The Road to Multilateral Recognition of Identity Assurance Programs

A Comparison of Requirements:
United Kingdom & United States Government

Editor: KENNETH DAGG

Contributors:

Howard Staple	Identity & Information Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office
Alastair Treharne	Identity Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office
Joni Brennan	Executive Director, Kantara Initiative

Abstract:

This study is one of a set of reports prepared by the Kantara Initiative to assess if it is viable for the United Kingdom (UK) Cabinet Office to recognize Identity Providers approved by other international bodies for use in the UK. The purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs.

This specific report presents, based upon a high level analysis, observations from a comparison of United States Government requirements with the requirements specified by the UK. It also recommends activities for additional analysis to determine if United States Government requirements fully meet the specific requirements that the UK has established.

Contents

1 PROJECT OVERVIEW

1.1 Project Purpose

This project is being undertaken by the Kantara Initiative to assess the processes currently being used by other international bodies to accredit and certify/approve Identity Providers (IDAs) with the goal of determining if it is viable for the United Kingdom (UK) Cabinet Office to recognize these IDAs for use in the UK. The purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs.

To test the feasibility of this approach of the UK Cabinet Office, and start down the road to multilateral recognition, this project will provide a high level assessment of the processes used by the Federal Identity, Credential, and Access Management (FICAM) program of the Government of the United States of America (US) to accredit and approve IDAs for use by the US Government.

1.2 Project Business Objectives

This project will specifically identify options, recommendations and timeframes based upon an:

- Assessment of the equivalence of Kantara Initiative's Identity Assurance Framework (IAF) requirements against the UK's requirements for Certification Bodies (CBs) and IDAs.
- Assessment of the equivalence of US Government and Cabinet Office requirements for CBs and IDAs including authentication governance.
- Assessment of the future direction and evolution of the National Institute of Standards and Technology (NIST) Electronic Authentication Guideline (Special Publication 800-63).

The options, recommendations and timeframes identified in this assessment will contribute to the Cabinet Office of the UK Government recognizing other jurisdictions as Accredited CBs that are able to certify IDAs to Cabinet Office standards, so that the Cabinet Office does not have to carry out the assessment of the IDAs. This in turn contributes to the Cabinet Office realizing its vision to create a market of certified, customer-focused services in the private sector that will provide a consistent way for customers to access any public service, and potentially private sector services.

2 Contents

Section 3 of this document presents, based upon a high level analysis, a comparison of United States Government and United Kingdom requirements. It should be noted that The US requirements are only applicable to the US Government while UK requirements are applicable to both the public and private sectors.

Section 4 identifies US Government requirements that the UK might want to consider incorporating.

Section 5 summaries the findings from the comparison of FICAM's requirements with the requirements specified by the UK.

Appendix A contains a list of the Acronyms, Abbreviations and terms used in the document. Appendix B identifies the materials that were analyzed. Appendix C contains more details on the findings of the analysis.

3 Requirements Comparison

This section presents, based upon a high level analysis, the observations and recommendations from a comparison of FICAM's requirements to the requirements specified by the UK in the following documents:

- GPG 43: Requirements for Secure Delivery of Online Public Services (RSDOPS) - Issue No: 1.1
- GPG 44: Authentication Credentials in Support of HMG Online Services - Issue No: 2.0, and
- GPG 45: Validating and Verifying the Identity of an Individual in Support of HMG Online Services - Issue No: 2.3
- GPG 53: Transaction Monitoring for HMG Online Service Providers, Issue No: 1.0
- Specification for Organisations Providing Proofing and Authentication of Digital Identities, v0.3 Draft
- Specification for Certification Bodies Certifying Identity Assurance Providers, Draft
- IPV (Identity Proofing and Verification) Operations Manual, version 2.3.1
- Identity Assurance Hub Service SAML 2.0 Profile, version 1.1a

The following documents contain the requirements used by the US Government:

- E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) M-04-04 December 16, 2003
- Electronic Authentication Guideline, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, Version 2, August 2013
- Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS), Trust Framework Provider Adoption Process (TFPAP) For All Levels of Assurance, Version 2.0.2, March 14, 2014

This section also recommends additional analysis activities to determine if FICAM requirements fully meet some very specific requirements established by the UK.

Appendix C contains details of the high level assessment.

It should be noted, as a general observation, FICAM requirements are for LOA Level 1, Level 2, and Level 3 non-PKI. FICAM requirements do not address LOA Level 3 PKI or Level 4 requirements.

3.1 GPG 43

Levels of Assurance

Observations

The US Government's approach, while seeming to examine different aspects of the situation, covers essentially the same overall aspects as the UK's analysis with the exception of explicitly examining privacy. The US Government explicitly examines privacy as a separate trust criteria outside determination of the required Level of Assurance.

The result of both risk analyses is that Service Providers identify the Level of Assurance they require for the electronic transaction system.

The following provides an overview of the equivalency of the levels.

Authentication Assurance		Identity Assurance	
UK	FICAM	UK	FICAM
1	1	1	1
	2	2	2
2	3	3	3
3	4	4	4

The UK does not have an equivalent to FICAM Authentication Level 2.

Recommendations

The UK could examine extracting privacy requirements out of the determination of Level of Assurance and include them as a separate set of requirements in GPG 44 or in Service Delivery Requirements.

3.2 GPG 44

3.2.1 AC Element A: Credential Type

Observations

FICAM does not include a requirement:

- at LOA Level 1 that specify that the user demonstrate they are in possession of a Secret (e.g. a password, PIN, etc.) belonging to the legitimate account holder.
- at LOA Level 3 that specifies that the user demonstrate that they are in possession of a biometric belonging to the legitimate account holder.

3.2.2 AC Element B: Quality of the Credential

Observations

FICAM has similar requirements.

3.2.3 AC Element C: Management of the Credential

Observations

FICAM does not include requirements:

- at LOA Level 1 that require:
  - credentials be stored so that they are protected from unauthorised physical and electronic access.
  - changes to the state of the Credential (revocation, recovery, replacement) only be made by the person to whom the Credential belongs and that CSPs revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised.
- at LOA Level 1 and 3 that request that the Authentication Provider ensure:
  - a credential manufacturer has a quality management process to ensure consistency,
  - an information security management system that protects information from compromise is in place, and
  - a process for exchanging information that protects its integrity and confidentiality is in place.
- at LOA Level 3 that ensure that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.

3.2.4 AC Element D: Monitoring

Observations

FICAM does not include requirements:

- at LOA Level 1 to ensure that the Authentication Provider check for indications that the Credential maybe being used by someone other than its owner.
- at LOA Level 3 to explicitly require analysis and reporting of abnormal authentication behaviour.

Recommendations

The UK add requirements at LOA Level 2 for a capability to detect fraudulent behavior e.g. velocity of transactions, customer history and behavior etc. as well as to analyze and report this abnormal authentication behaviour.

