Identity Assurance Principles

Privacy and Consumer Advisory Group (PCAG)
V3.1 (for publication)

Contents

1. Introduction

1.1 These Principles have been developed to support an Identity Assurance Service that allows individual users to control when to reveal their own identifying information. This focus on individual control and consent is far removed from old-fashioned notions of imposing central identity solutions and databases, supported by mandatory disclosure and compulsion. The intention is instead to bring about a secure Identity Assurance Service that is attractive to citizens and allows them to control a number of identity credentials, chosen by them, which can be voluntarily used with different online Service Providers.

1.2 Public trust in an Identity Assurance Service will enable various benefits to follow: Service Providers will be less worried about identity fraud and impersonation since claims based on the use of fraudulent identities become nearly impossible. At the same time, the individuals are reassured that their identity is secure and any transaction is safely delivered to the right destination. This is a collaborative win-win outcome for both the individual and the government: everybody benefits.

1.3 To deliver these objectives there has to be a framework that gives real meaning to terms such as "individual privacy" and "individual control". Such a framework is set out in the nine Identity Assurance Principles contained in this document: these Principles have been developed by the independent Privacy and Consumer Advisory Group (PCAG), including open public consultation on earlier working drafts.

1.4 These Principles are designed around the needs of the individual – and not on the needs of any state body or commercial corporation. In order to demonstrate that these Principles serve the interest of the individual, below are one-sentence summaries, expressed in the first person, which define the intended effect of each Principle.

Identity Assurance Principle	**Summary of the control afforded to an individual**
User Control	I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them
Transparency	Identity assurance can only take place in ways I understand and when I am fully informed
Multiplicity	I can use and choose as many different identifiers or identity providers as I want to
Data Minimisation	My interactions only use the minimum data necessary to meet my needs
Data Quality	I choose when to update my records
Service User Access and Portability	I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want
Certification	I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements
Dispute Resolution	If I have a dispute, I can go to an independent Third Party for a resolution
Exceptional Circumstances	I know that any exception has to be approved by Parliament and is subject to independent scrutiny

2. The Context of the Principles

2.1 These Principles have been produced by the Privacy and Consumer Advisory Group, but are not devoted solely to privacy, data protection or consumer issues. These Principles apply to the operation of a user-centric, Identity Assurance Service that places the individual Service User (i.e. the person who has registered the identity, or someone authorised to act on their behalf) in control of when and how they assert their identity.

2.2 The Principles are equal to each other and do not overlap. Each Principle has a specific role and, in combination, they are all necessary to engender trust in the Identity Assurance Service.

2.3 These Principles are limited in their application to the processing of data in an Identity Assurance Service (e.g. establishing and verifying identity of a Service User; conducting a transaction that uses an identity; maintaining audit requirements in relation to a transaction associated with the use of a service that needs identity verification etc.). They do not apply to other data (e.g. data that are used to deliver a service, or to measure its quality).

2.4 The nine Principles assume that an Identity Assurance Service is mature and well established. We acknowledge however that in the early stages of its development there may well be a phasing-in period in relation to each Principle, or that in some cases a Principle might need a degree of initial flexibility. However, we believe that within a reasonable time frame, all of these Principles should be fully implemented by the Identity Assurance Service.

2.5 We recognise that special interests (e.g. law enforcement) may need exemptions and this is the purpose of the ninth Principle. Such special interests should be subject to a simple rule: exemptions have to be explicitly defined and publicly reported. The Group recommends that this should ideally be enabled through legislation to establish the Identity Assurance Service infrastructure coupled with robust contractual terms that enforce all of the Principles. We do not think it advisable to allow existing legislation to define access to any data from the Identity Assurance Service since such legislation, when it was originally enacted, could not have been scrutinised in the context of an Identity Assurance Service. Any exemption from these Principles needs public scrutiny in order to gain credibility and maintain trust. However, in the absence of specific legislation establishing the Identity Assurance Service, it is essential that other mechanisms be implemented to ensure transparency, scrutiny and, where necessary, debate. As these Principles only apply to Identity Assurance Data used by the Identity Assurance Service, they have no impact on any operational matter of any law enforcement agency, except where the operational matter relates to obtaining such data from an Identity Assurance Service. In such cases, the Exceptional Circumstances Principle will apply.

