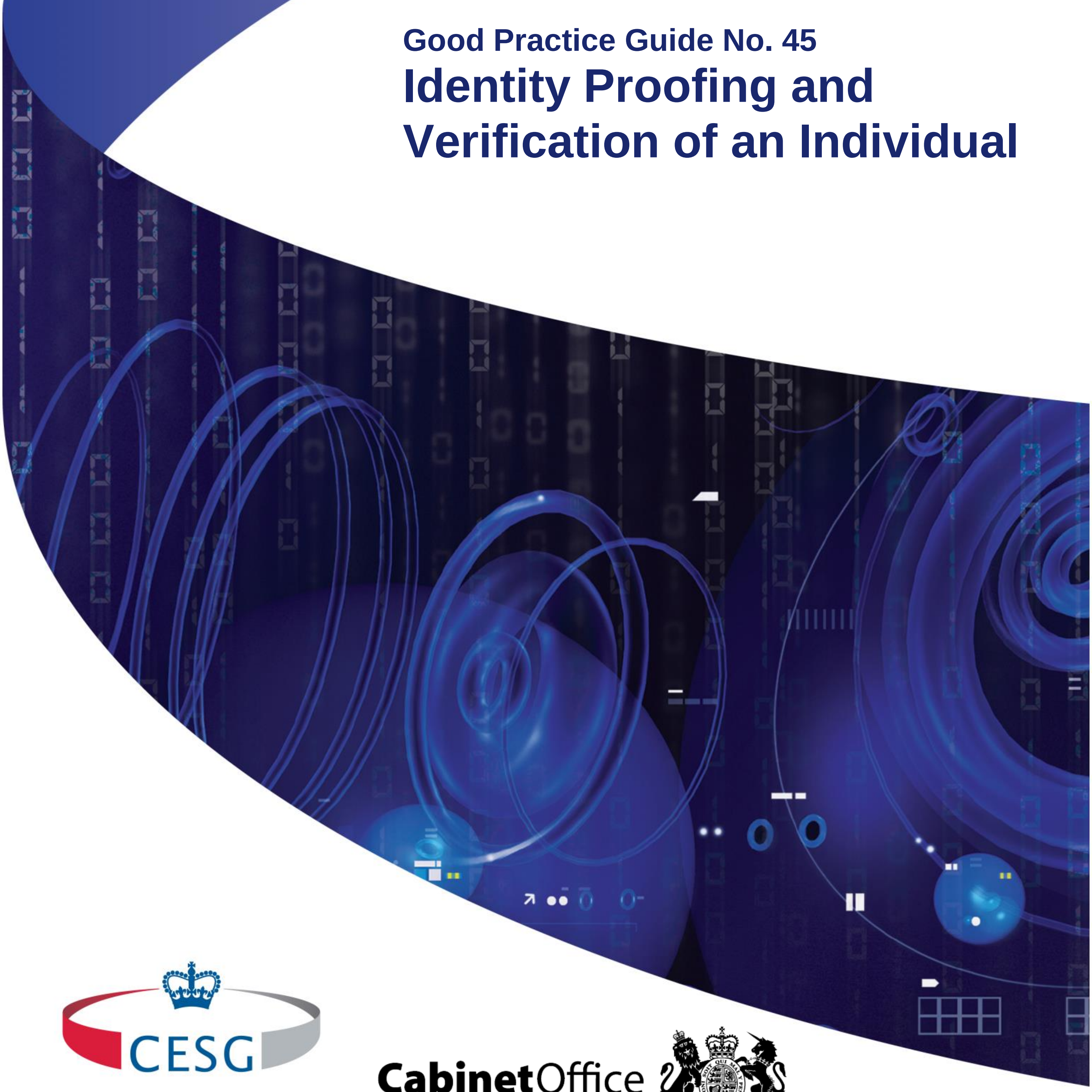
October 2015
Issue No: 2.4

Good Practice Guide No. 45

Identity Proofing and Verification of an Individual



CESG
NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

CabinetOffice

Good Practice Guide No. 45

Identity Proofing and Verification of an Individual

Issue No: 2.4
October 2015

This document is issued jointly by CESG, the UK's National Technical Authority on Information Assurance and Cabinet Office, Government Digital Service. It is provided "as is" as an example of how specific requirements could be met, but it is not intended to be exhaustive, does not act as endorsement of any particular product or technology and is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take the appropriate technical and legal advice in using this document (and others accessed from the GCHQ/CESG website).

Document History

Version	Date	Comment
1.0	April 2012	First issue
1.1	January 2013	Updated in accordance with IDAP schedule
2.0	May 2013	Second issue
2.1	September 2013	Included changes as a result of lessons learned. Not published
2.2	December 2013	Updated post 2.1 review, version number updated to align with IDAP operations manual
2.3	July 2014	Updated post 2.2 review
2.4	October 2015	First public release

Purpose & Intended Readership

This document should be read by organisations that are responsible for identity proofing an individual where any HMG Department or service will be relying on that identity. This includes those responsible for the procurement, assessment or delivery of an Identity Assurance (IdA) service.

Executive Summary

Within the UK there is no official or statutory attribute or set of attributes that are used to uniquely identify individuals across Government. Neither is there a single official or statutory issued document whose primary purpose is that of identifying an individual.