3.2.5 AC Element E: Authentication Service Characteristics

Observations

FICAM does not include requirements:

- at LOA Level 1 and 3 that explicitly require technology systems to deliver its authentication services.
- at LOA Level 1 to ensure that the Authentication service suspend or revoke a Credential after a number of failed Authentication attempts or that the Authentication service protect authentication sessions using Good Industry Practice security measures.
- At LOA Level 1 to ensure that the user of the Authentication service can determine that they are using a secure channel.
- at LOA Level 3 that check for measures that are effective at preventing use by non-human operators.
- at LOA Level 3 that check for measures that protect the Credential from compromise, even if the communication channel is compromised.

3.2.6 AC Element F: Information Assurance Maturity of the Authentication Provider

Observations

FICAM does not include requirements:

- at LOA Level 1 and 3 that address the requirements identified by the UK for information assurance maturity.
- at LOA Level 1 that require:
- an effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, be in place.
- the Authentication Provider be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service.
- all systems supporting the use of the Credential have a consistent time.
- the Authentication Provider have a monitoring regime that detects unexpected and undesirable activity within the service it does require that it apply controls during system development, procurement, installation, and operation that protect

the security and integrity of the system environment, hardware, software, and communications.

- the Authentication Provider conducts regular risk assessments and have defined processes for exception handling.
- the Authentication Provider apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.

3.3 GPG 45

3.3.1 IPV Element A – Strength of Identity Evidence

Observations

FICAM does not include requirements at LOA Level 1 for In-Person Public Identity Proofing that meet the requirements of the UK.

Recommendations

Additional analysis is required to determine if the identity proofing activities required by FICAM to meet LOA Level 3 satisfy UK Money Laundering Regulations 2007.

3.3.2 IPV Element B – Outcome of the Validation of Identity Evidence

Observations

FICAM does not include a requirement at LOA Level 1 to confirm that all Personal Details from the Identity Evidence has been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source.

3.3.3 IPV Element C – Outcome of Identity Verification

Observations

FICAM does not include requirements at LOA Level 1 to verify that the Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity.

3.3.4 IPV Element D – Outcome of Counter-Fraud Checks

Observations

FICAM does not include requirements concerning Counter-Fraud Check processes.

Recommendations

The UK should consider adding requirements that the authentication process implement internet protocol (IP) reputation based tools (i.e., IP blacklisting capability) and anomaly detection capabilities (e.g., velocity of transactions, customer history and behavior) to mitigate fraudulent activity.

3.3.5 IPV Element E – Activity History of the Claimed Identity

Observations

FICAM does not include requirements concerning the Activity History of the Claimed Identity.

3.4 Service Delivery Requirements

Observations

FICAM does not have the requirements for Service Delivery identified by the UK.

3.5 Specification for Organisations Providing Proofing and Authentication of Digital Identities

Observations

FICAM does not include requirements to ensure that:

- liability is covered for the entirety of the Service.
- an organization that has been suspended by one Certification Body, due to a failure to implement the requirement in this specification, shall not be allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.
- an organization has written procedures for Control of documents, Control of records, Control of non-conforming services, Corrective action, Preventative action, Internal audit, and Management review.
- an organization has a quality management system and that they meet a recognised standard for Quality Management (e.g. ISO9001).
- an organization has an Information Security Management System (ISMS) and that they meet a recognised standard for ISMS (e.g. ISO27001).
- an organization agrees to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate.
- at least five per cent of Identities proofed are internally audited within a 12-month period.
- an organization is required to identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.
- an organization is required to carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.
- an organization is required to have in place and operate a documented complaints procedure.

- an organization is required to have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service.
- only applications that meet the requirements, as defined in FICAM's equivalent to the IPV Operations Manual and Service Delivery Requirements, are registered.

FICAM does not include Gender and Evidence details in the records associated with each Identity Assurance Assessment undertaken OR the UK could make the capture of Gender and Evidence details optional.

Recommendations

Determine if US Government requirements concerning protecting all sensitive data, including Personally Identifiable Information (PII), meet UK requirements.

Determine if US Government requirements concerning the processing of personal data meet UK requirements.

3.6 Specification for Certification Bodies Certifying Identity Assurance Providers

Observations

The US Government's Trust Framework Provider Adoption Process does not require Trust Framework Providers to be accredited against BS EN ISO/IEC 17065.

Recommendations

Further investigation will need to be undertaken to determine if the requirements of the US Government's TFPAP could be satisfied by requiring that TFPs be accredited against BS EN ISO/IEC 17065.

4 Potential Modifications to GPG 44 Requirements

FICAM includes the following requirements that the UK might want to consider.

1. FICAM includes requirements that the authentication process have internet protocol (IP) reputation based tools (i.e., IP blacklisting capability) and anomaly detection capabilities (e.g., velocity of transactions, customer history and behavior) to mitigate fraudulent activity.
2. FICAM has slightly different requirements according to the following types of identity proofing:
    - In-Person Public Identity Verification
    - Remote Public Identity Verification
3. FICAM includes requirements at LOA Level 2 for a capability to detect fraudulent behavior e.g. velocity of transactions, customer history and behavior etc. as well as to analyze and report this abnormal authentication behaviour.

5 Conclusions

A high-level analysis of FICAM requirements indicates that FICAM has equivalent requirements to the majority of the requirements established by the UK. Unless the UK is willing to eliminate those requirements that FICAM does not include it will need to discuss with the United States Government how FICAM proposes to address those requirements.

It should be noted that any FICAM approved service at LOA Level 2 will be considered to be a LOA Level 1 service by the UK.

There are several cases where further analysis of FICAM requirements must be undertaken to ensure that these requirements meet jurisdictional specific requirements that have been established by the UK.

The high-level analysis also identified several requirements contained in FICAM that the UK might wish to consider for inclusion in their requirements.

While the processes used by both FICAM and the UK appear to be similar further investigation is required by experts in that process to validate that they are equivalent. This could be accomplished by either undertaking further analysis or by having FICAM have its process certified by the American National Standards Institute (ANSI) as meeting the specifications of ISO/IEC 17065.

APPENDIX A – ACRONYMS, ABBREVIATIONS AND GLOSSARY

This appendix expands acronyms and abbreviations used in the project.