2.6 The wording of each Principle has been carefully chosen to balance any competing claims. They have been widely debated within the Privacy and Consumer Advisory Group and through the associated open consultation process, so we request that any changes to the text of any Principle be supported by the detail of any problem that has been encountered. We intend to review the Principles at least annually in the light of experience and any comments received.

2.7 Where appropriate, we expect that the application of these Identity Assurance Principles will be described:

- in public documents that explain the operation of the Identity Assurance Service
- in presentations about the Identity Assurance Service
- in procurement processes, technical design and associated procedures of the Identity Assurance Service

2.8 The Principles are limited to their application to the Identity Assurance Service in the UK, with a particular emphasis on the UK Government's objective to deliver public services electronically. We note, however, that these Principles could have international reach, especially in the USA, or in the European Union, OECD and APEC countries. However, our starting assumption has been that such interchangeability with any other nationally-based Principles will only become relevant when the UK Principles have established a proven track record in gaining the confidence of individuals who use a Service. However, we believe that these Principles are fully consistent with all national and international data protection requirements and the obligations arising from the UK's common law of confidence.

2.9 The Principles are drafted in a way that allows for a degree of precision. They are not drafted in a way that defines statutory Principles, but the text could form the basis of a Statutory Code of Practice, similar, for example to the model provided by the Statutory Code of Practice on Data Sharing. A Statutory Code of Practice would cover all types of organisation, of any size and in any usage context, which might wish to provide or consume any services from the Identity Assurance Service.

2.10 These Principles represent good practice guidance and the requirements of other legal duties under human rights and data protection legislation and the common law. The Principles apply to all identity assurance activities described in "Good Practice Guide (GPG) 43 – Requirements for Secure Delivery of Online Public Services". The architecture of the Identity Assurance Service must be based on open standards.

3. Definitions

3.1 These Principles are limited to the processing of Identity Assurance Data (IdA Data) in an Identity Assurance Service (e.g. establishing and verifying identity of a Service User; conducting a transaction that uses a user identity; maintaining audit requirements in relation a transaction associated with the use of a service that needs identity verification etc.). They do not cover, for example, any data used to deliver a service, or to measure its quality (see para 2.3).

3.2 In the context of the application of the Identity Assurance Principles to an Identity Assurance Service, "Identity Assurance Data" (IdA Data) means any recorded information that is connected with a "Service User" including:

- **"Audit Data".** This includes any recorded information that is connected with any log or audit associated with an Identity Assurance Service
- **"General Data".** This means any other recorded information which is not personal data, audit data or relationship data, but is still connected with a "Service User"
- **"Personal Data".** This takes its meaning from the Data Protection Act or subsequent legislation (e.g. any recorded information that relates to a "Service User" who is also an identifiable living individual)
- **"Relationship Data".** This means any recorded information that describes (or infers) a relationship between a "Service User", "Identity Provider" or "Service Provider" with another "Service User", "Identity Provider" or "Service Provider" and includes any cookie or program whose purpose is to supply a means through which relationship data are collected

3.3 Other terms used in the Principles are defined as follows:

- **"Identity Assurance Service".** This includes relevant applications of the technology (e.g. hardware, software, database, documentation) in the possession or control of any "Service User", "Identity Provider" or "Service Provider" that is used to facilitate identity assurance activities; it also includes any IdA Data processed by that technology or by an Identity Provider or by a Service Provider in the context of the Service; and any IdA Data processed by the underlying infrastructure for the purpose of delivering the IdA service or associated billing, management, audit and fraud prevention
- **"Identity Provider".** This means the certified individual or certified organisation that provides an Identity Assurance Service (e.g. establishing an identity, verification of identity); it includes any agent of a certified Identity Provider that processes IdA data in connection with that Identity Assurance Service
- **"Participant".** This means any "Identity Provider", "Service Provider" or "Service User" in an Identity Assurance Service. A "Participant" includes any agent by definition
- **"Processing".** In the context of IdA data means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, correlating, aggregating, accessing" the data and includes any other operation performed on IdA data
- **"Provider".** Includes both "Identity Provider" and/or "Service Provider"

