Data Protection – Secure Transmission; or
- NIST SP 800-213A: Device Security – Secure Communication.

12.3.2. Cryptography

12.3.2.a. For further information on handling cryptographic modules, you could consult the following:

- NIST FIPS 140-2 – Security Requirements for Cryptographic Modules; and
- NIST FIPS 140-3 – Security Requirements for Cryptographic Modules (140-3 aligns with standards from ISO/IEC).

12.3.2.b. The specific standards and best practices you follow may vary depending on the maturity of the technical approach. As well as the standards above, you could consult the following standards:

- NIST SP 800-175B – Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms;
- ETSI TS 103 458 – Application of Attribute Based Encryption (ABE) for PII and personal data protection on Internet of Things (IoT) devices, WLAN, cloud and mobile services.

12.3.2.c. Additional guidance for encryption algorithms can be found in the ISO/IEC 18033 family of standards.

12.3.2.d. For guidance on hash functions, you could read the following standards:

- ISO/IEC 9797-2 – Information security — Message authentication codes (MACs);
- ISO/IEC 9797-3 – Information technology — Security techniques — Message Authentication Codes (MACs);
- ISO/IEC 10118 – Information technology — Security techniques — Hash-functions;
- NIST FIPS 180-4 – Secure Hash Standard (SHS);
- NIST FIPS 202 – SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions; and
- NIST SP 800-107 – Recommendation for Applications Using Approved Hash Algorithms.

12.3.2.e. For key management and generation you could follow:

- ISO/IEC 11770 – Information technology — Security techniques — Key management;
- ISO/IEC 18031 – Information technology — Security techniques — Random bit generation; and
- ISO/IEC 18032 – Information security — Prime number generation.

12.3.3. Entity authentication

12.3.3.a. To evidence how you achieve entity authentication for verification of the sender, there are several cryptography-based mechanisms and protocols you could apply. These could include symmetric systems, digital signatures, zero-knowledge techniques and checksums. These topics are covered in: ISO/IEC 9798-1:2010 – Information technology — Security techniques — Entity authentication.

12.3.4. Digital signatures

12.3.4.a. Digital signature mechanisms are essential to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity.

12.3.4.b. It must be computationally unfeasible for an attacker:

- to produce a valid signature on a new message;
- to recover the signature key; or
- in some circumstances, to produce a different valid signature on a previously signed message.

12.3.4.c. It must be computationally unfeasible, even for the signer, to find two different messages with the same signature.

12.3.4.d. If your service includes electronic signatures, and unless you can evidence that another standard achieves the same outcomes, you must follow current Digital Signature Standards, such as:

- NIST FIPS 186-5 – Digital Signature Standard (DSS);
- ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- ISO/IEC 9796 – Information technology — Security techniques — Digital signature schemes giving message recovery;
- ISO/IEC 14888 – IT Security techniques. Digital signatures with appendix;
- ISO/IEC 18370 – Information technology — Security techniques — Blind digital signatures; and
- ISO/IEC 20008 – Information technology — Security techniques — Anonymous digital signatures.

12.3.4.e. There are techniques, symmetric and asymmetric, for the provision of non-repudiation services. Digital signatures can be used to provide non-repudiation by ensuring that the sender and receiver of a message cannot deny that they, respectively, sent or received the message. You could follow ISO/IEC 13888 – Information security — Non-repudiation to achieve these techniques.

12.4. Fraud management

12.4.a. You must follow best practice guidance on fraud management. Best practice can vary between sectors and regulatory environments. For example, this could include:

- Guidance from the Chartered Institute of Public Finance and Accountancy (CIPFA);
- Government Functional Standard GovS 013: Counter fraud;
- Government Functional Standard GovS 009: Internal Audit;
- Guidance from the Association of Certified Fraud Examiners (ACFE); and/or
- Guidance from the Chartered Institute of Management Accountants.

12.4.1. Fraud monitoring

12.4.1.a. You must have processes in place to monitor for threats to your service and attempted fraud (whether successful or not). Where relevant to your service, these must include:

- misuse of your service – where your service is not being used in compliance with your terms of service or the trust framework;
- impersonation – where someone is using the identity of someone else;
- synthetic identity – where someone is using a made up identity;
- takeover – where someone uses an account that is not theirs; and
- document fraud – where counterfeit, forged or camouflaged documents are being used within your service.

12.4.1.b. Your monitoring processes must take into account all channels that are used to deliver your service.

12.4.1.c. Where relevant to your service, your monitoring processes must include:

- known fraud – you must undertake checks to establish whether there is a potential link to previous incidents of known fraud. This must be done at registration and at sufficient intervals to manage the risk of enabling the use of a synthetic identity or impersonation of a real person. This must include a check on if the individual has been a victim of fraud; and
- evidence failures – you must monitor whether a user fails an evidence check that they should pass, especially in the case of repeated failure. You must have a process to establish whether the failure is indicative of potential fraud.

12.4.1.d. Your fraud monitoring processes must be assessed during internal audits. You must conduct fraud audits at least annually. You must also have a process to establish whether incidents where there is a suspicion of fraud should trigger additional fraud audits or exceptional audits conducted by an independent internal auditor or a third-party.

