TISA

Enabling Financial Services use of GPG45 Proofing Techniques

Nick Mothershaw

22nd August 2023 v1.0

About TISA

The Investing and Saving Alliance (TISA) is a unique, rapidly growing membership organisation for UK financial services.

Our ambition is to improve the financial wellbeing of all UK consumers. We do this by focusing the convening the power of our broad industry membership base around the key issues to deliver practical solutions and devise innovative, evidence-based strategic proposals for government, policy makers and regulators that address major consumer issues.

TISA membership is representative of **all sectors of the financial services industry.** We have **over 240-member firms involved in the supply and distribution of savings, investment products and associated services**, including the UK's major investment managers, retail banks, online platforms, insurance companies, pension providers, distributors, building societies, wealth managers, third party administrators, Fintech businesses, financial consultants, financial advisers, industry infrastructure providers and stockbrokers.

As consumers, the financial services industry and the economy react to and recover from the effects of the pandemic, the importance of the three key pillars of work that TISA prioritises has never been more apparent:

- **Strategic policy initiatives** regarding the financial wellbeing of UK consumers & thereby enhancing the environment within which the industry operates in the key areas of **consumer guidance, retirement planning, later lifetime lending, vulnerable customers, financial education, savings and investments**.

- TISA is recognised for the **expert technical support provided to members** on a range of operational and regulatory issues targeted at improving infrastructure and processes, establishing standards of good practice and the interpretation and implementation of new rules and regulations covering **MiFID II, CASS, ESG/RSI, operational resilience, Cyber Risk, SM&CR** and a range of other areas.

- **Digital transformation initiatives** that are driving ground-breaking innovation and the development of industry infrastructure for greater operational effectiveness and revenue promoting opportunity for firms. TISA has become a major industry delivery organisation for consumer focused, digital industry infrastructure initiatives – **TISAtech** (a digital marketplace that brings together financial institutions and FinTechs for greater collaboration and innovation) and **TURN** (TISA Universal Reporting Network – a digital platform providing a secure data exchange for financial services using blockchain technology) – alongside projects **Digital ID** and **Open Savings & Investment**. This reflects TISA's commitment to open standards and independent governance.

1 Introduction

The creation of the Digital Identity and Attributes Trust Framework (DIATF) in the UK introduces a much-needed benchmark for identity proofing techniques through its good practice guide (GPG) 45 “How to prove and verify someone’s identity”.

GPG45 introduces guidelines for validation of an ID through document scanning and verification of ID through biometric cross match on an image of the user to the image recorded on an ID document. This is a rapidly evolving area of ID proofing that financial services firms have had to quality test themselves. Through inclusion of these proofing approaches in guidelines and the simultaneous introduction of certification to the guidelines, financial services firms should be able to accept these proofing techniques with the confidence that they have been independently tested to a high standard.

For many years financial services has used the Joint Money Laundering Steering Group (JMLSG) guidelines for ID proofing in the context of AML KYC checks. These guidelines cover proofing approaches for both manual checking of ID evidence and electronic evidence. The guidelines have been in place for many years and allow financial services to take a risk-based approach to ID proofing. The JMLSG guidelines do not however really cover the afore mentioned more modern ID proofing methods of document scanning and biometric image cross matching. There is an opportunity to extend the JMLSG guidelines to more clearly reference these techniques and refer to the detail now provided in GPG45 as to how these techniques should be benchmarked.

GPG45 introduces more detail on how proofing techniques should be undertaken. The certification approach to the DIATF involves an independent certification body assessing the proofing techniques and ID Provider offers and determining if they meet the requirements of GPG45. This is very useful for financial services as they can then be confident that an ID Provider is working to a defined level of quality.

JMLSG and GPG45 guidelines both:

- List documents and other evidence that are acceptable for ID proofing.
- Lists acceptable validation and verification (risk of impersonation) techniques for proofing the user.

JMLSG guidelines allows financial services providers to choose which evidence, validation and verification techniques meet their needs based on risk, channel and their user demographic.

2 The Challenge with GPG45 Levels of Confidence

GPG45 introduces the concept of levels of confidence. Different validation and verification techniques are scored and combined via profiles to achieve a level of confidence. When an ID Provider is certified to the DIATF, they are awarded certification to a level of confidence.

