tScheme Trust Services

OIX OPEN IDENTITY EXCHANGE White Paper

Self Certification and Mandatory Assessment Regimes - A Parallel Review

Author: Jim Lound (Jim Lound Consultancy Limited)

November 2018

Contents

Executive Summary

This paper explores the features of two different certification regimes in the context of Open Banking and GOV.UK Verify. Open Banking has adopted a self assessment approach whilst GOV.UK Verify has prescribed the use of mandatory independent assessments. It is intended that the reader will be able to formulate their own views on the merits of each approach.

The introduction of major schemes designed to enhance competition, improve individual's online productivity, make things work better (such as removing friction and effort, risk and cost) and to increase online safety (such as secure transmission and assurance about transactions and data contained in them), all have one theme in common - they all need to have the confidence of all the stakeholders to be successful and sustainable.

In August 2016, the CMA ruled that the nine largest current account providers in the UK should allow direct access to their data, including transactions, thereby allowing their customers to have ownership and control of their own data to use with other financial services organisations. The Open Banking initiative is designed to create more competition, making it easier for smaller and newer banks to compete with the older, larger banks. The Open Banking Implementation Entity (OBIE) was set up and is governed by the CMA and is funded by the nine banks. Open Banking went live in the UK in January 2018.

GOV.UK Verify allows the citizen to create one or more sets of credentials and link them to an assured digital identity using one or more of the identity providers associated with the scheme. The citizen is then able to use their assured digital identity with any of the 15 government services that rely on GOV.UK Verify, whilst transacting online. GDS state that 2.9 million citizens have signed up to GOV.UK Verify. The service was delivered into private beta in February 2014 and then into public beta in October 2014, becoming officially recognised as a live service in May 2016.

Schemes impacting consumers and citizens in relation to the acquisition, use and storage of their personal data and the initiation of payments, need to have the confidence of all the stakeholders involved in order for the scheme to be successful.

In order to establish an appropriate level of confidence, the scheme has to create 'the rules of the road' that define what 'good' looks like. Having published the rules of the road, the participating organisations need to be able to demonstrate the degree to which they comply with the requirements of the scheme. Those organisations that satisfy the scheme's requirements should then be able to continue to be a member of the scheme as a certified entity.

The degree of effort and cost to achieve certification needs to be proportionate to the risks inherent within the service and the reputational risk of being associated with the scheme itself.

Can a voluntary self certification scheme that is subject to peer review, where the certification is undertaken once and once only and does not expire, be sufficient to protect the reputation of Open Banking and the customers whose data is being accessed and used?

Does GOV.UK Verify need independent annual assessments of each IdP's services and operations against a profile and certification regime that can get underneath what the organisation really does in practice day to day?

Chapter 1 - Introduction

The introduction of major schemes designed to enhance competition, improve individual's online productivity, make things work better (such as removing friction and effort, risk and cost) and to increase online safety (such as secure transmission and assurance about transactions and data contained in them), all have one theme in common - they all need to have the confidence of all the stakeholders to be successful and sustainable.

The major schemes being alluded to here are: -

- Competition & Markets Authority (CMA) & Open Banking
- Government Digital Service (GDS) & GOV.UK Verify
- Office of Gas & Electric Markets (Ofgem) & Smart Meters
- Department for Digital Culture Media & Sport (DCMS) & Child Safety Online
- Department for Work & Pensions (DWP) & Pensions Dashboard

This paper is going to focus on two of these schemes - Open Banking and GOV.UK Verify

What is Open Banking?

In October 2015 the European Parliament introduced PSD2 (a second version of the Payments Services Directive). Within PSD2 are rules aimed at promoting innovation in the financial services sector with reference to open banking. Open banking refers to the use of Open APIs that allow third party organisations to build applications and services aimed at consumers having more control of their financial data and the means of authorising and making payments. This is consistent with the shift towards the individual having greater control over the data about them and their life, as reflected in GDPR, for example.

In August 2016, the CMA ruled that the nine largest current account providers in the UK should allow direct access to their data, including transactions, thereby allowing their customers to have ownership and control of their own data to use with other financial services organisations. The Open Banking initiative is designed to create more competition, making it easier for smaller and newer banks to compete with the older, larger banks. The Open Banking Implementation Entity (OBIE) was set up and is governed by the CMA and is funded by the nine banks.