Without such attributes or documentation it is difficult for any person to be absolutely certain of the identity of another. This document is designed to demonstrate how a combination of the breadth of evidence provided, the strength of the evidence itself, the validation and verification processes conducted and a history of activity can provide various levels of assurance around the legitimacy of an identity.

Feedback

CESG welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. Please email: enquiries@cesg.gsi.gov.uk

Contents

Chapter 1 - Introduction 3

Purpose..3
Desired Outcomes and Aims 3

Chapter 2 - Relationship to IPV standards 4

Relationship to IPV standards.........4

Chapter 3 - Overview of Identity Proofing...5

Chapter 4 - Levels of Identity Proofing Assurance 7

Level 1 Identity................................7
Level 2 Identity................................7
Level 3 Identity................................7
Level 4 Identity................................7

Chapter 5 - Identity Proofing and Verification (IPV) Elements..............8

Identity Proofing and Verification (IPV) Elements................................8
IPV Element A – Strength of Identity Evidence 8
IPV Element B – Outcome of the Validation of Identity Evidence 9
IPV Element C – Outcome of Identity Verification 11
IPV Element D – Outcome of Counter-Fraud Checks..................12
IPV Element E – Activity History of the Claimed Identity 12

Chapter 6 - Requirements for each Level of Identity 14

Requirements.............................. 14

Chapter 7 - Identity Proofing Definitions 17

Definitions 17

Annex A - Evidence Examples (IPV Element A) 20

Annex B - Validation (IPV Element B) 22

Determining whether Identity Evidence is Genuine 22
Checking if the Identity Evidence is Valid 22

Annex C - Verification (IPV Element C).. 23

Static Knowledge Based Verification (KBV) 23
Dynamic Knowledge Based Verification 23
Physical Comparison 24
Biometric Comparison.................. 25

Annex D - Counter-fraud Capabilities (IPV Element D)......... 26

Annex E - Example Activity Events (IPV Element E) 27

Reference 28

Chapter 1 - Introduction

Key Principles

- This document is intended to provide guidance on the Identity Proofing and Verification (IPV) of an individual
- This document is intended to state HMG IPV requirements and show how they can be interpreted in the context of International Standards
- This document is under regular review with the content and context made available for indicative purposes only

Purpose

1. The purpose of this document is to establish a common framework for establishing the requirement for identity proofing and verifying the identity of an individual.

2. This document will provide assurance guidance regarding the acceptability, validation and verification of identity evidence that may be presented by an individual to support their identity.

3. In addition this document will characterise the elements of validation and verification processes that should be carried out.

4. This Good Practice Guide (GPG) is not intended to provide guidance on how to implement Identity Proofing and Verification requirements.

Desired Outcomes and Aims

5. This document has a number of aims:

    - To provide organisations with an understanding of the capabilities they will need to be able to demonstrate in order to perform identity proofing
    - To provide information to independent assessment organisations so that benchmarks or profiles can be developed to support the independent assessment and certification of organisational and technical capabilities
    - To establish a common framework establishing requirements for the validation and verification of the identity of individuals

Chapter 2 - Relationship to IPV standards

Key Principles

- This document covers identity proofing and verification only and has been written to align with, but not directly correlate to other National and International standards and guidance
- The identity levels provided in this document are intended to fulfil the criteria for identity levels in other National and International standards and guidance

Relationship to IPV standards

6. This document has been written with the intention of achieving alignment to National and International standards describing levels of identity assurance, including CESG Good Practice Guide No. 43 (GPG 43), Requirements for Secure Delivery of Online Public Services (RSDOPS) (reference [a]). It provides an interpretation of these levels of assurance in the context of IPV for UK public sector for both citizen and internal system users.

7. This is not meant to imply that there is direct correlation between the Assured Identity Levels in this document and the levels in those standards but that it is seen that this document fulfils the criteria as demonstrated in those standards.

8. This document only covers the identity proofing and verification processes, therefore, it may only fulfil part of the requirements of these standards and further measures are required in order to wholly comply (e.g. issuing of a credential).

GPG 45	RSDOPS	STORK 2.0	29115:2011	ISO 29003	NIST 800-63
N/A	Level 0[1]	N/A	N/A	N/A	N/A
Level 1	Level 1	QAA Level 1	LoA 1	LoA 1	Level 1
Level 2	Level 2	QAA Level 2	LoA 2	LoA 2	Level 2
Level 3	Level 3	QAA Level 3	LoA 3	LoA 3	Level 3
Level 4	N/A[2]	QAA Level 4	LoA 4	LoA 4	Level 4

Table 1 - Relationship to IPV standards

[1] RSDOPS defines level 0 over 15 security components, there are no personal registration requirements at level 0 therefore identity proofing is not needed.

[2] RSDOPS is only concerned with delivery of online services, this limits its scope to identity levels 1, 2 and 3; a level 4 identity mandates that the person is physically present.