The problem with the level of confidence concept is that the actual evidence, validation, and verification techniques used to achieve the profile is not transparent to the relying party. This is an issue for financial service providers who are working to the JMLSG guidelines as:

- some evidence, validation and verification techniques supported in GPG45 are not acceptable for financial services (e.g. knowledge based verification)
- the combinations of proofing techniques that go to make up profiles are not the same combinations that financial services make under the JMLSG guidelines to meet their risk-based proofing assessments.
- the evidence used in ID Proofing must be understood and recorded for record keeping purposes.

The following considerations illustrate why finance services cannot rely on a GPG45 level of confidence:

1. **Use of single pieces for evidence to achieve a level of confidence.**

JMLSG guidelines do permit the check of a single physical document. However, many organizations simply won't accept a single document proof and require a second proof. When using electronic evidence, JMLSG guidelines recommend multiple evidences are used to proof the user: *"5.3.50 - An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register, or at a single point in time), is not normally enough on its own to verify identity, although it may be sufficient where, for example, the source has been issued by a government authority and contains cryptographic security features".* So, a passport that is cryptographically read is acceptable, but cannot meet the requirements of financial service firms as it does not contain address.

GPG45 profiles allow achievement of a level of confidence using a single piece of evidence. This is usually:

Evidence	**Position regarding JMLSG guidelines**
Passport	Does not contain address, which financial services firms always seek to validate
Driving Licence	Theoretically acceptable as a single physical document proof as includes address, but rarely accepted without supplementary proofs. As electronic evidence, it would need to be accompanied by a second proof.
Bank Account	Regarded as reliance under AML guidelines

2. **Use of knowledge-based verification**

A GPG45 level of confidence may have been achieved using KBVs. Whilst JMLSG guidelines do support the use of this technique the vast majority of financial services firms do not accept it as:

- it is perceived as vulnerable to ID theft due to the use of evidence that comes primarily from credit reference agencies. If KBVs are extended in future to cover a greater variety of data sources (e.g., government data) then attitudes to KBVs in financial services may change, but this will take some time.
- KBVs are too hard for users to answer correctly, leading to high levels of abandonment in the proofing process.

3. Absences of key evidence options

The JMLSG guidelines permits some commonly used evidence that are not part of GPG45 (e.g. Electoral Roll). In order not to exclude users who can get through financial services firms proofing approaches today, it is necessary to overlay additional permitted evidence options into the process that the GPG45 profiles do not recognise.

In summary, GPG45 introduces much more detailed guidelines for proofing, which is welcomed by financial services, but the level of confidence approach also introduced does not work for financial services due to the lack of transparency of evidence and proofing techniques.

3 The Way Forward – Transparency of Evidence and Proofing Techniques

This paper proposes that the way forward is to introduce the required transparency of evidence and proofing technique used into GPG45 and into the certifications that ID Providers receive.

Financial Services firms, or Overlay Schemes specialising in financial services, can then assemble GPG45 certified proofing components to meet their needs on a risk-based basis per the prevailing guidelines.

This also has an inclusion benefit, as finance services firms and schemes can ensure that they choose a mix of ID providers that offer an inclusive range of ID proofing techniques, including ID documents, electronic evidence, paper evidence and vouching; for UK and non-UK residents.

The JMLSG guidelines could then be updated to reference GPG45. The JMLSG guidelines could state that readers who are dealing with a DIATF certified ID Provider can map the requirements in the JMLSG guidelines to GPG45 evidence proofing techniques published in the DIATF. This can be a high-level update to the JMLSG guidelines referring to the use of GPG45 evidence and proofing techniques. JMLSG does not need to go so far as to specifically cross-referencing actual GPG45 proofing techniques against the detailed JMLSG guidance (various paragraphs in Part 1 5.3.36-89); financial services firms, or schemes such as ID Connect, can make this cross reference for themselves.

JMLSG Guidelines may also still reference other acceptable evidence for financial services that are not referenced in GPG45, such as electoral roll.

As part of the certification process to the DIATF ID Providers are already assessed on an evidence and proofing technique basis, so introducing this level of transparency on ID Provider certifications should not be too much of an overhead.