12.4.1.e. If an identity has been verified at a low level of confidence, has been recently repaired or you have recently detected fraud activity associated with that identity, it is considered ‘higher-risk’ and you must put additional security policies in place. These could include details about how you will work with relying parties to manage higher-risk identities. If you determine an identity to be higher-risk for other reasons, you could apply similar additional security policies.

12.4.2. Policies and procedures for fraud management

12.4.2.a. You must make sure you follow all relevant legislative requirements for the sector(s) you work in or with, including:

- thresholds for investigating;
- data sharing agreements;
- fraud dispute and resolution processes; and

- interacting with individuals you believe or suspect to have committed fraud.

12.4.2.b. You must do a risk analysis and identify the potential ways that someone may use your service for fraud or to carry out fraud against your service.

12.4.2.c. When setting thresholds for investigating, you must consider whether the thresholds could unfairly impact genuine users or allow inappropriate or unacceptable activity to take place. You must demonstrate you review your thresholds at least annually to make sure that they are still effective.

12.4.2.d. If you suspect any criminal activity has taken place, you must have processes in place to prevent further criminal activity and ensure your cooperation with appropriate law enforcement agencies.

12.4.2.e. You must also have a clear understanding of legal and regulatory mechanisms for sharing fraud data. What these are may depend on which industry or sector you are working in.

12.4.3. Reporting fraud

12.4.3.a. You must:

- define a set of indicators to make sure reporting and analysis is consistent;
- have a standardised, structured, clear reporting process for all connected services, organisations, users, regulators, and agencies;
- have minimum operational rules for monitoring fraud and threat alerts;
- following an incident, send reporting and analysis to the relevant authorities to help manage the threat of identity fraud and identity misuse;
- keep a log of any revoked or suspended accounts;
- keep a log of any breaches; and
- advise when an external source has been breached.

12.4.3.b. Information your report could include is, for example:

- the claimed identity;
- all information that was gathered or used during the proofing process;
- any persistent identifiers; and
- the indicators discovered, where they came from and details of any actions taken. For example this could include indicators related to:
    - evidence that is known to be lost, stolen or revoked;
    - evidence that is not known to exist;
    - a unique reference number, issue data or expiry date from evidence that is known to be false;
    - email address or phone number that might be compromised, or used to create a lot of accounts recently;
    - a user that does not look like the person on a piece of evidence;
    - biometric information that does not match what is on the evidence;
    - any other information you have used to determine that the user may not be genuine;

- IP addresses used by the user; and
- date, time and session identifiers.

12.4.4. Intelligence and fraud analysis

12.4.4.a. You must have a way to:

- actively look for suspicious activity;
- monitor transactions, including for harvesting of data where a third-party is using your service to gather information and data about your users;
- detect indications of coercive behaviour; and
- carry out threat intelligence.

12.4.4.b. You could carry out this analysis using methods such as:

- device monitoring – analysing if the device can be linked to other registrations, to known fraud or suspicious devices;
- anomaly detection – analysing if there are discrepancies or patterns in key information that are indicative of a potential attack or fraud; and
- velocity detection – analysing if there is repeated use of key information and behavioural discrepancies such as if the user is not 'realistic' or 'normal'.

12.4.4.c. Where transactions are part of your service, you could follow the NCSC guidance on transaction monitoring for online services.

12.4.5. Sharing threat indicators

12.4.5.a. You must:

- have a structured and secure way to send and receive relevant identity and attribute data and intelligence;
- notify all relevant parties, including the victim, if there is a fraud incident;
- have a process for sharing information around detected and mitigated fraud threats; and
- have a process for reporting cyber security and fraud incidents.

12.4.5.b. You could also sign up to an agreed shared signals approach for sharing threat and fraud intelligence with other trust framework participants.

12.4.5.c. If fraud or crime is suspected (either during initial interaction with the user or on an ongoing basis) that meets the approved threshold for your industry or sector, you must save the relevant metadata and artefacts (where doing so complies with relevant data protection and other legal considerations) for investigation.

12.4.5.d. You could use open and/or common standards to share cyber threat indicators with other participants, for example STIX and TAXII.

12.5. Responding to incidents

12.5.a. You must have processes for dealing with incidents that could have an impact on your product, service or users. These incidents might be related to:

- fraud, for example if a user's identity is being used by someone else to sign in to your service;

- service delivery, for example if users cannot use your product or service because it is temporarily unavailable; or
- a data breach.

12.5.b. Your processes must follow industry best practice, such as the NCSC guidance on incident management and the NCSC best practice on logging and monitoring, in addition to any legislative requirements.

12.5.c. You must publish easily accessible details about your incident response processes, including the contact details your customers can use to report an incident. You could also publish the timelines you expect to meet when dealing with incidents.

12.5.d. You must have processes in place to identify, notify and support a user whose information has been compromised due to incidents such as fraud or a data breach. For users with a holder service account, refer to section 12.5.4. which details how to do this.

12.5.e. You must have processes in place to manage requests from law enforcement agencies, your CAB, OfDIA or another trust framework participant if they are investigating an incident. You must ensure that you comply with the data protection legislation when responding to any such request.

12.5.1. Responding to a fraud incident

12.5.1.a. You must follow industry best practice and guidance if you suspect that fraudulent activity has taken place, for example if a user is:

- using a synthetic (made up) identity; or
- pretending to be someone they are not, alive or dead.