Chapter 3 - Overview of Identity Proofing

Key Principles

- The process should enable a legitimate individual to prove their identity in a straightforward manner whilst creating significant barriers to those trying to claim to be somebody they are not
- The individual shall expressly declare their identity
- The individual shall provide evidence to prove their identity[†]
- The evidence shall be confirmed as being Valid and/or Genuine and belonging to the individual[†]
- Checks against the identity confirm whether it exists in the real world[†]
- The breadth and depth of evidence and checking required shall differ depending on the level of assurance needed in that the identity is real and belongs to the individual[†]

Process

9. The Applicant shall be required to declare the name, date of birth and address that they wish to be known as so that there is no ambiguity about the identity that is going to be used (Claimed Identity).[†]

10. The Applicant shall be required to provide evidence that the Claimed Identity exists (Identity Evidence Package). This may be provided electronically or physically depending on the level of assurance required and the capabilities of the organisation that is going to proof the Applicant.[†]

11. The evidence provided shall be checked in order to determine whether it is Genuine and/or Valid (Validation).[†]

12. The Applicant shall be compared to the provided evidence and/or knowledge about the Claimed Identity to determine whether it relates to them (Verification).[†]

13. The Claimed Identity shall be subjected to checks to determine whether it has had an existence in the real world over a period of time (Activity History).[†]

14. The Claimed Identity shall be checked with various counter-fraud services to ensure that it is not a known fraudulent identity and to help protect individuals who have been victims of identity theft (Counter-Fraud Checks).[†]

15. At the end of the process there is an Assured Identity that describes the level of confidence that the Applicant is the owner of the Claimed Identity and that identity is genuine.

[†] Not applicable for Level 1 Identities

16. The identity proofing process does not need to be performed in the order outlined above, however the organisation performing the proofing shall ensure that all the steps are adequately completed.