Also, the DIATF already supports the communication of proofing techniques used as ‘check methods' with the data schema referenced in section 15.1 Making your products and services interoperable.

GPG45 levels of confidence achieved should also be listed as part of the certification, this paper does not suggest they are removed. They are important for ID interoperability across sectors, as other markets and use cases that do not have the existing processes financial services work to in place may choose to adopt these, and as the Digital ID market matures and trust in Digital IDs grows accordingly financial services may move to use these in due course.

The introduction of evidence and proofing techniques transparency will allow financial services firms and schemes to show how they meet the guidelines by listing the proofing techniques and evidence they accept.

The table in the appendix shows how this would work in the context of several JMLSG compliant combinations of proofing techniques that the TISA ID Connect scheme will support.

4 Recommendations

This paper makes the following recommendations:

- **DSIT introduce the required transparency into GPG45 and into the certifications ID Providers receive**.
- JMLSG updates the JMLSG guidelines at a high level to allow readers, when appropriate, to map the requirements in the JMLSG guidelines to GPG45 proofing techniques published in the DIATF. This can be a fairly high-level update to the JMLSG guidelines; detailed cross reference of JMLSG requirements to GPG45 techniques should be left to implementing financial services firms or schemes
- JMLSG guidelines are extended to include clearer references to ID proofing techniques of Document Scanning and Biometric Image Cross Matching, with reference to the detailed techniques benchmarked in GPG45.

5 APPENDIX: TISA ID Connect PILOT – Example ID Proofing Options

The following are examples of ID proofing options supported in the ID Connect scheme. References to Evidence and Proofing techniques are highlighted in yellow

Method		**Scanned Passport with separate Address Verification via Electronic Evidence**
Validation Evidence 1	**Proving the User Exists**	Cryptographic chip read of passport by an identity provider app on the user's phone using NFC Must be in the same session as the selfie taken to prove the user is who they are claiming to be, thus ensuring possession of the driving licence by the genuine user.
	Evidence	Passport
	Proofing Technique	Document Scanning
	JMLSG Guideline Compliance	The Passport is a physical document permitted for use under section 5.3.75 list of single documents. The Passport confirms the users name and date of birth.
Validation Evidence 2	**Proving the User Exists**	Electronic Evidence that confirms the address of the user
	Evidence	Electoral Roll, Credit Reference Agency, Utilities
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	The Electronic Evidence confirms the users name, self-entered address and date of birth as "positive information" per section 5.3.47 of the JMLSG guidelines.
Verification and Mitigation of Impersonation Risk	**Proving the user is who they Claim to Be**	The ID Provider cross checks a selfie image of the user with the image taken from the face of the document using GPG45 guidance.
	Proofing Technique	Biometric Image Cross Match
	JMLSG Guideline Compliance – Electronic Evidence/ Digital ID	Uses biometric information to ensure the applicant is who they claim to be per 5.3.44

	JMLSG Guideline Compliance - Mitigation of Impersonation Risk	Additional verification check for customer who is not physically present under section 5.3.89: “requesting the applicant to confirm a … biometric factor that links him/her incontrovertibly to the claimed electronic/digital”

Method		NFC read Passport with Separate Address Verification
Validation Evidence 1	Proving the User Exists	Scan/Picture of Photocard Driving Licence or UK Biometric Residency Permit using natural light. Must be in the same session as the selfie taken to prove the user is who they are claiming to be, thus ensuring possession of the driving licence by the genuine user.
	Evidence	Passport
	Proofing Technique	NFC Document Read
	JMLSG Guideline Compliance	The Passport is a physical document permitted for use under section 5.3.75 list of single documents. The Passport confirms the users name and date of birth.
Validation Evidence 2	Proving the User Exists	Electronic Evidence that confirms the address of the user
	Evidence	Electoral Roll, Credit Reference Agency, Utilities
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	The Electronic Evidence confirms the users name, self-entered address and date of birth as “positive information” per section 5.3.47 of the JMLSG guidelines.
Verification and Mitigation of Impersonation Risk	Proving the user is who they Claim to Be	The ID Provider cross checks a selfie image of the user with the image taken from the face of the document using GPG45 guidance.
	Proofing Technique	Biometric Image Cross Match
	JMLSG Guideline Compliance – Electronic Evidence/ Digital ID	Uses biometric information to ensure the applicant is who they claim to be per 5.3.44
	JMLSG Guideline Compliance - Mitigation of Impersonation Risk	Additional verification check for customer who is not physically present under section 5.3.89: “requesting the applicant to confirm a … biometric factor that links him/her incontrovertibly to the claimed electronic/digital”