- **"Service Provider".** This means the certified individual or certified organisation that provides a service that uses an Identity Provider in order to verify identity of the Service User; it includes any agent of the Service Provider that processes IdA data from an Identity Assurance Service
- **"Service User".** This means the person (i.e. an organisation (incorporated or not) or an individual (dead or alive) who has established (or is establishing) an identity with an Identity Provider; it includes an agent (e.g. a solicitor, family member) who acts on behalf of a Service User with proper authority (e.g. a public guardian, or a Director of a company, or someone who possesses power of attorney). The person may be living or deceased (the identity may still need to be used once its owner is dead, for example by an executor)
- **"Third Party".** This means any person (i.e. any organisation or individual) who is not a "Participant" (e.g. the police or a Regulator). Note: we think it helpful to create a link to the language from the National Strategy for Trusted Identities in Cyberspace (NSTIC) which defines participants as "the collective subjects, identity providers, attribute providers, relying parties, and identity media taking part in a given transaction". This way, Third Parties are not Participants

4. The Nine Identity Assurance Principles

Any exemptions from these Principles must be specified via the "Exceptional Circumstances Principle."

4.1 User Control
"I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."

4.1.1 An Identity Provider or Service Provider must ensure any collection, use or disclosure of IdA data in, or from, an Identity Assurance Service is approved by each particular Service User who is connected with the IdA data.

4.1.2 There should be no compulsion to use the Identity Assurance Service and Service Providers should offer alternative mechanisms to access their services. Failing to do so would undermine the consensual nature of the service.

4.2 Transparency
"Identity assurance can only take place in ways I understand and when I am fully informed."

4.2.1 Each Identity Provider or Service Provider must be able to justify to Service Users why their IdA data are processed. Ensuring transparency of activity and effective oversight through auditing and other activities inspires public trust and confidence in how their details are used.

4.2.2 Each Service User must be offered a clear description about the processing of IdA data in advance of any processing. Identity Providers must be transparent with users about their particular models for service provision.

4.2.3 The information provided includes a clear explanation of why any specific information has to be provided by the Service User (e.g. in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service User (e.g. in relation to the User's role in securing his/her own identity information).

4.2.4 The Service User will be able to identify which Service Provider they are using at any given time.

4.2.5 Any subsequent and significant change to the processing arrangements that have been previously described to a Service User requires the prior consent or approval of that Service User before it comes into effect.

4.2.6 All procedures, including those involved with security, should be should be made publicly available at the appropriate time, unless such transparency presents a security or privacy risk. For example, the standards of encryption can be identified without jeopardy to the encryption keys being used.

4.3 Multiplicity
"I can use and choose as many different identifiers or identity providers as I want to."

4.3.1 A Service User is free to use any number of identifiers that each uniquely identifies the individual or business concerned.

4.3.2 A Service User can use any of his identities established with an Identity Provider with any Service Provider.

4.3.3 A Service User shall not be obliged to use any Identity Provider or Service Provider not chosen by that Service User; however, a Service Provider can require the Service User to provide a specific level of Identity Assurance, appropriate to the Service User's request to a Service Provider.

4.3.4 A Service User can choose any number of Identity Providers and where possible can choose between Service Providers in order to meet his or her diverse needs. Where a Service User chooses to register with more than one Identity Provider, Identity Providers and Service Providers must not link the Service User's different accounts or gain information about their use of other Providers.

4.3.5 A Service User can terminate, suspend or change Identity Provider and where possible can choose between Service Providers at any time.

4.3.6 A Service Provider does not know the identity of the Identity Provider used by a Service User to verify an identity in relation to a specific service. The Service Provider knows that the Identity Provider can be trusted because the Identity Provider has been certified, as set out in GPG43 – Requirements for Secure Delivery of Online Public Services (RSDOPS).

4.4 Data Minimisation
"My interactions only use the minimum data necessary to meet my needs."

4.4.1 Identity Assurance should only be used where a need has been established and only to the appropriate minimum level of assurance.

4.4.2 Identity Assurance data processed by an Identity Provider or a Service Provider to facilitate a request of a Service User must be the minimum necessary in order to fulfil that request in a secure and auditable manner.