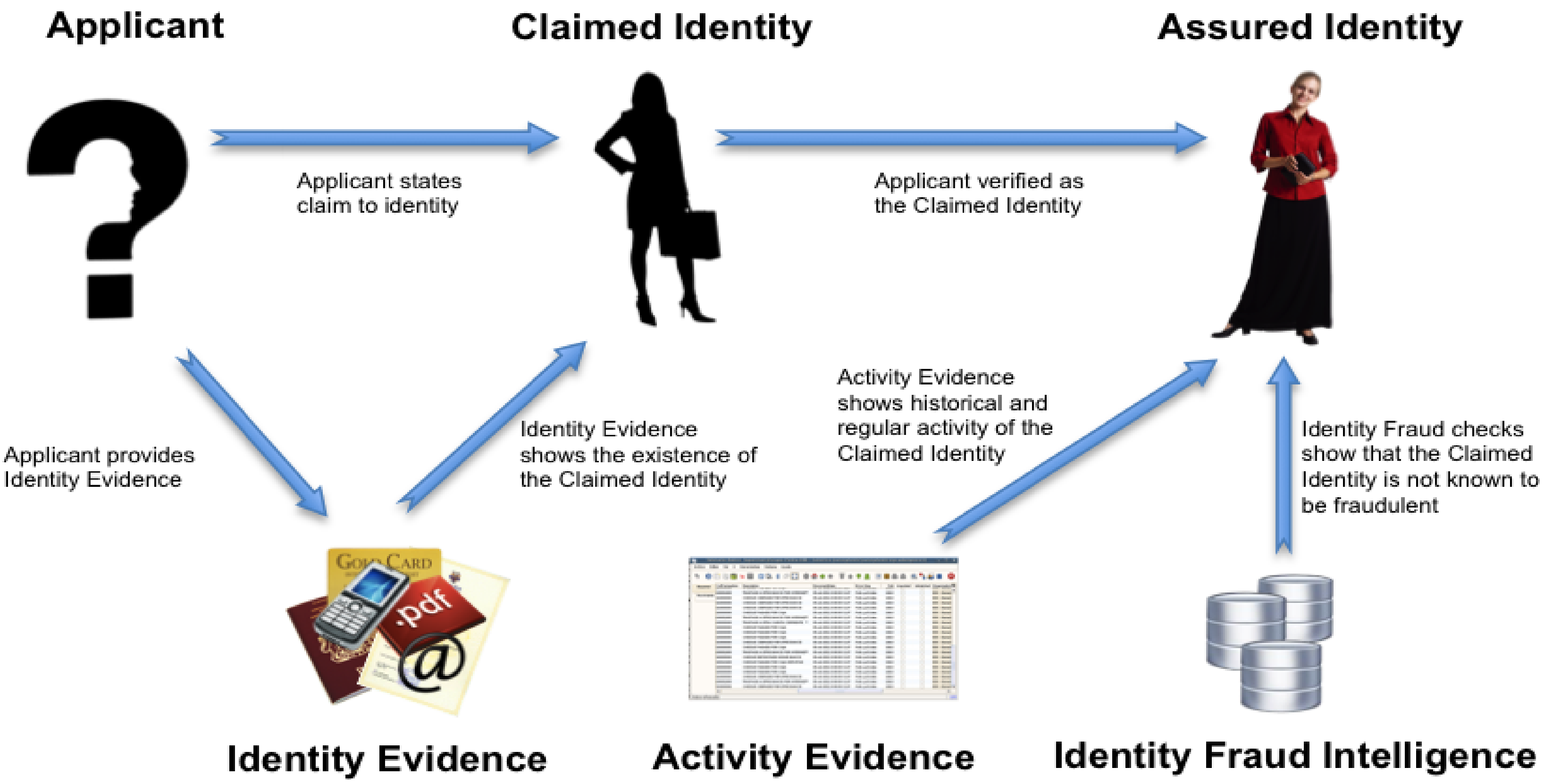

Applicant
Claimed Identity
Assured Identity
Applicant states claim to identity
Applicant verified as the Claimed Identity
Applicant provides Identity Evidence
Identity Evidence shows the existence of the Claimed Identity
Activity Evidence shows historical and regular activity of the Claimed Identity
Identity Fraud checks show that the Claimed Identity is not known to be fraudulent
GOLD CARD
.pdf
@
Identity Evidence
Activity Evidence
Identity Fraud Intelligence

Figure 1 - Overview of the Identity Proofing and Verification Process

Chapter 4 - Levels of Identity Proofing Assurance

Key Principles

- Four levels of identity proofing are provided, each of which provide an increasing level of confidence that the applicant’s claimed identity is their real identity
- There is no requirement to perform identity proofing when considering RSDOPS (GPG 43) (reference [a]) Level 0 for personal registration

Levels of Identity Proofing

17. This document has been written with the intention of achieving alignment to National and International standards describing levels of identity assurance, including RSDOPS, GPG 43, (reference [a]). For further information see Chapter 2; note that RSDOPS contains security controls at Level 0, however it has no personal registration requirements at Level 0 therefore identity proofing is not performed.

Level 1 Identity

18. At Level 1 there is no requirement for the identity of the Applicant to be proven. The Applicant has provided an Identifier that can be used to confirm an individual as the Applicant. The Identifier has been checked to ensure that it is in the possession and/or control of the Applicant.

Level 2 Identity

19. A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings.

Level 3 Identity

20. A Level 3 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of criminal proceedings.

Level 4 Identity

21. A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of Biometrics, to further protect the identity from impersonation or fabrication. This is intended for those persons who may be in a position of trust or situations where compromise could represent a danger to life.

Chapter 5 - Identity Proofing and Verification (IPV) Elements

Key Principle

- IPV elements are used to characterise and score the checks carried out against a claimed identity

Identity Proofing and Verification (IPV) Elements

22. There are 5 IPV elements that are described in the following sections.

IPV Element A – Strength of Identity Evidence

23. The purpose of this element is to record the strength of the Identity Evidence provided by the Applicant in support of the Claimed Identity. The following Table demonstrates the properties of the Identity Evidence and the corresponding score for this element. The Identity Evidence must, as a minimum, meet all the properties defined for a particular strength to achieve that score.

Score	Properties of the Identity Evidence
0	• No compliant Identity Evidence provided
1	• The issuing source of the Identity Evidence performed no identity checking • The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of an individual • The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates **OR** The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates
2	• The Issuing Source of the Identity Evidence confirmed the applicant's identity through an identity checking process • The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates • The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates **OR** The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates • Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed • Where the issued Identity Evidence is, or includes, a physical object it requires Proprietary Knowledge to be able to reproduce it
3	• The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007 • The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates • The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates • The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted • The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates **OR** The ownership of the issued Identity Evidence can be confirmed through Knowledge Based Verification

Score	Properties of the Identity Evidence
	• Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed • Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it
4	• The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007 • The Issuing Source visually identified the applicant and performed further checks to confirm the existence of that identity • The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates • The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates • The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted • The issued Identity Evidence contains a photograph/image of the person to whom it relates • The issued Identity Evidence contains a Biometric of the person to whom it relates • Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed • Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it

Table 2 - Strength of Identity Evidence

24. Examples of Identity Evidence are given in Annex A.

IPV Element B – Outcome of the Validation of Identity Evidence

25. The purpose of this element is to record the score obtained from the Identity Evidence Validation process. The following table demonstrates the characteristics of the Validation processes and the corresponding score for this element.

Score	Identity Evidence Validation
0	• Validation of the Identity Evidence was unsuccessful
1	• All Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source
2	• All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source **OR** • The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** • The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features

Score	Identity Evidence Validation
3	• The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features **AND** • All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source **OR** Evidence Details from the Identity Evidence have been confirmed as not known to be invalid by comparison with information held/published by the Issuing Source/Authoritative Source
4	• The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment including the integrity of any cryptographic security features **AND** • All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing Source/Authoritative Source

Table 3 - Outcome of the Validation of Identity Evidence

26. Guidance on determining if Identity Evidence is Valid or Genuine is in Annex B.

IPV Element C – Outcome of Identity Verification

27. The purpose of this element is to record the score obtained from the Identity Verification process. The following table demonstrates the outcomes of the Verification processes and the corresponding score for this element.