Method		Online Banking Logon and Electronic Evidence validation proof
Validation Evidence 1	**Proving the User Exists**	User self enters name, address, and date of birth. User then logs on to online banking by the user and agreed to release their account number and sort code to the identity provider. The identify provider checks that the name, address, date of birth, sort code and account number match Electronic Evidence held in a commercial bank account verification service.
	Evidence	Bank Account
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	Matching the sort code and account number returned from the online banking logon with the user provided name, address, and date of birth against a commercial bank account verification service proves that this bank account is in the name user of the user being proofed. The fact that the user can logon to the bank account to release the sort code and account number information proves this is the user who owns this bank account.
Validation Evidence 2	**Proving the User Exists**	Electronic Evidence that confirms the address of the user
	Evidence	Electoral Roll, Credit Reference Agency (must not use same bank as Evidence 1), Utilities
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	The Electronic Evidence confirms the users name, self-entered address and date of birth as "positive information" per section 5.3.47 of the JMLSG guidelines.
Verification and Mitigation of Impersonation Risk	**Proving the user is who they Claim to Be**	Matching the sort code and account number returned from the online banking logon with the user provided name, address, and date of birth against a commercial bank account verification service proves that this bank account is in the name user of the user being proofed. The fact that the user can logon to the bank account to release the sort code and account number information proves this is the user who owns this bank account.
	Proofing Technique	Authorised Logon to Account (Auth)
	JMLSG Guideline Compliance – Electronic Evidence/ Digital ID	Uses biometric information, private information or codes to ensure the applicant is who they claim to be per 5.3.44
	JMLSG Guideline Compliance - Mitigation of Impersonation Risk	Additional verification check for customer who is not physically present under section 5.3.89: "requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs, digital signing by a qualified

		trust service certificate or other secret data may be … through a verified bank account. AND From 5.2.90: internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other secure authentication means which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address.

Note: The second piece of Electronic Evidence from a non-bank source mitigates against reliance.

Method		**Two Electronic Evidence validation proofs and Knowledge Based Verification**
Validation Evidence 1	**Proving the User Exists**	The user enters their name, address, and date of birth. The identity provider obtains two matches on Electronic Evidence from separate authoritative sources. Either 2 x account information from a credit reference agency from different credit account providers, or 1 x account information from a credit reference agency and a match on electoral roll.
	Evidence	Electoral Roll, Credit Reference Agency, Utilities
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	The Electronic Evidence confirms the users name, address, and date of birth as "positive information" per section 5.3.47 of the JMLSG guidelines. The check uses "data from multiple sources" per section 5.3.50 of the JMLSG guidelines.
Validation Evidence 2	**Proving the User Exists**	The user enters their name, address, and date of birth. The identity provider obtains two matches on Electronic Evidence from separate authoritative sources. Either 2 x account information from a credit reference agency from different credit account providers, or 1 x account information from a credit reference agency and a match on electoral roll.
	Evidence	Electoral Roll, Credit Reference Agency, Utilities
	Proofing Technique	Authoritative Source Validation
	JMLSG Guideline Compliance	The Electronic Evidence confirms the users name, address, and date of birth as "positive information" per section 5.3.47 of the JMLSG guidelines. The check uses "data from multiple sources" per section 5.3.50 of the JMLSG guidelines.
Verification and Mitigation of	**Proving the user is who they Claim to Be**	The identity provider will ask the users to answer several knowledge-based verification questions. Questions must come from different sources and must achieve a verification score of 2 under GPG45.
	Proofing Technique	KBV

Impersonation Risk	**JMLSG Guideline Compliance – Electronic Evidence/ Digital ID**	Uses private information to ensure the applicant is who they claim to be per 5.3.44
	JMLSG Guideline Compliance - Mitigation of Impersonation Risk	Verifies “with the customer additional aspects of his identity … which are held electronically” per 5.3.89.