4.4.3 When a Service User stops using a particular Identity Provider, their data should be deleted. Data should be retained only where required for specific targeted fraud, security or other criminal investigation purposes.

4.5 Data Quality
"I choose when to update my records."

4.5.1 Service Providers should enable Service Users (or authorised persons, such as the holder of a Power of Attorney) to be able to update their own personal data, at a time at their choosing, free of charge and in a simple and easy manner.

4.5.2 Identity Providers and Service Providers must take account of the appropriate level of identity assurance required before allowing any updating of personal data.

4.6 Service User Access and Portability
"I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want."

4.6.1 Each Identity Provider or Service Provider must allow, promptly, on request and free of charge, each Service User access to any IdA data that relates to that Service User.

4.6.2 It shall be unlawful to make it a condition of doing anything in relation to a Service User to request or require that Service User to request IdA data.

4.6.3 The Service User must be able to require an Identity Provider to transfer his personal data, to a second Identity Provider in a standard electronic format, free of charge and without impediment or delay.

4.7 Certification
"I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements."

4.7.1 As a baseline control, all Identity Providers and Service Providers will be certified against a shared standard. This is one important way of building trust and confidence in the service.

4.7.2 As part of the certification process, Identity Providers and Service Providers are obliged to co-operate with the independent Third Party and accept their impartial determination and to ensure that contractual arrangements:

- reinforce the application of the Identity Assurance Principles
- contain a reference to the independent Third Party as a mechanism for dispute resolution

4.7.3 There will be a certification procedure subject to an effective independent audit regime that ensures all relevant, recognised identity assurance and technical standards, data protection or other legal requirements, are maintained by Identity Providers and Service Providers.

4.7.4 In the context of personal data, certification procedures include the use of Privacy Impact Assessments, Security Risk Assessments, Privacy by Design concepts and, in the context of information security, a commitment to using appropriate technical measures (e.g. encryption) and ever improving security management. Wherever possible, such certification processes and security procedures reliant on technical devices should be made publicly available at the appropriate time.

4.7.5 All Identity Providers and Service Providers will take all reasonable steps to ensure that a Third Party cannot capture IdA data that confirms (or infers) the existence of relationship between any Participant. No relationships between parties or records should be established without the consent of the Service User.

4.7.6 Certification can be revoked if there is significant non-compliance with any Identity Assurance Principle.

4.8 Dispute Resolution
"If I have a dispute, I can go to an independent Third Party for a resolution."

4.8.1 A Service User who, after a reasonable time, cannot, or is unable, to resolve a complaint or problem directly with an Identity Provider or Service Provider can call upon an independent Third Party to seek resolution of the issue. This could happen for example where there is a disagreement between the Service User and the Identity Provider about the accuracy of data.

4.8.2 The independent Third Party can resolve the same or similar complaints affecting a group of Service Users.

4.8.3 The independent Third Party can co-operate with other regulators in order to resolve problems and can raise relevant issues of importance concerning the Identity Assurance Service.

4.8.4 An adjudication/recommendation of the independent Third Party should be published. The independent Third Party must operate transparently, but detailed case histories should only be published subject to appropriate review and consent.

4.8.5 There can be more than one independent Third Party.

4.8.6 The independent Third Party can recommend changes to standards or certification procedures or that an Identity Provider or Service Provider should lose their certification.

4.9 Exceptional Circumstances
"Any exception has to be approved by Parliament and is subject to independent scrutiny."

4.9.1 Any exemption from the application of any of the above Principles to IdA data shall only be lawful if it is linked to a statutory framework that legitimises all Identity Assurance Services, or an Identity Assurance Service in the context of a specific service. In the absence of such a legal framework then alternative measures must be taken to ensure, transparency, scrutiny and accountability for any exceptions.

4.9.2 Any exemption from the application of any of the above Principles that relates to the processing of personal data must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.

4.9.3 Any subsequent processing of personal data by any Third Party who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance.

4.9.4 Any exceptional circumstance involving the processing of personal data must be subject to a Privacy Impact Assessment by all relevant “data controllers” (where “data controller” takes its meaning from the Data Protection Act).

4.9.5 Any exemption from the application of any of the above Principles in relation to IdA data shall remain subject to the Dispute Resolution Principle.