Score	Identity Verification Outcome
0	• Unable to confirm that the Applicant is the owner of the Claimed Identity
1	• The Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity
2	• The Applicant's ownership of the Claimed Identity has been confirmed by a Static Knowledge Based Verification **OR** • The Applicant's ownership of the Claimed Identity has been confirmed by a Dynamic Knowledge Based Verification **OR** • The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **OR** • The Applicant's ownership of the Claimed Identity has been confirmed by a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity
3	• The Applicant's ownership of the Claimed Identity has been confirmed by physical comparison using a photograph/image **OR** Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **AND** • The Applicant's ownership of the Claimed Identity has been confirmed by a Static **OR** Dynamic Knowledge Based Verification
4	• The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant using a photograph/image to the strongest pieces of Identity Evidence **OR** By a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **AND** • The Applicant's ownership of the Claimed Identity has been confirmed by both a Static **AND** Dynamic Knowledge Based Verification **AND** • The Applicant's ownership of the Claimed Identity has been confirmed by an interaction with the Applicant via the declared address

Table 4 - Outcome of Identity Verification

28. Further guidance on Static and Dynamic Knowledge Based Verification is contained in Annex C.

IPV Element D – Outcome of Counter-Fraud Checks

29. The purpose of this element is to record the score obtained from the Counter-Fraud Check process. The following Table demonstrates the outcomes and the corresponding score once any investigation activity has been carried out for this element.

Score	Counter-Fraud Checks
0	• Applicant is suspected of being, or known to be, fraudulent
1	• No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity
2	• No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** • No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent
3	• No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** • No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** • No confirmed evidence, using HMG specified source(s), that the Applicant is fraudulent
4	• No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** • No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** • No confirmed evidence, using HMG specified source(s), that the Applicant is fraudulent **AND** • No confirmed evidence, using source(s) private to HMG, that the Applicant is fraudulent

Table 5 - Outcome of Counter-Fraud Checks

30. Further guidance on Counter-Fraud Checks is contained in Annex D.

IPV Element E – Activity History of the Claimed Identity

31. The purpose of Activity History is to prove a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment. Activity History is determined by collating Activity Events across multiple Evidence Categories into a single Activity Event Package.

32. To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity. Activity Event data must refer to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

33. The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used, how easily it can be fabricated and how well its integrity is protected. The proofing organisation shall take this in to account when assessing the Activity History, expanding the data sources and extending the history period where there is insufficient confidence in the Activity Events.

34. The proofing organisation shall be able to demonstrate with the Activity Events a continuous existence of the Claimed Identity over the period required by the Identity Level.

35. The following table describes the scoring profile for this element.

Score	Properties of Activity History
0	• Unable to demonstrate the required Activity History
1	• No demonstration of an Identity’s Activity History was required
2	• Claimed Identity demonstrates an Activity History of at least 180 calendar days
3	• Claimed Identity demonstrates an Activity History of at least 405 calendar days
4	• Claimed Identity demonstrates an Activity History of at least 1080 calendar days

Table 6 - Activity History of the Claimed Identity

36. Examples of Activity Evidence are given in Annex E.

Chapter 6 - Requirements for each Level of Identity

Key Principle

- The 4 levels of identity attract increasing requirements in terms of the IPV element scores as documented in Chapter 6

Requirements

37. The following tables set out the minimum criteria for each IPV element in the various Identity Levels. If higher scores are achieved in an IPV element, they do not materially affect the other IPV element requirements; e.g. if Level 4 Identity Evidence is provided yet only Level 3 Identity Evidence was required, the Validation and Verification requirements remain as Level 3.

Category	Requirements
Identity Evidence Profile	There is no Identity Evidence Package required, instead the Applicant must supply an Identifier.
Validation of Identity Evidence	There is no Validation of identity required, instead the Identifier shall be confirmed as being in existence.
Verification	There is no Verification of identity required, instead the Identifier shall be confirmed as being in the possession and/or control of the Applicant.
Counter-Fraud Checks	There is no requirement for Counter-Fraud Checks.
Activity History	There is no requirement to prove the activity of the Claimed Identity therefore there is no requirement for the Activity Event Package or for any Activity History to be demonstrated.

Table 7 - Requirements for a Level 1 Identity

Category	Requirements
Identity Evidence Profile	The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles: - 1 piece of Identity Evidence with a score of 3 - 1 piece of Identity Evidence with a score of 2 **OR** - 3 pieces of Identity Evidence with a score of 2 These are referred to as an Identity Evidence Profile of 3:2 and 2:2:2 respectively.
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 3:2 the Validation processes must be able to also achieve scores of 3:2 respectively, where it is 2:2:2 it must be able to achieve scores of 2:2:2.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 2 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 2.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 2 for the Activity History of the Claimed Identity.

Table 8 - Requirements for a Level 2 Identity

Category	Requirements
Identity Evidence Profile	The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles: - 2 pieces of Identity Evidence with a score of 3 **OR** - 1 piece of Identity Evidence with a score of 3 - 2 pieces of Identity Evidence with a score of 2 These are referred to as an Identity Evidence Profile of 3:3 and 3:2:2 respectively.
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 3:3 the Validation processes must be able to also achieve scores of 3:3 respectively, where it is 3:2:2 it must be able to achieve scores of 3:2:2 respectively.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 3 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 3.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 3 for the Activity History of the Claimed Identity.