Open Banking went live in the UK in January 2018.

How Does It Work?

As an example, when the consumer uses an online comparison site to recommend and almost approve a credit product such as credit card, the financial information available to the comparison site used to be constrained to the consumers own self asserted data that they enter e.g. salary and the data made available, via the consumer's consent, from a credit reference agency. With the advent of Open Banking, the consumer can now elect to add in the banking data from one or more of the banks live in the scheme to enable the credit risk

assessment to be enhanced with, for example, the credit and debit turnover from their current account(s).

At the point in the journey when the comparison site offers to allow the consumer to use their 'open banking data' the consumer will indicate which banks they have an account with and wish to utilise the associated data. In turn, the consumer will be asked to log in to their bank using their existing banking credentials. The comparison site will receive a token from each bank that allows the site to retrieve the consumers data for use in the credit risk assessment.

Organisations supporting this type of service are referred to as AISPs (Account Information Service Providers). The types of services also include money management tools, personal data stores, provision of quicker and more accurate access to financial products and speeding up manual processes such as applying for a mortgage, a loan etc. AISPs cannot move a consumer's money.

A second example would be where the consumer has a secure payment app on their smartphone which is associated with a Trusted Third Party (TTP) utilising the Open Banking Request for Payment APIs. When the consumer wishes to pay for goods online, the retailer would send a request for payment to the TTP and the payment app would allow the consumer to select the bank account they wish to use for the transaction and authorise the payment. This would remove the need to enter the details of a debit card, for example, and would allow the consumer to select the most appropriate account to make the payment from. This type of service could also give the user instant checkout with retailers the consumer regularly visits online.

Organisations supporting this type of service are referred to as PISPs (Payment Initiation Service Providers). PISPs can ask for permission to connect to a bank account and initiate payments on the consumer's behalf, from their bank account. The types of service would also extend to an app that helps the consumer manage their money in their various savings and current accounts to ensure they never go overdrawn and thereby avoid potentially hefty overdraft fees.

What is GOV.UK Verify?

The Identity Card Act 2006 was repealed by the Identity Documents Act 2010 instigated by the Coalition Government at the time. The Identity Card Act had established a single national identity database referred to as the National Identity Register which was closed down.

A new digital identity assurance programme began with the DWP OJEU notice issued on 28th February 2012 for the provision of identity assurance at DWP level 2 assurance. Subsequently, DWP novated the contract and procurement to Government Digital Service and GDS went out to tender for Identity Providers (IdPs) to create what would become referred to as GOV.UK Verify.

The service was delivered into private beta in February 2014 and then into public beta in October 2014, becoming officially recognised as live in May 2016.

The programme had an objective of creating a market of identity providers that the government and citizens could draw upon to get citizens' identities assured to the level

required. The scheme was designed so that there was not a single database of identities (unlike the Identity Card Act).

There are 15 government services that have signed up to be relying parties of the GOV.UK Verify scheme. These services are associated with a number of government departments including HMRC, DWP, DVLA, DEFRA.

From the citizen perspective, GOV.UK Verify allows the citizen to create a one or more sets of credentials and link them to an assured digital identity using one or more of the identity providers associated with the scheme. The citizen is then able to use their assured digital identity with any of the 15 services, whilst transacting online. GDS state that 2.9 million citizens have signed up to GOV.UK Verify. The transactions activity, post gaining access to a service, are not covered by GOV.UK Verify, so citizens are still required to fill in forms online and self assert other information about themselves that is required by the service they are working with.

How Does It Work?

The journey for the citizen starts at the government service where the option to use GOV.UK Verify will have been engineered into the process and the citizen will be able to click on the GOV.UK Verify selection 'button'. Having selected Verify, the citizen will be redirected to the Verify hub (essentially a web page that runs a process). For new users, the journey will take the citizen through a series of steps designed to present the best selection of IdPs that meet their circumstances in terms of identity evidence and access to a mobile or smartphone.

When the citizen chooses their IdP, the citizen is redirected to the IdP where they go through an identity proofing process and credential set up procedure. At this point they have created a GOV.UK Verify assured digital identity with the IdP and a set of credentials for logging in thereafter.