12.5.1.b. You must have an incident response plan that:

- makes sure effective and timely action is taken if fraud happens;
- explains who in your organisation will be involved in responding to the incident;
- minimises losses for users;
- ensures you collect evidence that could be required for future investigations;
- notifies the relevant organisations if an identity or attribute is found to be fraudulent;
- covers any necessary communication security rules; and
- explains how you will provide law enforcement agencies with information about the incident, in line with legal and regulatory requirements.

12.5.1.c. You must have policies for how you will support a relying party's investigation if they alert you to a suspected fraud incident involving your product or service.

12.5.1.d. If you discover a suspected fraud incident, you can refer to the flow down terms to establish what support a relying party can provide to investigate the incident.

12.5.2. Responding to a service delivery incident

12.5.2.a. You must have a process for managing and responding to service delivery incidents. This process must follow industry good practice, such as the Information Technology Infrastructure Library (ITIL)® service management processes. If you follow different best practices, your process must cover how you will:

- log, categorise, prioritise and assign incidents;

- create and manage tasks;
- manage and escalate service level agreements (SLAs); and
- resolve and close incidents.

12.5.3. Responding to data breaches

12.5.3.a. You must have documented processes for responding to a data breach. These processes must comply with the requirements under data protection legislation regarding data breaches, as explained in the ICOs guidance on how to respond to data breaches.

12.5.3.b. Data breaches can lead to:

- identity theft;
- threats to a user's safety or privacy; and/or
- emotional or financial damage to a user.

12.5.3.c. If a data breach happens, you must have a process to tell any users whose personal data might have been affected. You must contact them using a method that is appropriate for your users, product or service. You must also inform both OfDIA and your CAB with information about the incident within 72 hours of discovering a data breach, in addition to, where relevant, meeting legal requirements to inform the ICO.

12.5.4. Responding to suspicions that a user's holder service account is compromised

12.5.4.a. There are a variety of ways that a holder service account can become compromised. Usually this is a result of deliberate fraudulent activity where an impostor has obtained unauthorised access. This can also happen because there has been a data breach.

12.5.4.b. If a user suspects their holder service account is at risk of being compromised, you must be able to freeze or temporarily suspend it if they request this.

12.5.4.c. If you suspect a user's holder service account has been compromised, you must complete an investigation to confirm whether fraud has taken place.

12.5.4.d. If during your investigation, you suspect someone who should not have access to a holder service account has either accessed or used it, you must have processes in place to:

- suspend the holder service account until you establish if the user is genuine;
- let the user know their holder service account has been suspended;
- establish if the user is genuine; and
- ask them to look at their recent holder service account activity, and check if there are any interactions they do not recognise.

12.5.4.e. Your investigation process must mitigate the risks that you could cause emotional distress to a genuine user or educate an attacker on how your fraud controls work.

12.5.4.f. If your investigation concludes that the holder service account has been compromised, you must have a process in place to inform the rightful user (where contact is possible) and take them through a holder service account recovery process if they request it. This recovery process must follow the guidance in GPG 44 that outlines what to do if an authenticator has been forgotten, lost or stolen.

12.5.4.g. If you also verified the user's digital identity, you must prove and verify the user's identity again. You must reverify the user's identity using either:

- the same level of confidence originally adopted but a different identity profile;
- the same level of confidence and identity profile but different identity evidence; or
- a higher level of confidence than the one originally adopted. You could also consider using different identity evidence.

12.5.5. Helping a user repair their identity

12.5.5.a. Identity repair refers to users regaining the use of their rightful identity after becoming a victim of identity theft. You must:

- publish easily accessible contact details that your users can use to get support from you for identity repair; and
- have documented processes in place to follow the Action Fraud identity fraud victims' checklist to advise users on steps they can take.

12.5.5.b. Where you are able to confirm an instance of identity theft has occurred, you could, where requested, provide rightful users with evidence to support their onward identity repair.

12.6. Telling users about your product or service

12.6.a. You must make sure your users know exactly what your product or service does. You must clearly explain:

- any terms and conditions of use that the user needs to be aware of;
- any fees that the user will need to pay to use your product or service; and
- how you make money from your service ('business monetisation statement'), where relevant. This must be separate from the terms and conditions and easy for the user to access.

12.7. Privacy and data protection rules

12.7.a. Personal data is any information relating to an identified or identifiable natural person. You must follow data protection legislation whenever you do anything with users' personal data. The ICOs data protection guidance for organisations explains what requirements you must meet, and you must check your legal obligations carefully.

12.7.b. The trust framework does not determine which lawful basis you should use to process personal data. Choosing an appropriate lawful basis is your responsibility if you are a data controller. The lawful basis for processing data is distinct from the additional requirement in the trust framework to confirm a user understands how their data will be shared and processed. The rules for confirming a user's understanding are set out in sections 12.7.3. and 12.7.4.

12.7.c. Due to the importance of personal data to digital verification services, you will be audited as part of the trust framework certification process to ensure you are complying with data protection legislation and, in particular, that you are meeting the following legislative requirements or related best practice.

12.7.d. This list is not exhaustive of all data protection legislative requirements, but instead highlights areas which are particularly important for certified services. Any ICO guidance referenced explains the law and sets out recommended best practice to meet these statutory obligations.