Term	Definition
CB	Certification Body
CESG	Communications-Electronics Security Group
FIPS	Federal Information Processing Standards
GPG	Good Practice Guide
HMG	Her Majesties Government
IAF	Identity Assurance Framework
ICT	Information and Communications Technology
IDA	Identity Assurance Provider
IPV	Identity Proofing and Verification
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
RSDOPS	Requirements for Secure Delivery of Online Public Services
TLS	Transport Layer Security
UK	United Kingdom
UKAS	United Kingdom Accreditation Service
US	United States of America

APPENDIX B – ANALYSIS REFERENCE MATERIAL

- Good Practice Guide 43 - Requirements for Secure Delivery of Online Public Services, Issue No: 1.1, December 2012, Communications-Electronics Security Group (CESG), Crown copyright 2012.
- Good Practice Guide No. 44 - Authentication and Credentials for use with HMG Online Services, Issue No: 2.0, October 2014, CESG, Crown copyright 2014
- Good Practice Guide No. 45 - Identity Proofing and Verification of an Individual, Issue No: 2.3, July 2014, CESG, Crown copyright 2014
- Good Practice Guide No. 53 - Transaction Monitoring for HMG Online Service Providers, Issue No: 1.0, April 2013, CESG, Crown Copyright 2013
- Specification for Organisations Providing Proofing and Authentication of Digital Identities, v0.3 Draft, Date: Unknown
- Specification for Certification Bodies Certifying Identity Assurance Providers, Draft, Date: Unknown
- IPV (Identity Proofing and Verification) Operations Manual, version 2.3.1, December 4, 2014
- Identity Assurance Hub Service SAML 2.0 Profile, version 1.1a, September 11, 2013, Identity Assurance Programme, Crown Copyright 2013
- E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) M-04-04, December 16, 2003
- Electronic Authentication Guideline, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, Version 2, August 2013
- Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS), Trust Framework Provider Adoption Process (TFPAP) For All Levels of Assurance, Version 2.0.2, March 14, 2014
- National Strategy For Trusted Identities In Cyberspace (NSTIC), Enhancing Online Choice, Efficiency, Security, and Privacy, Appendix A - Fair Information Practice Principles (FIPPs), April 2011, United States White House

APPENDIX C – SPECIFIC ANALYSIS OF REQUIREMENTS

This appendix provides further details of the high-level comparison.

Service Delivery Requirements

Service Delivery Requirements	Observations about FICAM

Requirements that a provider must meet in order to be operational are identified in the following areas:
• Service Readiness Assessment Criteria
• Service Reporting
• Service Management Information
• ICT Release and Deployment Management
• IDA Onboarding
• Configuration and Configuration Management
• Incident and Problem Management
• Service Desk
• User Experience
	The US Government defines Trust Frameworks including a governance structure for a specific identity system consisting of:
	• The Technical and Operational Specifications that have been developed to:
	  • Define requirements for the proper operation of the identity system (i.e., so that it works),
	  • Define the roles and operational responsibilities of participants, and
	  • Provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that it is trustworthy); and
	• The Legal Rules that govern the identity system in order to
	  • Regulate the content of the Technical and Operational Specifications,
	  • Make the Technical and Operational Specifications legally binding on and enforceable against the participants, and
	  • Define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.
	However, there are no specific requirements set forth for a provider to ensure the proper operation of the identity system.

A Comparison of Requirements: United Kingdom & United States Government

OBSERVATION: FICAM does not have service assessment criteria to address the requirements for Service Delivery identified by the UK.

GPG 43 Comparison – Levels of Assurance

GPG 43 states that a Service Provider should undertake a risk analysis that considers threats, vulnerabilities and service or transaction value as well as the expectations of the stakeholders. Based on the results of the risk analysis, an understanding of the budgets, capabilities, motivations, and risk tolerances of the organisation, and an understanding of the direct and indirect consequences of a failure of each security component, a security profile is developed that specifies a level for each of the following security components:

- End User
  - Personal Registration
  - Corporate Registration
  - Authentication
  - Authorisation
  - Privacy
- Server
  - Information Access
  - Information Availability
- Network
  - Communications Security
  - Network Authentication
  - Network protection
  - Situational awareness
- Business logic
  - Internal accountability
  - External accountability
- Assurance
  - Organisational assurance
  - Technical assurance

The US Government states that to successfully implement a government service electronically (or e-government), Federal agencies must determine the required Level of Assurance in the authentication for each transaction. This is accomplished through a risk assessment for each transaction that identifies risks, and their likelihood of occurrence.

To determine the appropriate Level of Assurance in the user's asserted identity, agencies must assess the potential risks as a function of the potential harm or impact, and the likelihood of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information

- Personal safety
- Civil or criminal violations.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the following potential impact values:

- Low impact
- Moderate impact
- High impact.

The US Government's approach, while seeming to examine different aspects of the situation, covers essentially the same overall aspects as the UK's analysis with the exception of explicitly examining privacy. Privacy is one of the seven specific trust criteria that are examined.

The result of both risk analyses is that Service Providers identify the Level of Assurance they require for the electronic transaction system.

As shown in the following, the UK and FICAM both have definitions for Identity and Authentication Assurance.

Authentication Assurance

Level	UK (GPG44)	FICAM
1	The authentication demonstrates that the person requesting authentication is in possession of the Credential for a legitimate account. At this level, it is not necessary to link the use of the Credential to the owner, therefore there is no protection against Credential theft.	Little or no confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.
2	The authentication provides sufficient confidence that the Credential is being used by the legitimate account holder, or with the explicit consent of the legitimate account holder, and might be offered in support of civil proceedings. The Credential is bound to its owner and provides protection against Credential theft.	Some confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.
3	The authentication provides sufficient confidence that the Credential is being used by the legitimate account holder, or with the explicit consent of the legitimate account holder, and might be offered in support of criminal proceedings. The Credential is bound to its owner and protects the transaction from attacks where the Credential may have been compromised.	High confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.
4	None	Very high confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.

Identity Assurance

Level	UK (GPG45)	FICAM
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.	Little or no confidence that an individual is who he or she claims to be.
2	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.	Some confidence that an individual is who he or she claims to be.
3	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.	High confidence that an individual is who he or she claims to be.
4	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.	Very high confidence that an individual is who he or she claims to be.

The meaning of the increase in Level of Assurance (i.e., from Level 1 to Level 2) means in essence the same for both the US Government and the UK: as levels of risk to a

service or transaction increase then what needs to be done from a security and assurance perspective increases in proportion.

The following provides an overview of the equivalency of the levels.

Authentication Assurance		Identity Assurance	
UK	FICAM	UK	FICAM
1	1	1	1
	2	2	2
2	3	3	3
3	4	4	4

For both the UK and US Government, the Level of Assurance specifies the strength and rigour of the identity proofing process, the credential's strength, and the management processes required of the electronic trust service provider that is to provide the authentication service. Both the UK and US Government have established service assessment criteria at each assurance level for electronic trust services providing credential management services. These service assessment criteria will be compared in later sections.

Conversely, in both the UK and US Government, IDAs can determine the assurance level at which their services might qualify by evaluating their overall business processes and technical mechanisms against the published criteria.

OBSERVATION: The UK does not have an equivalent to FICAM Authentication Level 2.

RECOMMENDATION: The UK could examine extracting privacy requirements out of the determination of Level of Assurance and include them as a separate set of requirements in GPG 44 or in Service Delivery Requirements.

GPG 44

AC Element A: Credential Type

It is considered that the following Credential types, and combination of Credential types, are appropriate to support each of the authentication levels. The following table demonstrates the type of Credential required in order to meet the defined authentication levels.