The citizen is redirected back to the government service via the Verify hub and continues with the government service journey. The government service receives a set of identity attributes relating to the citizen and confirmation that the citizen has attained the correct level of identity assurance. These attributes are used to match the citizen to an existing record they have but it may require the citizen to answer more questions. Once matched this step should not be needed to be done in the future.

The government service does not know which IdP the citizen has used and the IdP does not know which government service the citizen came from and was returned to.

There are currently two levels of identity assurance supported by GOV.UK Verify, LoA1 and LoA2. As part of the onboarding process for a new service using GOV.UK Verify, the government service will choose the appropriate level(s) of assurance to meet the identity risks associated with the service(s) that the citizen can utilise their Verify digital identity with.

Where the citizen already has a Verify digital identity, the citizen will indicate this in the Verify hub. The citizen will select the relevant IdP and be redirected to the IdP. The citizen will authenticate using their set of credentials and if the level of assurance they hold matches the service providers requirement they will be redirected as a successful assertion back to the

government service. If their level of assurance needs to be increased they will have to complete additional assurance checks.

Assured identities under the scheme need to be maintained, this involves a number of factors not least elapsed time since last used and consideration of specific events that may require renewal of assurance of the identity linked to the set of credentials.

Chapter 2 - What are the Objectives of Certification?

For a scheme to be successful it needs to have the full confidence of all the stakeholders affected by or involved in the scheme.

These stakeholders would include, for example: -

- Citizens / consumers who give their permission to allow the scheme to work
- Instigators of the scheme e.g. UK Government - CMA, Cabinet Office
- Regulatory bodies e.g. FCA, GDS
- Organisations responsible for operating the scheme e.g. AISPs, PISPs, IdPs and Fintech companies who facilitate these processes
- Custodians of personal data who allow the personal data to be passed to relying party organisations e.g. Banks, IdPs, personal data store providers
- Relying party organisations who utilise the citizens/consumers data to make decisions & recommendations

For Individuals

A key objective of certification is to ensure that individuals utilising the scheme are adequately protected from having their identity hijacked and their personal data from being misappropriated or misused for reasons not approved, thereby mitigating the risk of potential financial loss and a compromised personal identity or loss of privacy.

Personal data is not spent once like money, it can be used again and again and where used inappropriately can create lasting harm that is hard to recover from. Compromised data can act as a gateway to a broad range of fraud issues as well as loss of privacy, credit ratings and access and control of identity.

Individuals need to have confidence in the scheme in terms of how their data is being utilised, what is being stored, how it is being stored, what it is being used for. Default safe should be the core objective.

The risks and trust in the attributes being shared as part of the scheme is a key area to consider. How do you know that the data has not been modified in transit? Is there any level of warrant or trust implied by the source and is it being maintained and current?

It is recognised that some regulations can appear to conflict e.g. PSD2 and GDPR, where the first is looking to open up sensitive data and the second is about protecting sensitive data. Both, however, agree on the need for consent.

Even where a regulation cannot be influenced by other regulations, GDPR is a regulation that organisations must consider carefully in the context of ensuring these requirements can be met: -

- Transparency of data usage including sharing with third parties covering use by whom, for what purpose, when it was used, how it was processed and where

- Informed Consent - clear specific approval for the use of their data in one or more given contexts
- Data portability - machine readable, available via API's which means the data needs metadata about itself to travel with the data
- Right to be forgotten - as a minimum not to be included in datasets or search results even if retention is legally required of the data
- Right not to be processed by an Algorithm or to have the algorithms decisions explained

For Organisations

Organisations engaging in the scheme need to be confident there is a level playing field and that everyone is operating by the same rule book and no-one is gaining advantage at the expense of others by for example: -

- Using the consumer's data inappropriately
    - Within the scheme
    - Outside of the scheme.
- Offering services inappropriately outside of the scheme rules
- Cutting corners and thereby bypassing the rules to: -
    - Reduce their costs
    - Achieve the contractual service levels
    - Maximise revenues
    - Improve the customer experience
    - Increase market share

Certification is much more than just complying with the scheme's standards (technical, & processes) and regulatory approval.

Certification is about trust in the motives of the organisations engaging in the scheme and their intents in terms of the service they offer and how they really operate.

Organisations can become more confident that their contractual obligations, associated with the scheme, can be met by becoming certified.