12.7.e. You must:

- have appointed a data protection officer (DPO) to carry out the tasks defined in article 39 of the UK GDPR, even if you do not meet legislative requirements outlined in article 37;
- identify whether you are a data controller (including joint controller) or data processor, and demonstrate that you have understood your resulting obligations;
- have completed a Data Protection Impact Assessment (DPIA), also known as a 'privacy impact assessment', for your service(s), before processing any data if you are a data controller. This must include, amongst other things, justification for your lawful basis for processing, and detail all forms of personal data which may be processed or created as a result of your service (e.g. analytics data);
- be registered with the ICO as a data protection fee payer, unless you are exempt;
- have processes in place to ensure compliance with the 'data minimisation' principle, particularly when sharing data with other organisations, within the parameters of your particular service or use case;
- have processes in place to ensure 'data accuracy', including accuracy of personal data you collect and create;
- have established a clear process to ensure compliance with the 'storage limitation' principle and have set retention periods for the data you hold;
- have a clear process to manage requests related to 'right of access', 'right to rectification', 'right to data portability' and 'right to erasure'. These rights have been highlighted for auditing, but you must have a clear process for all data protection rights;
- have given consideration to how your service safely accommodates and protects children. Where relevant, you must comply with the Age Appropriate Design Code;
- meet the requirements of Article 22 of the UK GDPR on automated decision-making and profiling, where automated decision-making is part of your service. This includes having a clear process for managing user requests about their rights with regards to automated decision-making. The ICO guidance on automated decision-making and profiling can help you meet legislative obligations; and
- follow legislative requirements where your service processes biometric or other special category data. When processing special category data, you need to ensure you have identified a specific condition for the processing under Article 9 of the UK GDPR. The ICO guidance on special category data can help you meet legislative obligations.

12.7.1. Transparency

12.7.1.a. You must comply with the UK GDPR principle of 'transparency' by using a privacy notice. In addition to the information which you must provide to data subjects under either Article 13 or 14 of the UK GDPR, for the purposes of the trust framework, where sections 12.7.3. and/or 12.7.4. apply, your privacy notice must:

- specifically emphasise the lawful basis you are using for data processing; and
- make clear what the role of the user confirmation is.

12.7.1.b. You must regularly review the information you provide to users through the privacy notice and update it as required. You must also inform users of any new uses or changes to the third-party organisations you partner with, before making any such changes.

12.7.2. Data protection by design and default

12.7.2.a. You must follow privacy best practice, including legal requirements, and the ICO guidance on 'data protection by design and default'.

12.7.2.b. If you are a data controller, you must also demonstrate that your privacy compliance process follows an industry standard such as ISO/IEC 27701. If you do not follow this standard, you must demonstrate that you have processes to achieve the same outcomes.

12.7.3. Confirming a user's understanding of how their data will be shared

12.7.3.a. If your service has direct contact with end users, as opposed to only providing services to other organisations, you must confirm that the end user understands how their identity or attribute information will be shared or disclosed. This must include any data processing undertaken by third-party services or components you use as part of your service, and is in addition to legal requirements to provide a privacy notice and determine the lawful basis for processing personal data (see section 12.7.1. above).

12.7.3.b. When confirming understanding you must:

- use clear, plain language that is easy to understand;
- ask the user to positively confirm their understanding;
- name your organisation;
- specify why you or others in your supply chain are processing the data and what you are going to do with it, including whether the data will be retained in databases for future fraud checks;
- describe or name the third-party services that will process the user's data. For example, you could confirm the user's data will be checked with a credit reference agency; and
- record when and how a user confirmed their understanding, and what they were told at the time.

12.7.3.c. You must also clearly explain to the user:

- what the consequences of refusing to confirm their understanding would be, including the impact on their ability to access services; and
- whether they can withdraw this confirmation at a later stage, and what the implications of doing this would be.

12.7.3.d. You may wish to provide additional information about what it means for a user to confirm their understanding, for example by providing more information on the relationship between confirming a user's understanding and requirements under data protection legislation. In these situations, you could include this information in your privacy notice, in line with the requirements in section 12.7.1. above.

Illustrative example 9

Raya has to complete a right to rent check before leasing her new flat. Her landlord offers her the option of a digital right to rent check, using a service certified against the trust framework and the supplementary code for digital right to rent checks.

Raya starts the digital check and reads an explanation of how her identity data will be processed, shared and disclosed in the verification process.

Raya is not confident she understands the information provided, so she declines to confirm her understanding. Without Raya confirming her understanding of how her data will be disclosed, the provider is unable to offer Raya a digital check.

Raya returns to her landlord who instead undertakes a right to rent check using physical documents.

12.7.4. Confirming a user's understanding for holder services

12.7.4.a. If you are a holder service provider, you must follow the requirements in section 12.7.3. to confirm a user's understanding of how you will share and disclose their identity and attribute information when a user first signs up to use your service.

12.7.4.b. You must also have processes in place to reconfirm a user's understanding at appropriate intervals. You must reconfirm a user's understanding by following the requirements in section 12.7.3.:

- if you make any changes to how your service handles their data;
- if your service's purpose deviates from that which the user originally confirmed their understanding about when signing up; or
- before allowing your service to be used again, if it has been more than 14 months since you last reconfirmed their understanding.

12.7.4.c. Where feasible, you could also reconfirm a user's understanding whenever there is a request that their data is shared or disclosed to a third-party, including a relying party, so long as this does not conflict with any requirements in sections 12.4. and 12.5. As outlined above, in section 12.7.1., this is a separate process to any legislative requirements to recontact data subjects which may be relevant.