Score	GPG 44 Requirement	Observations about FICAM
1	A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, etc.) belonging to the legitimate account holder (see Annex A for further guidance on Secrets).	LOA Level 1 does not require demonstration that the user is in possession of a Secret (e.g. a password, PIN, etc.) belonging to the legitimate account holder.
2	Requirements for Score 1, plus one of the following: • A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, OTP, LTS, etc.) belonging to the legitimate account holder that is exchanged over a channel that is separate to the authentication channel (see Annex A for further guidance on Secrets). • A Credential type that demonstrates the user is in possession of a biometric belonging to the legitimate account holder (see Annex D of GPG 44 for further guidance on the use of biometrics).	LOA Level 3 requires proof of possession of the allowed types of tokens through a cryptographic protocol. Authentication requires the Claimant to prove through a secure authentication protocol that he or she controls the token. However, LOA Level 3 does not require the user to demonstrate that they are in possession of a biometric belonging to the legitimate account holder.
3	Requirements for Score 1, plus the following: • A Credential type that demonstrates the user is in possession of a hardware or software token belonging to the legitimate account holder.	No published requirements.

OBSERVATION: FICAM does not include a requirement at LOA Level 1 that specify that the user demonstration they are in possession of a Secret (e.g. a password, PIN, etc.) belonging to the legitimate account holder.

OBSERVATION: FICAM does not include a requirement at LOA Level 3 that specifies that the user demonstrate that they are in possession of a biometric belonging to the legitimate account holder.

AC Element B: Quality of the Credential

The effectiveness of measures that the Credential employs to protect it from being predicted, duplicated or otherwise compromised are important factors in assessing its suitability for use. The following Table demonstrates the properties for the quality of the Credential and the corresponding score for this element. The Credential must, as a minimum, meet all the properties defined for the quality to achieve that score.

Score	GPG 44 Requirement	Observations about FICAM
1	The Credential contains no protective measures to prevent prediction or duplication (e.g. it is a Secret that is memorised by the user). Users shall be encouraged through process, or guidance, to use Credentials with good security properties.	Similar requirements.
2	The Credential uses measures that make it unlikely to be predicted. The Credential has measures that prevent duplication without direct access to the Credential. The Credential has measures that resist tampering. Hardware and software tokens are implemented in accordance with current Good Industry Practice (e.g. NIST SP 800-63-2) including protection against offline attack. Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level 2).	Similar requirements.
3	Requirements for Score 2, plus the following: • The Credential has measures that prevent duplication. • The Credential has measures that	No published requirements.

	detect and prevent compromise from tampering. • Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level).	

OBSERVATION: FICAM has similar requirements.

AC Element C: Management of the Credential

The confidence in the Credential is not only dependent on its properties, as the Authentication Provider must carefully manage the Credentials over their lifetime. The following Table demonstrates the required Credential management processes and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for Credential management to achieve that score.

Score	GPG 44 Requirement	Observations about FICAM
1	The Authentication Provider stores Credentials so that they are protected from unauthorised physical and electronic access to prevent theft or damage. Further information on the storage of Credentials can be seen at Annex C. The Authentication Provider shall be able to suspend a Credential immediately from the primary system that stores the records of the currently authorised Credentials. The Authentication Provider shall be able to permanently revoke a Credential with immediate effect. The Authentication Provider shall enable the user to recover/request a replacement Credential.	LOA Level 1 does not require that: • credentials be stored so that they are protected from unauthorised physical and electronic access. • changes to the state of the Credential (revocation, recovery, replacement) can only be made by the person to whom the Credential belongs and that CSPs revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised. • a credential manufacturer have a quality management process to ensure consistency, or an information security management system which protects information from compromise, or a process for exchanging information that

	The Authentication Provider shall ensure that changes to the state of the Credential requested by the user can only be made by the person to whom the Credential belongs. The Authentication Provider shall ensure the Credential is bound to a single account. The issuing process for the Credential shall take measures that attempt to deliver it into the possession of the user that requested it. The Authentication Provider shall ensure that the Credential is under the control of the person/user to whom it belongs before, or on, first use. Where the Credential has been manufactured, the manufacturer shall have a quality management process to ensure consistency. Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an information security management system which protects that information from compromise (e.g. ISO27001). Where a Credential manufacturer supplies information to the Authentication Provider, which is required as part of the Authentication, then the process for exchanging that information shall protect its integrity and confidentiality.	protects its integrity and confidentiality.
2	Requirements for Score 1, plus the following: • The issuing process for the Credential shall take sufficient measures so that it can reasonably be assumed to have been	LOA Level 3 does not explicitly require: • a credential manufacturer to have an independently audited quality management process to ensure consistency;

	delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an independently audited quality management process to ensure consistency (e.g. ISO 9000 series). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an independently audited information security management system which protects that information from compromise (e.g. ISO 27001).	• an independently audited information security management system which protects that information from compromise, or • the Authentication Provider to have taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.
3	Requirements for Scores 1 and 2, plus the following: • The issuing process for the Credential shall take all reasonable measures to ensure it has been delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an independently certified quality management process to ensure consistency under a Good Industry Practice certification scheme (e.g. ISO 9000 series). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an independently certified information security management system which protects that information from compromise (e.g. ISO 27001).	No published requirements.

OBSERVATION: FICAM does not include requirements in LOA Level 1 that require:

- credentials be stored so that they are protected from unauthorised physical and electronic access.
- changes to the state of the Credential (revocation, recovery, replacement) only be made by the person to whom the Credential belongs and that CSPs revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised.

OBSERVATION: FICAM does not include requirements in LOA Level 3 that ensure that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.

OBSERVATION: FICAM does not include requirements in LOA Level 1 and 3 that request that the Authentication Provider:

- a credential manufacturer has a quality management process to ensure consistency,
- an information security management system that protects information from compromise, and
- a process for exchanging information that protects its integrity and confidentiality.'

AC Element D: Monitoring

The qualities and management of the Credential contribute to its security, but it is also necessary to monitor its use. Therefore, the Authentication Provider shall monitor the use of a Credential, its services and sources to detect and react (e.g. incident management) to the misuse of a Credential. The following table demonstrates the monitoring requirements and the corresponding scores for this element. The Authentication Provider must, as a minimum, meet all the properties defined for monitoring to achieve that score.

Score	GPG 44 Requirement	Observations about FICAM
1	The Authentication Provider shall check for indications that the Credential maybe being used by someone other than its owner. Where the Authentication Provider has reasonable suspicion that the Credential is being used by someone other than its owner, the Authentication Provider shall take sufficient measures in order to determine the user is the owner of the Credential, which may include	LOA Level 1 does not require that the Authentication Provider check for indications that the Credential maybe being used by someone other than its owner.

	revoking and replacing the Credential.	
2	Requirements for Score 1, plus the following: • The Authentication Provider shall take measurements to establish what normal and legitimate authentication behaviour looks like (see GPG 53), Transaction Monitoring for HMG Online Service Providers. • The Authentication Provider shall detect, and where applicable report, abnormal authentication behaviour (see GPG 53).	LOA Level 3 optionally requires a capability that is capable of detecting fraudulent behavior e.g. velocity of transactions, customer history and behavior etc. However, it does not explicitly require analysis or reporting of this abnormal authentication behaviour.
3	Requirements for Scores 1 and 2, plus the following: • The Authentication Provider shall check HMG provided services for indications that the Credential maybe being used by someone other than its owner.	No published requirements.

OBSERVATION: FICAM does not include requirements at LOA Level 1 to ensure that the Authentication Provider check for indications that the Credential maybe being used by someone other than its owner.

OBSERVATION: FICAM does not include requirements at LOA Level 3 to explicitly require analysis and reporting of abnormal authentication behaviour.

RECOMMENDATION: The UK add requirements at LOA Level 2 for a capability to detect fraudulent behavior e.g. velocity of transactions, customer history and behavior etc. as well as to analyze and report this abnormal authentication behaviour.

AC Element E: Authentication Service Characteristics

Confidence in the use of a Credential, during the Authentication, is built upon the characteristics of the authentication service. The Authentication Provider shall ensure its authentication service protects the user, and itself, from compromise. The following Table demonstrates the required characteristics of the authentication service and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for the authentication service characteristics to achieve that score.

Score	GPG 44 Requirement	Observations about FICAM
1	• The Authentication Provider shall design, develop, implement and maintain the technology systems that deliver its authentication services to protect the confidentiality, integrity and availability of the information processed. • The Authentication service shall only return a success where the user has successfully authenticated using their Credential. • The Authentication service shall reject an Authentication when a suspended or revoked Credential is presented. • The Authentication service shall suspend or revoke a Credential after a number of failed Authentication attempts. • The Authentication service shall protect authentication sessions using Good Industry Practice security measures to ensure its confidentiality, integrity and authenticity and provide non-repudiation (e.g. using TLS v1.2), digital signatures FIPS 186-4. • The Authentication service shall ensure that the user can determine that they are using a secure channel to the Authentication Provider (e.g. where certificates are being used, then these are not self-signed but are signed by an industry recognised authority). • Where the Authentication service uses cryptography, then the cryptographic algorithms and keys shall be used in accordance with	LOA Level 1 does not require that the Authentication service suspend or revoke a Credential after a number of failed Authentication attempts or that the Authentication service protect authentication sessions using Good Industry Practice security measures. While LOA Level 1 requires that the transmission of data take place over a protected session it does not require the Authentication service to ensure that the user can determine that they are using a secure channel.

	current Good Industry Practice. For further information, see GPG 44 Annex B.	
2	Requirements for Score 1, plus the following: • The Authentication Provider shall use measures that are effective at preventing use by non-human operators (see Good Practice Guide 53). • The Authentication service shall use measures that prevent the observation and replay of Credentials that were used in a previous Authentication. • The Authentication service shall use methods that ensure the integrity of the information exchanged with a user. • The Authentication service shall use measures that protect the Credential from compromise, even if the communication channel is compromised.	LOA Level 3 requires measures that prevent the observation and replay of Credentials that were used in a previous Authentication and that ensure the integrity of the information exchanged with a user. However, it does not have requirements for measures that are effective at preventing use by non-human operators or that protect the Credential from compromise, even if the communication channel is compromised.
3	Requirements for Scores 1 and 2, plus the following: • The Authentication service shall use measures that detect and prevent the illegitimate use of a user's Credential.	No published requirements.

OBSERVATION: FICAM does not include requirements at LOA Level 1 and 3 that explicitly require technology systems to deliver its authentication services.

OBSERVATION: FICAM does not include requirements at LOA Level 1 to ensure that the Authentication service suspend or revoke a Credential after a number of failed Authentication attempts or that the Authentication service protect authentication sessions using Good Industry Practice security measures.

OBSERVATION: While FICAM LOA Level 1 has requirements that the transmission of data take place over a protected session it does not include requirements to ensure that

the user of the Authentication service can determine that they are using a secure channel.

OBSERVATION: FICAM does not include requirements at LOA Level 3 that check for measures that are effective at preventing use by non-human operators.

OBSERVATION: FICAM does not include requirements at LOA Level 3 that check for measures that protect the Credential from compromise, even if the communication channel is compromised.

AC Element F: Information Assurance Maturity of the Authentication Provider

The information assurance maturity of the Authentication Provider is an important element in providing confidence in the delivery of the authentication service. The following Table demonstrates the information assurance maturity requirements for the Authentication Provider and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for the information assurance maturity to achieve that score.

Score	GPG 44 Requirement	Observations about FICAM
1	• The Authentication Provider shall have an effective information security management system which protects the integrity, confidentiality and availability of its service including a forensic readiness plan. • The Authentication Provider shall have an audit regime that covers all systems supporting the use of the Credential. • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent time. • The Authentication Provider shall have a records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting	LOA Level 1 has requirements for the Authentication Provider to demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information. However, these requirements do not apply to records in general. LOA Level 1 does not require that: • an effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body be in place. • the Authentication Provider be subjected to a first-party audit at least once every 12 months for the effective provision of the specified

	the use of the Credential. • The Authentication Provider shall conduct regular risk assessments and have defined processes for exception handling. • The Authentication Provider shall have a monitoring regime that detects unexpected and undesirable activity within the service. • The Authentication Provider shall have an internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and logical access to the systems that support the authentication service.	service by internal audit functions of the enterprise responsible for the specified service. • all systems supporting the use of the Credential have a consistent time. • the Authentication Provider have a monitoring regime that detects unexpected and undesirable activity within the service it does require that it apply controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications. • the Authentication Provider conducts regular risk assessments and have defined processes for exception handling. • the Authentication Provider apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.
2	Requirements for Score 1, plus the following: • The Authentication Provider shall have an independently audited information security management system which protects the integrity and confidentiality of its service (e.g. ISO27001), including a forensic readiness plan. • The Authentication Provider shall have an independently audited audit regime that covers all systems supporting the use of its service, including a forensic readiness plan. • The Authentication Provider shall ensure that all systems supporting	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied.

	the use of the Credential have a consistent accurate time using a Good Industry Practice time source. • The Authentication Provider shall have an independently audited records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential. • The Authentication Provider shall conduct regular risk assessments, and have defined processes for exception handling, using Good Industry Practice guidance (e.g. ISO 27005). • The Authentication Provider shall have an independently audited monitoring regime that detects unexpected activity within the service. • The Authentication Provider shall test its monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered. • The Authentication Provider shall have an independently audited internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and logical access to the systems that support the authentication service. • The Authentication Provider shall test its internal monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered.	

.3	Requirements for Scores 1 and 2, plus the following: • The Authentication Provider shall have an independently certified information security management system which protects the integrity and confidentiality of its service (e.g. ISO 27001), including a forensic readiness plan. • The Authentication Provider shall have an independently certified audit regime that covers all systems supporting the use of the Credential (e.g. ISO 27001). • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent and accurate time synchronised from a Stratum 1 time source (or equivalent). • The Authentication Provider shall have an independently certified records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential (e.g. ISO 15489).	No published requirements.

OBSERVATION: FICAM does not include requirements at LOA Level 1 and 3 that address the requirements identified by the UK for information assurance maturity.

OBSERVATION: FICAM does not include requirements at LOA Level 1 that require:

- an effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, be in place.
- the Authentication Provider be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service.
- all systems supporting the use of the Credential have a consistent time.

- the Authentication Provider have a monitoring regime that detects unexpected and undesirable activity within the service it does require that it apply controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.
- the Authentication Provider conducts regular risk assessments and have defined processes for exception handling.
- the Authentication Provider apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.

GPG 45 Comparison

IPV Element A – Strength of Identity Evidence

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. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	GPG 45 Requirements	Observations about FICAM
0	No compliant Identity Evidence provided	Not applicable
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	For LOA Level 1 the service is not required to do identity checking.

	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	For LOA Level 2 the Applicant must undergo identity proofing by a trusted RA through the presentation of identifying materials or information. *In-Person Public Identity Verification* requires possession of a valid current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record. *Remote Public Identity Verification* requires possession of a valid Government ID (e.g. a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card, or tax ID).
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	**ISSUE:** *Equivalence to the identity checking requirements of The Money Laundering Regulations 2007 needs to be established.* For LOA Level 3 the Applicant must undergo identity proofing by a trusted RA through the presentation of identifying materials or information.

	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 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	*In-Person Public Identity Verification* requires that the applicant is in possession of a verified current primary Government Picture ID that contains the Applicant's picture and either address of record or nationality (e.g. driver's license or passport). *Remote Public Identity Verification* requires the applicant to be in possession of a valid Government ID (e.g. a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via records of both numbers shall be required.
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	No published requirements.

	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.	

OBSERVATION: FICAM does not include requirements at LOA Level 1 for In-Person Public Identity Proofing that meet the requirements of the UK.

RECOMMENDATION: Additional analysis is required to determine if the identity proofing activities required by FICAM to meet LOA Level 3 satisfy UK Money Laundering Regulations 2007.

IPV Element B – Outcome of the Validation of Identity Evidence

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. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	GPG 45 Requirement	Observations about FICAM
0	Validation of the Identity Evidence was unsuccessful	Not Applicable
1	All Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source	For LOA Level 1 the service is not required to do identity validation.
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	*In-Person Public Identity Verification* requires the RA to inspect the photo-ID, compare picture to Applicant, record ID number, address and date of birth (DOB). If photo ID appears valid and the photo matches Applicant then if personal information in the records includes a telephone number or email address, that can be used to send notice. Otherwise the address of record should be used. *Remote Public Identity Verification* requires the RA to inspect both photo-ID number and account number supplied by the Applicant and verify the information, including ID number OR account number, through record checks. Address/phone number confirmation and notification shall be done.

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	*In-Person Public Identity Verification* requires that the RA inspect the Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. The RA shall confirm that name, DOB, address and other personal information in the records are consistent with the application. The RA shall compare the picture to the Applicant and record the ID number. If personal information in the records includes a telephone number or email address, that can be used to send notice. Otherwise the address of record should be used. *Remote Public Identity Verification* requires the RA to verify information provided by the Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases. The RA shall confirm that name, DOB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. At a minimum, the records check for both the ID number AND the account number s shall confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.)
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	No published requirements.

	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	

OBSERVATION: FICAM does not include a requirement at LOA Level 1 that confirms all Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source.

IPV Element C – Outcome of Identity Verification

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. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	Identity Verification Outcome	Observations about FICAM
0	Unable to confirm that the Applicant is the owner of the Claimed Identity	Not Applicable
1	The Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity	For LOA Level 1 the service is not required to do confirmation.
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	For *In-Person Proofing* the RA shall inspect the photo-ID, compare picture to Applicant. In addition, if personal information in the records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at the phone number or email address associated with the Applicant in the

	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	records. If ID confirms address of record, the RA authorizes or the CSP shall issue credentials and notice shall be sent to the address of record; OR if the ID does not confirm address of record, then the CSP shall issue credentials in a manner that confirms the claimed address. For *Remote Proofing* the RA shall inspect both the ID number and account number supplied by the Applicant (e.g. for correct number of digits) and the RA shall verify the information provided by the Applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DOB, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. In addition, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in records OR if personal information in records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records.
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	For *In-Person Proofing* the RA shall inspect the Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases and confirm that name, DOB, address and other personal information in the records are

	Identity **AND** The Applicant's ownership of the Claimed Identity has been confirmed by a Static **OR** Dynamic Knowledge Based Verification	consistent with the application. In addition, if personal information in the records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at the phone number or email address associated with the Applicant in the records. If ID confirms address of record, the RA authorizes or the CSP shall issue credentials and notice shall be sent to the address of record; OR if the ID does not confirm address of record, then the CSP shall issue credentials in a manner that confirms the claimed address. For *Remote Proofing* the RA shall verify information provided by the Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases and confirm that name, DOB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. At a minimum, the records check for both the ID number AND the account number s shall confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. In addition, the CSP shall issue credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in records OR if personal information in records includes a telephone number or email address, the CSP shall issue credentials in a manner that confirms the ability of the

		Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records.
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	No published requirements.

OBSERVATION: FICAM does not include requirements at LOA Level 1 to verify that the Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity.

IPV Element D – Outcome of Counter-Fraud Checks

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. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	Counter-Fraud Checks	Observations about FICAM
0	Applicant is suspected of being, or known to be, fraudulent	Not applicable.
1	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity	For LOA Level 1 the service is not required to check that the 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	As an optional requirement the authentication process shall implement internet protocol (IP) reputation based tools (i.e., IP blacklisting capability) and anomaly detection capabilities (e.g., velocity of transactions, customer history and behavior) to mitigate fraudulent activity.
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	As an optional requirement the authentication process shall implement internet protocol (IP) reputation based tools (i.e., IP blacklisting capability) and anomaly detection capabilities (e.g., velocity of transactions, customer history and behavior) to mitigate fraudulent activity.
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	No published requirements.

	specified source(s), that the Applicant is fraudulent **AND** No confirmed evidence, using source(s) private to HMG, that the Applicant is fraudulent	

OBSERVATION: FICAM does not include requirements concerning Counter-Fraud Check processes.

RECOMMENDATION. The UK should consider adding requirements that the authentication process implement internet protocol (IP) reputation based tools (i.e., IP blacklisting capability) and anomaly detection capabilities (e.g., velocity of transactions, customer history and behavior) to mitigate fraudulent activity.

IPV Element E – Activity History of the Claimed Identity

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.