Table 9 - Requirements for a Level 3 Identity

Category	Requirements
Identity Evidence Profile	The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles: - 1 piece of Identity Evidence with a score of 4 - 1 piece of Identity Evidence with a score of 3 **OR** - 2 pieces of Identity Evidence with a score of 3 - 1 piece of Identity Evidence with a score of 2 These are referred to as an Identity Evidence Profile of 4:3 and 3:3:2 respectively.
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 4:3 the Validation processes must be able to also achieve scores of 4:3 respectively, where it is 3:3:2 it must be able to achieve scores of 3:3:2 respectively.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 4 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 4.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 4 for the Activity History of the Claimed Identity.

Table 10 - Requirements for a Level 4 Identity

Chapter 7 - Identity Proofing Definitions

Key Principle

- The definitions of identity relevant terms provided here are intended to support a common understanding in the context of this document

Definitions

38. The following definitions explain the purpose and meanings of the terms used within this document.

Term	Definition
Activity Event	An action, transaction or other point in time occurrence (including issue date) that demonstrates an interaction between the Claimed Identity and another entity. Only Activity Events that are connected to an Identity with Personal Details that match those of the Claimed Identity can be used however, shortenings and aliases are permitted (e.g. Mike for Michael).
Activity Event Package	The Activity Event Package is the collection of Activity Events that is used to evaluate the Activity History of the Claimed Identity. The Activity Event Package must contain Activity Events across multiple Evidence Categories (C, M and L).
Applicant	The individual who is stating the claim to an identity.
Assessment	The activity of performing the identity proofing process as defined in this document.
Assured Identity	A Claimed Identity that is linked to an Applicant with a defined level of confidence that it is the Applicant’s real identity.
Authoritative Source	An authority that has access to sufficient information from an Issuing Source that they are able to confirm the validity of a piece of Identity Evidence.
Biometric	A measure of a human body characteristic that is captured, recorded and/or reproduced in compliance with ICAO 9303 or ISO/IEC 19794.
Citizen Category	A type of evidence category. To be included in the Citizen category at least one of the following criteria shall be met: • Be issued by a Public Authority (or national equivalent) • Be issued by an organisation through a process determined by a Public Authority (or national equivalent)
Claimed Identity	A declaration by the Applicant of their current Personal Name, date of birth and address.
Evidence Categories	A collective term for the categories of evidence i.e. Citizen (C), Money (M) and Living (L). Evidence shall be assessed against every category and can be considered in multiple categories where it meets the required criteria. Where evidence meets the required criteria for multiple categories it may only be used to fulfil one category requirement at a time per IPV Element (i.e. it doesn’t count as fulfilling two categories for a specific IPV Element but can be in different categories for different IPV Elements). This does not mean the evidence must be in the same category for all Applicants, the same type of evidence (e.g. a Bank credit account) may be used in different categories for different Applicants.
Evidence Details	A combination of the unique reference number(s) and, where applicable, issue date and expiry date included on a piece of Identity Evidence.
Financial Organisation	An organisation that has been classified as a “financial institution” or “credit institution” by the Money Laundering Regulations 2007.

Term	Definition
Genuine	To be what something is said to be; i.e. authentic not counterfeit.
Identifier	A thing that is used to repeatedly recognise an individual. The Identifier isn't required to demonstrate the Identity of the individual only that it can be used to recognise the same individual.
Identity	A collection of attributes that uniquely define a person or organisation. The fact of being whom or what a person or thing is.
Identity Assurance	A process that determines that level of confidence that the Applicant's Claimed Identity is their real identity.
Identity Evidence	Information and/or documentation that is provided by the Applicant to support the Claimed Identity. Identity Evidence must, as a minimum, contain the Personal Details **OR** the Personal Name and photo/image of the person to whom it was issued. Identity Evidence must be current, i.e. it must not have an expiry date that is before the time of Assessment. Examples of Identity Evidence are given in Annex A.
Identity Evidence Package	The Identity Evidence Package is the collection of Identity Evidence provided to support the Claimed Identity. The Identity Evidence Package must contain at least one piece of Identity Evidence that demonstrates address and one that demonstrates date of birth. The Identity Evidence Package must only contain one piece of Identity Evidence in any Evidence Category.
Identity Evidence Profile	The Identity Evidence Profile sets out the minimum criteria for the strength of Identity Evidence in the Identity Evidence Package.
Issuing Source	An authority that is responsible for the generation of data and/or documents that can be used as Identity Evidence.
Knowledge Based Verification (KBV)	**Static** Where a secret has been previously exchanged between two parties. One party uses the secret to verify that they are the other party with whom the secret was originally exchanged. Also referred to as a shared secret. **Dynamic** A process where the Applicant is required to provide answers to questions relating to the Claimed Identity.
Living Category	A type of evidence category. To be included in the Living category at least one of the following criteria shall be met: • Be issued by an organisation that provides employment to the Applicant • Be issued by an organisation that provides education services to the Applicant • Be issued by an organisation that provides training services to the Applicant • Be issued by an organisation that provides certified assessment of the Applicant • Be issued by an organisation that provides licensing of the Applicant • Be issued by an organisation that provides an essential utility to the Applicant • Be issued by an organisation that provides living support to the Applicant • Be issued by an organisation that operates a community or social group/network to which the Applicant belongs • Be issued by an organisation that operates a loyalty programme to which the Applicant belongs • Be issued by an organisation that operates a subscription service to which the Applicant subscribes • Be issued by an organisation that provides health services to the