12.7.4.d. You must take third-party services throughout your supply chain into account when confirming a user's understanding.

12.7.5. Prohibited processing of personal data

12.7.5.a. In addition to legislative requirements in respect of the processing of personal data, you must not collect and process identity or attribute data to:

- 'profile' users for third-party marketing purposes; or
- create aggregate data sets that could reveal sensitive information about users. You may create aggregate data sets where appropriate anonymisation techniques have been used and you are confident sensitive information will not be revealed about users, or that the user could be re-identified. The ICO has developed guidance on anonymisation that could be helpful to refer to.

12.7.5.b. Your service must not collect, share or otherwise process identity or attribute data without having confirmed the user's understanding of how their identity and attribute data will be shared and disclosed.

12.8. Using biometrics in your service

12.8.a. Biometric data used for identification purposes is special category data. You must comply with the requirements of data protection legislation in respect of processing biometric data. This includes completing a Data Protection Impact Assessment as described in section 12.7.e. It may be helpful to review the ICO guidance on biometric recognition.

12.8.b. For GPG 45 confidence profiles up to medium, if your service offers a non-biometric check as well as a biometric check, you must offer the non-biometric alternative to users at the same time that the biometric option is offered.

12.8.1. Performance and security of biometric solutions

12.8.1.a. Any biometric technology you use must have been developed and tested to be inclusive and accessible. You must specifically be able to demonstrate in a biometric testing report that you have considered whether:

- the number of ‘false matches’ and ‘false non-matches’ in your system are appropriate for your security and usability needs;
- the attack presentation classification error rate (APCER), and bona fide presentation attack classification error rate (BPCER) in your system are appropriate for your needs; and
- the performance of any biometric technology you use is consistent across demographics.

12.8.1.b. You must also follow industry standards that cover performance, presentation attack detection, and security testing and bias reduction, such as ISO/IEC 19795 and ISO/IEC 30107. If you do not follow these standards, you must demonstrate that you have processes to achieve the same outcomes.

12.8.2. Testing

12.8.2.a. There are two types of biometric tests that you must perform if you are using a biometric system in your service:

- performance testing – how well a system performs in terms of matching a person to their reference template, for example the photo in their passport; and
- security testing – how susceptible a system is to attacks, for example presentation attacks, injection attacks and cyber attacks.

12.8.2.b. Biometric testing can be delivered in the following ways:

- external independent testing delivered by an ISO/IEC 17025 accredited biometric test laboratory; or
- internal testing delivered within your organisation. This must follow a recognised testing methodology that meets international standards.

12.8.2.c. Biometric testing reports must include information about the specific test environment evaluated. They must also make clear how the test environment relates to your service. For example, test reports relating to a building entry system are not suitable evidence for a remote onboarding system on a mobile device.

12.8.3. Transparency

12.8.3.a. You must explain the performance and security of biometric technologies you use to relying parties, to other services you work with and to your users. This information must be easily accessible and include details of how testing was carried out.

12.8.3.b. When capturing biometric data, you must explain to users what will happen to that data. This includes whether the data is being used for a face match or checked against multiple records, how long the data will be retained, where it is stored and whether it will be used as training data for artificial neural networks. This information must be communicated in easily accessible language.

12.9. Working with relying parties

12.9.a. Relying parties do not need to be certified against the trust framework in order to adopt digital identities. However, it is vital that their practices do not undermine the principles of the trust framework.

12.9.b. Where you work directly with a relying party, you must set out flow down terms through your contractual arrangements. These flow down terms seek to ensure relying parties support providers in meeting their certification obligations.

Figure 4

12.9.c. There is flexibility in how you agree and implement these responsibilities with relying parties. But the terms must ensure the relying party understands its responsibilities that flow down from its contract with you, as well as confirm the boundaries for liability between you and the relying party. You must evidence terms specifically confirming the role of the relying party in supporting:

- fraud management requirements;
- information security requirements;
- data retention requirements;
- personal data processing requirements;
- data minimisation requirements, including avoiding excessive processing;
- data accuracy and repair requirements;
- identity repair and recourse requirements;
- the resolution of incidents and complaints; and
- holder service provider requirements for the reverification of identities and/or attributes (where applicable).

Illustrative example 10
Victoria is shopping in a clothes shop and decides to create a digital identity with the shop's chosen identity service provider so she can participate in a new digital shopping experience.

Victoria is unhappy with the experience of creating her digital identity and makes a complaint to the shop.

The provider and shop have agreed to work together to help customers with complaints. Given the topic of Victoria's complaint, the shop passes it to the identity service provider to ensure it is suitably resolved without needing Victoria to make a separate complaint with them directly.

13. The register of digital identity and attribute services

13.a. The register is a public, managed list of providers with services certified against the trust framework and any supplementary codes. It is maintained by OfDIA.

13.b. To apply to join the register, you must make an application by following the process that is set out on GOV.UK.

13.c. You must not misrepresent the registration status of your organisation or the services you offer, or allow others you work with to misrepresent their organisation or services through reliance on your registration. This does not preclude a third party from disclosing that a registered service forms part of their supply chain, particularly where the registered service is conducting specific activities in line with regulatory requirements.

13.d. The rules in the remainder of section 13. assume you are on the register.

13.1. Presence on the register

13.1.a. OfDIA will regularly carry out checks to maintain the integrity of the register. You must comply with these checks. You must have documented processes in place that demonstrate how you would respond and comply. These checks could include:

- certificate validation checks, including supplementary code certifications;
- security checks;
- requests for further information related to your presence on the register; or
- requests for applications to be resubmitted.

13.1.b. You can apply to amend your entry on the register. The process for applying for amendments will be set out in guidance on GOV.UK.

13.2. Withdrawal and removal from the register

13.2.a. You can apply to withdraw from the register. The process for applying for withdrawal will be set out in guidance on GOV.UK.

13.2.b. Your service will be removed from the register if the relevant certificate is suspended, revoked or expires and is not renewed before the certificate's expiry date. You will be notified in advance if OfDIA intends to take this action. It is your responsibility to ensure a certificate is renewed in good time to ensure your continued presence on the register.

13.2.c. If you only have one registered service and it is withdrawn or removed from the register, your entry as a registered provider will also be removed.

13.2.d. You must have a transition plan and policies in place in case you or your service are withdrawn or removed from the register. These must outline your commitment to:

- before applying for withdrawal, give your users and relying parties at least three weeks' notice that you plan to withdraw;
- on withdrawal or removal, immediately notify all users and relying parties when your service is no longer listed on the register;
- on withdrawal or removal, immediately cease all activities that promote yourself as a registered provider and/or your service as a registered service, including in promotional materials, communications, marketing and your website.

Part 4 - Additional information

14. Table of standards, guidance and legislation

This is a table of all standards, guidance and legislation referred to in the trust framework for ease of reference. Not all will be applicable to every trust framework participant and it is recommended that you read the relevant rules for your organisation in full.

STANDARD/GUIDANCE

Rules for identity service providers

STANDARD/GUIDANCE

Government guidance on how to prove and verify someone's identity

Rules for attribute service providers

Government guidance on how to create attributes

Government guidance on understanding attributes

Government guidance on how to score attributes

Rules for holder service providers

Government guidance on using authenticators to protect an online service

Government guidance on how to bind an attribute

Government guidance on how to prove and verify someone's identity

ICO guidance on qualified trust service providers (QTSPs)

Government guidance on delegated authority

Rules for component service providers

Government guidance on how to prove and verify someone's identity

STANDARD/GUIDANCE

Government guidance on using authenticators to protect an online service

Make sure your products and services are inclusive

Equality Act (2010)

Government guidance on how to accept a vouch as evidence of someone's identity

Government guidance on how to prove and verify someone's identity

Make sure your products and services are accessible

Government guidance on understanding the accessibility requirements for public sector bodies

Welsh Language Act (1993)

Welsh Language (Wales) Measure (2011)

Bilingual Technology Toolkit

W3C Web Content Accessibility Guidelines

EN 301 549 V3.2.1 (2021-03) - ETSI standard for accessibility requirements

Business probity

STANDARD/GUIDANCE

Government guidance on people with significant control (PSCs)

Money Laundering Regulations (2017)

Fraud Act (2006)

National Security and Investment Act (2021)

Staff and resources

ISO/IEC 27001 - Information security, cybersecurity and privacy protection – Information security management systems – Requirements

NCSC Cyber Assessment Framework (CAF)

NIST Cybersecurity Framework

BS 7858:2019 - Screening of individuals working in a secure environment. Code of practice

Service and quality management

ISO 9001 - Quality management systems – Requirements

ISO/IEC 20000 - Information technology – Service management

Information Technology Infrastructure Library® (ITIL)

STANDARD/GUIDANCE

Six Sigma™ methodology

Information management

ISO/IEC 27001 - Information security, cybersecurity and privacy protection – Information security management systems – Requirements

Information security

ISO/IEC 27001 - Information security, cybersecurity and privacy protection – Information security management systems – Requirements

ISO/IEC 27701 - Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guideline

NCSC guidance on building and operating a secure online service

Cyber Essentials and Cyber Essentials Plus

NCSC Cyber Assessment Framework (CAF)

NCSC guidance on Secure Design Principles

Risk management

ISO/IEC 27005 - Information technology – Security techniques – Information security risk management

STANDARD/GUIDANCE

ISO 31000 - Risk management

NCSC guidance on phishing attacks

NCSC guidance on cyber security-related risk management

Keeping records

ICO guidance on Article 30 of the UK GDPR

ICO guidance on retention policies

Freedom of Information Act (2000)

Freedom of Information (Scotland) Act (2002)

ICO guidance on freedom of information requests

Making your products and services interoperable with others

The trust framework data schema

OpenID Connect

W3C Verifiable Credentials

STANDARD/GUIDANCE

Checking if a user can act on behalf of an organisation or another person

Government guidance on delegated authority guidance

Encryption and cryptography

NCSC guidance on using TLS to protect data

NCSC guidance on using IPsec to protect data

NIST SP 800-213A: Data Protection – Secure Transmission

NIST SP 800-213A: Device Security – Secure Communication

NIST FIPS 140-2 - Security Requirements for Cryptographic Modules

NIST FIPS 140-3 - Security Requirements for Cryptographic Modules

SP 800-175B - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

ETSI TS 103 458 - Application of Attribute Based Encryption (ABE) for PII and personal data protection on Internet of Things (IoT) devices, WLAN, cloud and mobile services

ISO/IEC 18033 - Information security – Encryption algorithms

ISO/IEC 9797-2 – Information security — Message authentication codes (MACs)

STANDARD/GUIDANCE

ISO/IEC 9797-3 – Information technology — Security techniques — Message Authentication Codes (MACs)

ISO/IEC 10118 – Information technology — Security techniques — Hash-functions

NIST FIPS 180-4 - Secure Hash Standard (SHS)

NIST FIPS 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

NIST SP 800-107 - Recommendation for Applications Using Approved Hash Algorithms

ISO/IEC 11770 – Information technology — Security techniques — Key management

ISO/IEC 18031 – Information technology — Security techniques — Random bit generation

ISO/IEC 18032 – Information security — Prime number generation

ISO/IEC 9798-1:2010 – Information technology — Security techniques — Entity authentication

NIST FIPS 186-5 - Digital Signature Standard (DSS)

ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

ISO/IEC 9796 - Information technology — Security techniques — Digital signature schemes giving message recovery

ISO/IEC 14888 - IT Security techniques. Digital signatures with appendix

STANDARD/GUIDANCE

ISO/IEC 18370 - Information technology — Security techniques — Blind digital signatures

ISO/IEC 20008 - Information technology — Security techniques — Anonymous digital signatures

ISO/IEC 13888 – Information security – Non-repudiation

Fraud management

Guidance from the Chartered Institute of Public Finance and Accountancy (CIPFA)

Government Functional Standard GovS 013: Counter fraud

Government Functional Standard GovS 009: Internal Audit

Guidance from the Association of Certified Fraud Examiners (ACFE)

Guidance from the Chartered Institute of Management Accountants

NCSC guidance on transaction monitoring for online services

Open and/or common standards to share threat indicators - STIX and TAXII

Responding to incidents

NCSC guidance on incident management

STANDARD/GUIDANCE

NCSC guidance on best practice on logging and monitoring

Information Technology Infrastructure Library (ITIL)®

ICO guidance on how to respond to data breaches

Government guidance on using authenticators to protect an online service

Government guidance on how to prove and verify someone's identity

Action Fraud identity fraud victims' checklist

Privacy and data protection rules

ICO guidance on Data Protection

ICO guide to lawful basis

Data Protection Act (2018)

ICO guidance on Data Protection Officers

UK GDPR

ICO guidance on data controllers and processors

STANDARD/GUIDANCE

Data Protection Impact Assessment (DPIA)

Exemptions from ICO data protection fee

ICO guidance on data minimisation

ICO guidance on data accuracy

ICO guidance on storage limitation

ICO guidance on the right of access

ICO guidance on the right to rectification

ICO guidance on the right to data portability

ICO guidance on the right to erasure

ICO Age Appropriate Design Code

ICO guidance on children's information

ICO guidance on automated decision-making

ICO guidance on special category data

STANDARD/GUIDANCE

ICO guidance on the principle of transparency

ICO guidance on data protection by design and default

ISO/IEC 27701 - Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

ICO guidance on anonymisation

Using biometrics in your service

ICO guidance on special category data

ICO guidance on biometric recognition

ISO/IEC 19795 describes biometrics performance testing and reporting

ISO/IEC 19795-1 - Information technology – Biometric performance testing and reporting – Part 1: Principles and framework

ISO/IEC 19795-2 - Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation

ISO/IEC TR 19795-3 - Information technology – Biometric performance testing and reporting – Part 3: Modality-specific testing. This is a technical report.

ISO/IEC 19795-4 - Information technology – Biometric performance testing and reporting – Part 4: Interoperability performance testing

STANDARD/GUIDANCE

ISO/IEC 19795-5 - Information technology – Biometric performance testing and reporting – Part 5: Access control scenario and grading scheme

ISO/IEC 19795-6 - Information technology – Biometric performance testing and reporting – Part 6: Testing methodologies for operational evaluation

ISO/IEC 19795-7 - Information technology – Biometric performance testing and reporting – Part 7: Testing of on-card biometric comparison algorithms

ISO/IEC TS 19795-9 - Information technology – Biometric performance testing and reporting – Part 9: Testing on mobile devices

ISO/IEC 30107 describes the recommended approach to Presentation Attack Detection

ISO/IEC 30107-1 - Information technology – Biometric presentation attack detection – Part 1: Framework

ISO/IEC 30107-2 - Information technology – Biometric presentation attack detection – Part 2: Data formats

ISO/IEC 30107-3 - Information technology – Biometric presentation attack detection – Part 3: Testing and reporting

ISO/IEC 30107-4 - Information technology – Biometric presentation attack detection – Part 4: Profile for testing of mobile devices

FIDO Document Authenticity Requirements and Test Procedures for Document Authenticity Verification

15. Glossary of terms and definitions

Term	Definition
Accreditation	The independent, third-party evaluation of a conformity assessment body against recognised standards, conveying formal demonstration of its impartiality and competence to carry out specific conformity assessment tasks.
Anonymisation	Rendering personal data in such a way that individuals are not, or no longer are, identifiable.
Attribute	A piece of information that describes something about a person or an organisation. A combination of attributes can be used to create a digital identity.
Attribute service provider	An organisation providing a service that collects, creates, checks or shares pieces of information that describe something about a user.
Audit	The independent verification activity, such as inspection or examination of a product, process or service to ensure compliance to requirements.
Authenticator	Something that users can use to access a service. It could be some information (like a password), a piece of software or a device.
Biometric information	Measurements of a biological or behavioural attribute, like an iris or fingerprint
Certification	Represents a written assurance by an independent third-party, accredited by the UK Accreditation Service (UKAS), of the conformity of a product, process or service to specified requirements.
Certified service	A digital verification service that has been certified against the trust framework.

Component service provider	An organisation providing a service that specialises in designing and building components that can be used during part(s) of the identity proofing, verification or authentication processes.
Compromised account	An account has been compromised if a threat actor has accessed it to perform actions using a genuine user's credentials. This could happen because someone has been a victim of coercion, social engineering, phishing or other cyber attacks.
Conformity assessment body (CAB)	A body accredited by the UK Accreditation Service (UKAS) to certify a product, process or service to specified requirements. Approved trust framework conformity assessment bodies are accredited to undertake certification against the trust framework in keeping with ISO/IEC 17065.
Contra-indicators	A way of categorising any wrong or contradictory information that you might get from, or about, users.
Cryptographic	A way to guarantee the integrity and confidentiality of data transmitted over a public network. This is done by a combination of encryption and signing.
Data minimisation	Processing the minimum amount of personal data needed to deliver an individual element of a service.
Data protection legislation	The Data Protection Act (2018) and the UK General Data Protection Regulation (UK GDPR).
Data schema	Provides guidance for certified services and relying parties on how to organise and exchange information in a consistent way to enable interoperability. It describes the outcomes of different identity verification processes outlined in GPG 45 in a machine-readable format.
Delegated authority	When a user is authorised to act on behalf of someone else.
Digital identity	A digital representation of who a user is. It lets them prove who they are during interactions and transactions. They can use it online or in person.

Digital verification service (DVS)	Services that enable people to digitally prove who they are, information about themselves or their eligibility to do something.
Digital wallet	An electronic device, online service or software program that allows one party to make electronic transactions with another party for goods and services.
Electronic signature	Data in electronic form which is attached to or logically associated with data in electronic form which is used by the signatory to sign.
Encryption	A mathematical function that encodes data in such a way that only authorised users can access it.
False match	When a user is matched by a biometric system to the record of someone who is not them.
False non-match	When a biometric system fails to match a user to their own record.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic.
Hash function	When data is converted into a fixed-length value. A hash cannot be reversed to reveal the original data.
Holder service account	A user interface that allows a user to consistently access, manage and protect information held in their holder service. It also allows a provider to directly support and remotely manage a user's holder service.
Holder service provider	An organisation that creates a user-facing device, service, software or app that allows a user to collect, store, view, manage or share their identity and/or attribute information.
Identifier	A piece of information that can be used to make a connection between an attribute and a person or organisation.

Identity repair	A process that makes it possible for a user to use their rightful identity after experiencing identity theft.
Identity service provider	An organisation providing a service that proves and verifies a user's identity for one-off use at a single point in time. It can do this using online or offline channels, or a combination of both.
Industry standards	Relevant established standards from organisations including but not limited to ISO/IEC, ITU, ETSI, ENISA, ANSI, NIST, BSI.
Internet Protocol (IP) address	A numerical label assigned to any device connected to a computer network that uses Internet Protocol.
Intrusion detection system	Software that automatically looks for possible incidents during events in a computer system or network.
The register of digital identity and attribute services	A public, managed list of providers with services certified against the trust framework that is maintained by OfDIA.
Metadata	Data that provides information about other data.
Orchestration service provider	An organisation providing a service that makes sure data can be securely shared between participants in the trust framework through the provision of their technology infrastructure.
Participant	A collective term to refer to all organisations that interact with the trust framework and participate in the wider digital identity and attributes market. This includes certified services and relying parties.
Personal data	Any information relating to an identified or identifiable natural person
Personal data store	Service which lets an individual store, manage and deploy their key personal data in a highly secure and structured way.

Phishing	An attempt to trick users into submitting personal information by asking them to click on links within for example scam emails or text messages.
Provider	An organisation that offers digital verification services. Where a provider has had their service certified against the trust framework, we refer to it as a 'certified service'.
Pseudonymisation	A security technique that replaces or removes information in a data set that identifies an individual. It does not change the status of the data as personal data (ICO Guidance).
Qualified trust service	A service offered by a qualified trust service provider that meets the rules in the UK electronic identification and trust services for electronic transactions (eIDAS) regulation (assimilated direct legislation).
Relying party	An organisation that relies on (or 'consumes') certified products or services.
Relying party flow down terms	Terms included in contractual arrangements between certified services and relying parties.
Shared signals	When intelligence is shared across the trust framework to reduce the impact of fraud on its participants and users.
Supplementary code	A set of additional rules that providers can certify against, alongside the trust framework's rules, to demonstrate that they meet the requirements of a particular sector or use case.
Trust framework	A set of government-approved rules, which draws mainly on existing standards, guidance, best practice and legislation, that organisations agree to follow to have their service certified as a trustworthy digital verification service.
UK Accreditation Service (UKAS)	The national accreditation body for the UK. They are appointed by the Government to assess and accredit organisations that provide certification services.

The UK digital identity trust mark	A unique visual mark that signals to users and relying parties that a service is certified against the trust framework and listed on the register of digital identity and attribute services.
Unique identifier	Unique data used to represent someone’s identity and associated attributes.
User	A person who uses digital verification services.