For Government & Regulators

Using independent accredited certification benefits Government and Regulators by: -

- Allowing Regulators to define the overall policy for the scheme and the specific technical requirements and then allow the accredited certification bodies in the private sector to determine the organisation's level of compliance
- Removing the reliance on and risk in simply taking the word of an organisation and trusting them to deliver a compliant service. All too often brands claim that they would not risk their brand reputation to do otherwise but in reality the evidence shows that they do and all too often fail for a variety of reasons such as people, processes and internal policy. Without consequences comes complacency and damage to those who should be protected
- Ensuring risks are recognised and mitigated appropriately e.g. ensuring the risk associated with the theft of data from devices and the risk of a device being infected or taken control of are equally recognised
- Increasing public confidence because accredited certification is a recognisable way of demonstrating conformity
- Increasing confidence of relying parties and between scheme members
- Providing confidence on which to base public sector procurement decisions
- Provide confidence on which anyone entering a scheme can be independently assessed thereby opening up markets and opportunities via level playing field
- Reduce the extent to which Regulators to employ its own audit personnel

Examples of Certification Schemes

- Carbon Trust https://www.carbontrust.com/client-services/#service-1130
- EuroPrise https://www.european-privacy-seal.eu/EPS-en/Home
- FairData https://www.fairdata.org.uk/why-fair-data/
- Fairtrade https://www.fairtrade.org.uk/What-is-Fairtrade
- Investors in People https://www.investorsinpeople.com/solutions-accreditation/
- OpenID Foundation https://openid.net/certification/
- TrustMark https://www.trustmark.org.uk/privacy-policy
- tScheme https://www.tscheme.org/
- ISO27001 Information Security Management Systems https://www.iso.org/isoiec-27001-information-security.html

Chapter 3 - Overview of Open Banking Self Certification

The core elements of the Open Banking self certification regime are: -

Standards

- Technical specifications
- Security Profile
- Customer experience guidelines
- Conformance & certification

Specifications

- Open Data API specifications
- Read / Write Data API specifications
- Directory specifications

'How To' Specifications

- Guidelines for Read / Write participants
- Enrolling on to the Open Banking Directory
- Consent Model Guidelines - Implementation & User experience
- Deep linking for App-to-App redirection
- API Release Management Policy
- Open Banking Directory Usage (Directory Sandbox)
- Entity specific tailored guidance designed to help TPPs understand

Reference Applications

Providing test resources for the Account Service Payment Service Providers (ASPSPs) consisting of: -

- AISPs - Account Information Service Providers
- PISPs - Payment Initiation Service Providers

Liability & Consumer Protection

The Financial Conduct Authority (FCA) already mandates protection for the payment initiation assets, for example via the new Credit Card rules introduced in March 2018 and the existing Direct Debit Guarantee.

Non Mandatory OIDF Self Certification Test

The OBIE has adopted the OpenID Foundation (OIDF) specification and certification programme. Providers and Relying Parties (PISPs and AISPs) can, if they wish, elect to undertake tests for each profile adopted. The tests are undertaken by the organisation and the results are signed and submitted to the OIDF to attain certification. The organisation is making a formal declaration that their implementation conforms to the appropriate test. The certification does not expire.

Non Mandatory Peer Review of Test Results

The OBIE makes the results of the tests available for peer review. These results are available for anyone to review via the OBIE website. The listings include the name of the ASPSP, submission dates, status (e.g. Pass) and notes relating to known issues.

Scheme Approvals Body

The FCA is the Open Banking Scheme approvals body. To use Open Banking, providers must register with the FCA.

Chapter 4 - Overview of GOV.UK Verify Mandatory Certification

The core elements of the GOV.UK Verify mandatory certification regime are: -

Standards

- GPG45 - Identity Proofing & Verification of an Individual
- GPG46 - Authentication and Credentials for use with HMG Online Services
- GDS Operations Manual

Specifications

- Technical Architecture
- SAML2 specification
- Public Key Infrastructure

Liability & Consumer Protection

GDS mandates the protection of the citizen's digital identity and associated personal data with the IdPs accepting contractual obligations to ensure that this protection is maintained.

Scheme Approvals Body

GDS is the approvals body. IdPs are accepted as part of a procurement process initiated by GDS.

Mandatory Independent Certification Regime

GDS mandates that all IdPs join an independent certification regime recognised by GDS. GDS recognised tScheme as such a qualifying scheme. IdPs are subject to approval under the 'Verify Scheme'. Assessments include acceptance testing and monitoring against an operations manual and against the Verify Hub operations. Results of the tScheme assessments are sent to GDS where the final approval decision lies as the Verify Scheme Authority. Certification is required every year.

ISO 27001 Certifications ISMS

tScheme is underpinned by a requirement for the organisation to have in place an information security management system such as ISO 27001. This can be implemented as part of the tScheme certification process.

ISO 27001 Independent Auditors

One of the core functions of an information security management system (ISMS) is a periodic and independent internal audit of the ISMS against the requirements of the ISO 27001 standard. KPMG and LRQA are approved auditors and are both recognised by UKAS, the UK's National Accreditation Body.

tScheme Profiles for Independent Certification

Profiles cover the criteria against which IdPS are assessed when they apply for tScheme approval.

- Base Approval Profile
- Approval Profile for Identity Registration
- Approval Profile for Credential Validation
- Approval Profile for Attribute Registration
- Approval Profile for an Identity Provider
- Approval Profile for Credential Management

tScheme Approvals Body

This is an independent body that reviews the assessors reports and if satisfied with a report gives a grant of approval to the service being audited under tScheme. The results of the tScheme assessments are sent to GDS where the final approval decision lies as the Verify Scheme Authority.

tScheme Independent Auditors UKAS Approved

tScheme is underpinned by regular independent assessment by recognised external auditors. LRQA and KPMG are fully accredited by UKAS to prepare assessment reports to support IdPs applying for tScheme approval.

Ongoing Reporting

Ongoing reporting of service metrics, conversion rates, suspicious activity and identified policy frauds is provided by each IdP for consumption by the Scheme Approval Body, GDS.

Chapter 5 - Parallel Views of the Conformance & Certification Features of the Open Banking and GOV.UK Verify Certification Schemes

The table below provides a simple side by side comparison of the features of the two schemes

Scheme Comparison Table	Open Banking			GOV.UK Verify	
Conformance & Certification	**Scheme Authority**	**PISP assets**	**AISP assets**	**Scheme Authority**	**Assets**
Standards	OBIE	Y	Y	GDS	Y
Specifications	OBIE	Y	Y	GDS	Y
'How To' specifications	OBIE	Y	Y	GDS	Y
Reference applications	OBIE	Y	Y	GDS	Y
Liability & consumer protection	FCA	Y	N	GDS	Y
Non mandatory OIDF self certification tests	OIDF	Y	Y	N/A	N/A
Non mandatory peer review of test results	OIDF	Y	Y	N/A	N/A
Scheme approvals body	FCA	Y	Y	GDS	Y
Mandatory independent certification regime		N/A	N/A	GDS	Y
ISO 27001 Certification ISMS		N/A	N/A	ISO	Y
ISO 27001 Independent Auditors		N/A	N/A	ISO	Y
tScheme Profiles for independent certification		N/A	N/A	tScheme	Y
tScheme Profiles Approvals Body		N/A	N/A	tScheme	Y
tScheme Independent Auditors UKAS approved		N/A	N/A	Various	Y
Ongoing reporting of service metrics, conversion rates,		N	N	GDS	Y

suspicious activity and policy frauds identified					

Chapter 6. Summary

Schemes impacting consumers and citizens in relation to the acquisition, use and storage of their personal data and the initiation of payments, need to have the confidence of all the stakeholders involved in order for the scheme to be successful.

In order to establish an appropriate level of confidence, the scheme has to create ‘the rules of the road’ that define what ‘good’ looks like.

Having published the rules of the road, the participating organisations need to be able to demonstrate the degree to which they comply with the demands of the scheme.

Those organisations that satisfy the scheme’s requirements should then be able to continue to be a member of the scheme as a certified entity.

The degree of effort and cost to achieve certification needs to be proportionate to the risks inherent within the service and the reputational risk of being associated with the scheme itself.

Can a voluntary certification scheme that is subject to peer review, where the certification is undertaken once and does not expire, be sufficient to protect the reputation of Open Banking?

Does GOV.UK Verify need independent annual assessments of each IdP’s services and operations against a profile and certification regime that can get underneath what the organisation really does in practice?