Term	Definition
	Applicant • Be issued by an organisation that provides goods or services to the address of the Applicant
Money Category	A type of evidence category. To be included in the Money category at least one of the following criteria shall be met: • Be issued by a Financial Organisation regulated by a Public Authority (or national equivalent) • Be issued by a Financial Organisation regulated by a body mandated by national legislation
Personal Details	A combination of Personal Name and **at least one of** date of birth or address. (Not to be confused with Personal Data as defined by the Data Protection Act.)
Personal Name	A proper name used to identify a real person, as a minimum this contains forename and surname (also known as given name and family name); it may include titles, other/middle names and suffixes.
Proprietary Apparatus	Any apparatus that is, or has been, specially designed or adapted for the making of false documents, and any article or material that is, or has been, specially designed or adapted to be used in the making of such documents.
Proprietary Knowledge	Knowledge about the format, layout and material that is required for the making of a false document.
Public Authority	An organisation that has been classified as such by the Freedom of Information Act 2000.
Valid	To know that something stated is true.
Validation	A process performed to determine whether a piece of Identity Evidence is Genuine and/or Valid.
Verification	A process performed to determine whether the Applicant is the owner of the Claimed Identity.

Table 11 – Definitions

Annex A - Evidence Examples (IPV Element A)

39. No single piece of evidence can be considered as proof of identity. However combined with other pieces of evidence they can be used in order to develop a level of assurance as to the identity of an individual.

40. The following tables provide examples of the types of evidence data that may be provided and the Evidence Categories they could be considered to be in. The Tables should not be considered as complete or definitive.

Identity Evidence	Citizen	Money	Living
Fixed line telephone account			X
Gas supply account			X
Electricity supply account			X
Police bail sheet	X		X

Table 12 - Level 1 Identity Evidence

Identity Evidence	Citizen	Money	Living
Firearm Certificate	X		X
DBS Enhanced Disclosure Certificate	X		
HMG issued convention travel document	X		
HMG issued stateless person document	X		
HMG issued certificate of travel	X		
HMG issued certificate of identity	X		
Birth certificate	X		
Adoption certificate	X		
UK asylum seekers Application Registration Card (ARC)	X		
Unsecured personal loan account (excluding pay day loans)		X	X
National 60+ bus pass	X		X
An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)	X		X
An education certificate gained from a well recognised higher educational institution			X
Residential property rental or purchase agreement		X	X
Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)			X
Police warrant card	X		
Freedom pass	X		X
Marriage certificate	X		X
Fire brigade ID card	X		
Non bank savings account		X	
Mobile telephone contract account		X	X
Buildings insurance			X
Contents insurance			X
Vehicle insurance			X

Table 13 - Level 2 Identity Evidence

Identity Evidence	Citizen	Money	Living
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004	X		
Northern Ireland Voters Card	X		X
US passport card	X		
Retail bank/credit union/building society current account		X	
Student loan account		X	X
Bank credit account (credit card)		X	X
Non-bank credit account (including credit/store/charge cards)		X	
Bank savings account		X	
Buy to let mortgage account		X	X
Digital tachograph card	X		X
Armed forces ID card	X		
Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number)			X
Secured loan account (including hire purchase)		X	X
Mortgage account		X	X
EEA/EU full driving licences that comply with European Directive 2006/126/EC	X		X

Table 14 - Level 3 Identity Evidence

Identity Evidence	Citizen	Money	Living
Biometric passports that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g. UK/EEA/EU/US/AU/NZ/CN)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	X		
UK Biometric Residence Permit (BRP)	X		
NHS staff card containing a biometric			X

Table 15 - Level 4 Identity Evidence

Annex B - Validation (IPV Element B)

Determining whether Identity Evidence is Genuine

Examination of the security features of a physical document

41. The proofing organisation capability to Validate identity documents will affect the determined level of identity assurance. The proofing organisation shall have sufficiently trained staff and appropriate equipment to inspect the security features of common forms of physical documents that they accept as Identity Evidence. As a minimum a proofing organisation conducting physical inspection of Identity Evidence shall be able to detect the following common document frauds:

- Counterfeit documents – where a document has been created outside of the normal competent authority processes (e.g. a copy)
- Forged documents – where original documents have been modified to include false details (e.g. changed Personal Details)

Physical document containing cryptographically protected information

42. For physical documents provided by the Applicant that contains cryptographically protected information the proofing organisation shall have sufficient equipment, systems and training to be able to interrogate the cryptographically protected information, to ensure that it has not been altered since the Issuing Source produced the Identity Evidence and determine that the cryptographically protected information relates to the physical document to which it is attached.

Electronic evidence containing cryptographically protected information

43. For electronic Identity Evidence provided by the Applicant that contains cryptographically protected information (e.g. in a PDF document), the proofing organisation shall have sufficient systems and training to interrogate the cryptographically protected information and determine that it relates to the Identity Evidence, and that the Identity Evidence has not been altered since it was produced by the Issuing Source.