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.

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.

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.

The following table describes the scoring profile for this element.

Score	Properties of Activity History	Observations about FICAM
0	Unable to demonstrate the required Activity History	FICAM does not explicitly undertake checks of activity history for any LOA Level.
1	No demonstration of an Identity's Activity History was required	FICAM does not explicitly undertake checks of activity history for any LOA Level.
2	Claimed Identity demonstrates an Activity History of at least 180 calendar days	FICAM does not explicitly undertake checks of activity history for any LOA Level.
3	Claimed Identity demonstrates an Activity History of at least 405 calendar days	FICAM does not explicitly undertake checks of activity history for any LOA Level.
4	Claimed Identity demonstrates an Activity History of at least 1080 calendar days	No published requirement.

OBSERVATION: FICAM does not include requirements concerning the Activity History of the Claimed Identity.

Specification for Organisations Providing Proofing and Authentication of Digital Identities

Eligibility Requirement		Observa
Organisations shall demonstrate that they are able to meet the requirements of this Specification through the achievement of certification by a Certification Body in accordance with the certification specification.		FICAM
Organisations shall provide all information required by the Certification Body to meet their obligations in respect of identity proofing and authentication of individuals.		FICAM

Organisations shall provide the Certification Body with a detailed description of their Identity Assurance Service.		FICAM

Changes to Eligibility Status Requirements	Observations about FICAM
Organisations that have been suspended by one Certification Body, due to a failure to implement the requirement in this specification, shall not be allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.	FICAM does not have this requirement.
Should Identity Providers wish to transfer between certification bodies, they shall be allowed to do so subject to conditions laid down in the certification specification.	An organization, at all LOA Levels, must be assessed by a qualified Trusted Framework Provider. No other cross Trusted Framework Provider process is permitted.
Organisations shall inform their Certification Body of any significant changes on their service post certification. In such cases the Certification Body shall decide whether full recertification is required or any additional checks need to be completed. When an Organisation requests to extend their certification scope, for example Organisations that are certified to deliver services at LOA Level 2 wishing to deliver services at LOA Level 3, a full recertification audit shall be required.	FICAM must be informed of significant changes in TFP-approved entity (i.e., CSP) and identity service operations or policies that impact ongoing TFP approval or renewal (e.g., if a CSP changes privacy and security policies as a result of a merger or split, the TFP needs to notify the FICAM TFS and can be reassessed for continued approval).
Organisations shall ensure that they have arrangements to cover liability for the entirety of the Service undertaken under the scope of this Specification. Organisations shall ensure any policy is issued by an insurer included on the Financial Services Authority (FSA) register as 'Authorised', 'EEA 12 Authorised' or 'Appointed Representative' and provide the Certification Body with certificates of insurance at the initial certification,	FICAM does not have requirements to cover liability for the entirety of the Service.

surveillance audit and on renewal of any insurance policy.	
Organisations surrendering their certification under this Specification shall ensure indemnity cover of at least six years is provided for any identities proofed or authenticated. This may be in the form of an on-going indemnity policy or run off cover. Failure to comply with this requirement may result in civil action being taken against the Organisation.	FICAM does not have requirements to ensure indemnity coverage of at least six years is provided for any identities proofed or authenticated.

Robust and Credible Management Systems Requirements	Observations about FICAM
Organisations shall have documented procedures in place that can implement the requirements of this Specification and shall review their procedures in response to any change to the Identity Assurance Assessment process or this Specification.	FICAM has similar requirements.
Organisations shall have an Information Security Management System (ISMS) and demonstrate to the CB that they meet a recognised standard for ISMS e.g. ISO27001.	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied.
Organisations shall have a quality management system and demonstrate to the CB that they meet a recognised standard for Quality Management e.g. ISO9001.	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied.
All Organisations shall have written procedures for dealing with the following activities: • Control of documents; • Control of records; • Control of non-conforming services; • Corrective action; • Preventative action;	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied.

• Internal audit; • Management review.	
Organisations shall establish and maintain records in relation to each Identity Assurance Assessment undertaken containing at least the following information: • Name • Address • Date of Birth • Gender • Evidence details • The explicit consent to gather and use customer data for the service	FICAM does not maintain Gender and Evidence details as part of the basic record.
Organisations shall ensure that all information associated with the provision of the Service is securely stored for a minimum of seven years regardless of whether user chooses to cease using the identity services of the IDA. Organisations shall also make this information available to the Identity Assurance programme when requested.	A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representative. The record retention period of data is seven years and six months beyond the expiration or revocation (whichever is later) of the credential.
Organisations shall have systems to ensure compliance with the relevant data protection legislation within the UK and register with the Public Register of Data Controllers by notifying the Information Commissioner's Office (ICO). In particular, Organisations shall ensure that information obtained through the Identity Assurance process remains confidential outside of requirements to provide that information to the following parties: • The Identity Assurance Programme; • Where required, the Certification Body; • As covered by the Data Protection Act;	While organizations are required to sufficiently protect all sensitive data including Personally Identifiable Information (PII) it is not possible, at this time, to determine if this meets UK requirements.
Organisations will only process personal data in accordance with the Data Protection Act 1998, or EU Member	It is not possible, at this time, to determine if US Government requirements concerning the processing of personal

State national equivalent.	data meet UK requirements.
Organisations shall agree to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate, to allow for investigation of: • Their compliance with the requirements of this Specification; • Any on-going or completed disciplinary actions; • Complaints against the Organisation or their staff; • The outcome of any monitoring undertaken by Certification Bodies.	FICAM does not require organizations to agree to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate, to allow for investigations.

Internal Audit and Corrective Action	Observations about FICAM
Organisations shall keep a schedule of audits to be undertaken to check compliance with this Specification and shall keep records of such audits and any resulting actions. This shall ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.	While FICAM requires a review of the sufficiency of the bona fides of CSPs that must be satisfied, there are no specific requirements concerning a schedule of audits to be undertaken.
Organisations shall identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied, there are no specific requirements concerning examining the causes and consequences of any issues raised during internal audits.
Organisations shall carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.	While FICAM requires a review of the sufficiency of the bona fides of CSPs that must be satisfied, there are no specific requirements concerning carrying out corrective actions regarding particular occurrence(s) identified during internal audits.

A Comparison of Requirements: United Kingdom & United States Government

Complaints Management Requirements	Observations about FICAM
Organisations shall have in place and operate a documented complaints procedure appropriate for the following activities: • Receiving, recording, acknowledging and resolving all complaints from customers. The records shall include actions taken to resolve issues that have been the subject of a complaint and of the outcome including evidence that the complainant is satisfied with the outcome; • Receiving, recording and addressing complaints from the IDA Service. The records shall include actions taken to resolve issues that have been the subject of a complaint and of the outcome including evidence that the complainant is satisfied with the outcome; • Informing their customers what the procedures are and what further recourse is available, including informing their customers that accessing the complaints procedures does not affect their statutory rights; • Informing their Certification Body of all complaints including details of the issue(s) resolved and disclose all material correspondence and other evidence if requested; • Acknowledging a complaint within seven days and escalating the complaint if it is not resolved in line with the Service Delivery Requirements, including the customer's right to take the matter the Certification Body.	While FICAM requires a review of the sufficiency of the bona fides of CSPs that must be satisfied, there are no specific requirements concerning a documented complaints procedure.

Operational Procedures	Observations about FICAM
Organisations shall demonstrate to Certification bodies how they meet the	Organizations are not required to demonstrate that they meet the

requirements of the following documents, to the version that has been stated in the service description. • Good Practice Guide 44; • Good Practice Guide 45; • IPV Operations Manual; • Service Delivery Requirements; • Good Practice Guide 53.	requirements specified by yhr UK.
Organisations shall have a documented process to register applications that meets the requirements as defined in the latest version of the IPV Operations Manual and Service Delivery Requirements.	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied.
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, that meets the required level for IPV Element A, as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element A under GPG 45
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, is valid and meets the required level for IPV Element B as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element B under GPG 45
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, has been linked to the individual, through verification. The process shall meet the required level for IPV Element C as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element C under GPG 45
Organisations shall have a documented process to detect if the evidence supplied by a customer or the customer themselves, have indicators of fraud or fraudulent use against them. This	See IPV Element D under GPG 45

process shall include the actions required to determine whether the customer is acting fraudulently or not and the reporting mechanisms both internally and externally as required. The process shall meet the required level for IP Element D as defined in the latest version of GPG 45 and IPV Operations Manual.	
Organisations shall have a documented process to determine that the activity history of the identity has been checked to the required level for IPV Element E as defined in the latest version of GPG 45 and IPV Operations Manual.	See IPV Element E under GPG 45
Organisations shall have a documented process to determine that the authentication mechanism used to identify a returning customer meets the required level as defined in the latest version of GPG 44 and IPV Operations Manual.	See GPG 44
Organisations will have documented processes for the management of authentication including issuance, activation, misuse detection, revocation, and renewal, as defined in the latest version of GPG 44 and IPV Operations Manual.	See GPG 44
Organisations shall have a documented process for Transactional Monitoring of the use of the credential and the identity when they are interacting with a customer as defined in the latest version of GPG 44 and GPG 53.	See GPG 44
Organisations shall have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service. This will include other systems within the Organisation that interconnects or impacts on the IDA Service.	While FICAM requires a review of the sufficiency of the bona fides of CSPs there are no specific requirements that must be satisfied concerning a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service.

Organisations shall have documented procedures to meet the requirements laid down within the latest version of the Operations Manual.	See GPG 45.
Organisations shall have documented procedures to meet the requirements laid down within the latest version of the Service Delivery Requirements.	See Service Delivery Requirements.
Organisations shall demonstrate to the Auditors, how these processes are implemented and demonstrate their compliance with their own processes.	An organization must meet this requirement in order to be approved.

OBSERVATION: FICAM does not include requirements to requirements to cover liability for the entirety of the Service.

OBSERVATION: FICAM does not include requirements to ensure that an organization that has been suspended by one Certification Body, due to a failure to implement the requirement in this specification, shall not be allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.

OBSERVATION: FICAM does not include Gender and Evidence details in the records associated with each Identity Assurance Assessment undertaken OR the UK could make the capture of Gender and Evidence details optional.

OBSERVATION: FICAM does not include requirements to ensure that an organization has written procedures for Control of documents, Control of records, Control of non-conforming services, Corrective action, Preventative action, Internal audit, and Management review.

OBSERVATION: FICAM does not include requirements to ensure that an organization has a quality management system and that they meet a recognised standard for Quality Management (e.g. ISO9001).

OBSERVATION: FICAM does not include requirements to ensure that an organization has an Information Security Management System (ISMS) and that they meet a recognised standard for ISMS (e.g. ISO27001).

OBSERVATION: FICAM does not include requirements to ensure that an organization agrees to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate.

OBSERVATION: FICAM does not include requirements to ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.

OBSERVATION: FICAM does not include requirements to ensure that an organization is required to identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.

OBSERVATION: FICAM does not include requirements to ensure that an organization is required to carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.

OBSERVATION: FICAM does not include requirements to ensure that an organization is required to have in place and operate a documented complaints procedure.

OBSERVATION: FICAM does not include requirements to ensure that an organization is required to have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service

OBSERVATION: FICAM does not include requirements to register applications that meets the requirements as defined in FICAM's equivalent to the IPV Operations Manual and Service Delivery Requirements.

RECOMMENDATION: Determine if US Government requirements concerning protecting all sensitive data, including Personally Identifiable Information (PII), meet UK requirements.

RECOMMENDATION: Determine if US Government requirements concerning the processing of personal data meet UK requirements.

Specification for Certification Bodies Certifying Identity Assurance Providers

Certification Bodies must achieve United Kingdom Accreditation Service (UKAS) accreditation against BS EN ISO/IEC 17065 which consists of the following 13 steps / requirements: • General • Application • Application Review • Evaluation • Review • Certification Decision	The US Government considers the assessment and adoption of Trust Framework Providers (TFPs) to be critical to the success of the FICAM. A TFP is an organization that defines a Trust Framework and then certifies CSPs compliant with that Trust Framework. Adoption means that any identity service certified by that TFP is qualified to provide identity assertions to federal agencies. During the assessment of a TFP two comparability assessments are conducted:

• Certification Documentation
• Directory of Certified Products
• Surveillance
• Changes Affecting Certification
• Termination, Reduction, Suspension or Withdrawl of Certification
• Records
• Complaints and Appeals
	• Trust Criteria Assessment – determination that the criteria applied by the TFP to its member CSPs are comparable to Identity, Credential, and Access Management (ICAM) criteria. Trust criteria assessment includes:
	  • Technical policy and privacy policy comparability based upon defined trust criteria;
	  • Determination of whether the TFP sufficiently reviews member CSP bona fides to ensure member CSP organizational maturity, legitimacy, stability, and reputation.
	• Audit Criteria Assessment – determination of adequacy of:
	  • TFP auditor qualifications. At a minimum, the TFP's auditors must:
	  • Demonstrate competence in the field of compliance audits;
	  • Be thoroughly familiar with all requirements that the TFP imposes on member CSPs;
	  • Perform such audits as a regular ongoing business activity; and
	  • Be Certified Information System Auditors (CISA) and IT security specialist – or equivalent.
	  • TFP processes used to audit its member CSPs; and
	  • Ongoing TFP processes used to re-certify member CSPs.

NOTES:

It is unclear from the level of detail provided that the US Government TFPAP could benefit from requiring accreditation against BS EN ISO/IEC 17065.

REVISION HISTORY

0.1	April 10, 2015	Initial Draft
0.2	April 30, 2015	Revised based on revision of Authentication Level of Assurance mapping