Checking if the Identity Evidence is Valid

44. The proofing organisation should confirm that forms of Identity Evidence that include features such as check digits and specific identifier structures are consistent with their specification. Only an Issuing/Authoritative Source may confirm whether the Identity Evidence is Valid; Identity Evidence cannot be determined to be Valid simply from inspection of the Identity Evidence itself (see Genuine).

Annex C - Verification (IPV Element C)

Static Knowledge Based Verification (KBV)

45. Static KBV requires that the Applicant and the proofing organisation have a pre-existing shared secret, or that the proofing organisation uses an external trusted source with which the Applicant already has a shared secret.

46. There must be a reasonable expectation that the Applicant is aware that they should not disclose this secret to any person or organisation other than the one with whom they share the secret.

47. The secret must be random enough to make it unlikely to be guessed by an attacker who is given a number of opportunities to guess it.

48. A shared secret may only be exchanged via a method where the proofing organisation has confirmed that the delivery method is linked to the Claimed Identity.

49. External trusted source where the Applicant already has such a relationship can be used as a static KBV. Where an external trusted source is used, the process shall be able to confirm to the proofing organisation that an individual with matching Personal Details has successfully passed the Static KBV process.

Dynamic Knowledge Based Verification

50. Dynamic KBV needs the proofing organisation to gather information about the Claimed Identity and then requires the Applicant to demonstrate that they have such knowledge about the Claimed Identity that it is likely they are the owner of that identity.

51. The quality and success of the Dynamic KBV process is dependent on a number of factors:

    - The questions should be relevant, sensible and proportionate
    - There shall be an expectation that the owner of the Claimed Identity can reasonably be expected to know the answer
    - The questions shall be unambiguous as to be easily understood by the Applicant
    - The ease by which the Applicant can enter the correct answer
    - The availability of the answer from information in the public realm, especially social networking sites and public registers
    - The likelihood of friends and family knowing the answer
    - The difficulty by which the questions could be correctly answered by guesswork
    - The risk of datasets containing the required information being made available to organised crime

- The risk that the theft of a possession such as a wallet or purse could provide the required information to an imposter

Dynamic KBV data

52. The degree of assurance that can be taken from the KBV process is linked to the quality and availability of the data used to generate the questions.

53. Wherever it is practical to do so, KBV data should not be used if it is already in the public domain. Information in the public domain means that the KBV data can be accessed by another person either with or without a degree of research or is contained within a public facing information site.

Dynamic KBV principles

54. There must be a sensible balance between achieving assurance that the Applicant is the owner of the Claimed Identity and presenting an attractive Applicant journey. With this in mind the proofing organisation shall follow a number of basic KBV principles:

- The proofing organisation should try to use KBV data of the highest quality where possible. Fewer questions about KBV data that is highly unlikely to be known by someone other than the owner of the Claimed Identity is preferable to many questions about KBV data that is more likely to be available to others
- KBV questions shall be based on a range of KBV data and not reliant upon one single KBV source
- KBV questions should be carefully constructed as to be clear and obvious to the Applicant what is being asked
- KBV questions should cover facts about the Claimed Identity that fall into different Evidence Categories
- Where the proofing organisation offers the Applicant a selection of suggested answers (i.e. multiple choices) then all the answers must be plausible and the correct answer should not be easily guessed or determined using publicly available information
- It must be recognised that the process cannot account for every eventuality when using KBV, e.g. it must accepted that certain KBV data items may be known to close family members

Physical Comparison

55. The physical comparison step of verification requires the Applicant to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued. The two methods by which this may be completed are an in person face-to-face process and a remote process (e.g. using a video/video streaming link). In either case the proofing organisation shall consider a number of basic principles:

- Any person performing the comparison must be able to clearly see both the Applicant and the image to which the Applicant is being compared

- Any person performing the comparison shall have sufficient training in performing identification of persons
- The quality of images must be sufficient to allow the identification of the Applicant as the person depicted by the Identity Evidence

Biometric Comparison

56. The biometric comparison step of verification requires the Applicant to be verified by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued. The proofing organisation shall consider a number of basic principles:

- The False Non-Match Rate (FNMR) of the biometric matching system
- The False Match Rate (FMR) of the biometric matching system
- The quality of the biometric against which the Applicant is being compared

57. In particular the proofing organisation shall ensure they have a sufficiently low FMR in order to have confidence that the biometric system is effective at detecting imposters.

Annex D - Counter-fraud Capabilities (IPV Element D)

58. As part of the counter fraud checks the proofing organisation shall have, through their own internal data sets or via reliable and independent sources, the following counter fraud checking capabilities:

- Whether the Claimed Identity has been subject to identity theft, regardless whether it was successful or not
- Whether the Claimed Identity is known to other organisations
- Whether the Claimed Identity is likely to be targeted by third parties
- Whether the Claimed Identity may be deceased
- Whether the Claimed Identity is known to be a fraudulent identity

Annex E - Example Activity Events (IPV Element E)

59. The following Table provides examples of activity events that could be used to demonstrate a history of activity.

Citizen	Money	Living
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

Table 16 - Example Activity Events

Reference

[a] CESG Good Practice Guide No. 43, Requirements for Secure Delivery of Online Public Services – latest issue available from the CESG website.

“CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.”

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk