OPEN IDENTITY EXCHANGE

White Paper

VERIFY SANDBOX ENVIRONMENT

WRITTEN BY JIM PURVES

DEC 2016

Table of Contents

1. Introduction

The GOV.UK Verify service uses certified companies to provide citizens with a verified identity account for access to Government services. One of the strategic goals of Verify is to facilitate 'digital by default' policy for public services to equip UK citizens with a digital identity that meets high government standards.

In order to empower citizens with the true value of their trustworthy digital identity, they must be able to use it in private sector digital services. Adoption by the private sector will also deliver significant value to the private sector. There are two white papers that are key inputs to this document which is firstly the 'UK private sector needs for Identity assurance' and secondly 'Accelerating the UK Digital Identity Services Market' which discusses the requirements for the creation of a test infrastructure.

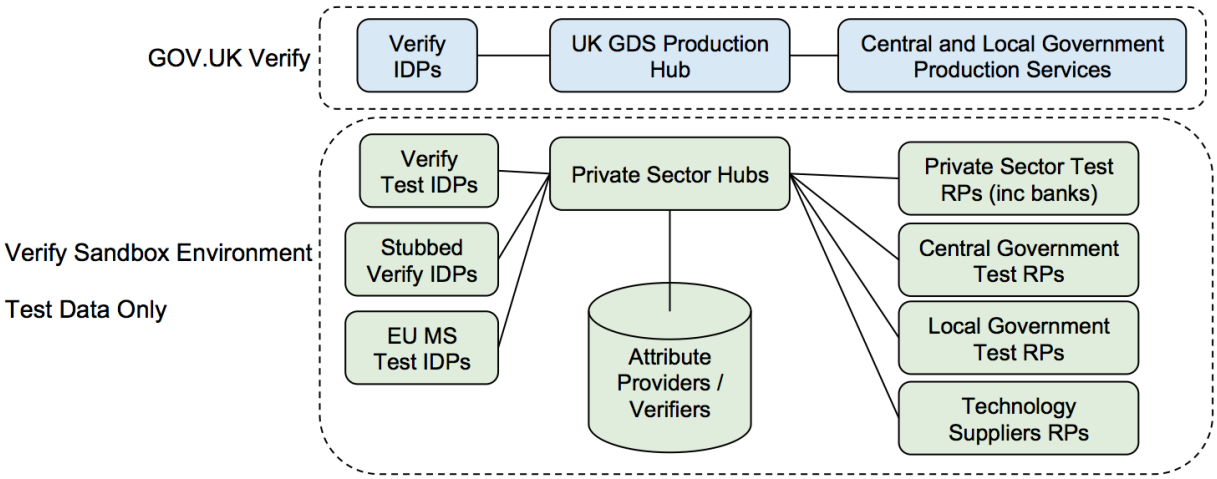
In order to facilitate the adoption of Verify in the private sector, there needs to be a governance structure that describes the responsibilities of all parties (certified Identity Providers (IDPs), Hub Providers, Attribute Providers / Verifiers and Relying Parties) and ensure these responsibilities are met. The Governance process needs to describe how new services are on-boarded onto Verify and 'move' from a pre-production (alpha) environment to controlled release through a beta phase before becoming a live service.

However, before the formal governance process starts there needs to be a light weight testing environment - a so-called 'Sandbox' Environment - that will allow Relying Parties and technology suppliers, from both public and private sectors, to 'play' with the technical components that align with Verify. The goal of this environment is to allow the Relying Parties to test and learn to understand what needs to be done before they move into a formal project to adopt Verify. There is no commitment needed from any of parties to progress from a Sandbox Environment to an Alpha project and also no commitment to continue with the same Hub Provider.

The purpose of this document is to describe the process and activities required for the Private Sector Hub Providers to set up a first instantiation of a Verify Sandbox Environment. It is envisaged that these processes will change as the governance process for Verify in the private sector emerges.

2. Involved Parties

The diagram below shows the parties that can engage to create the Verify Sandbox Environment. The key party is the Private Sector Hub Provider who will need to undertake a lightweight self certification process to set up their Sandbox Environment.



3. Context with Private Sector Verify

This document is going to focus on the process for the Sandbox Environment only. The main outcomes of testing in the Verify Sandbox Environment is to enable (and their technology suppliers) to have a technical and functional understanding of Verify which will inform their business case to be able to progress to live service. The Government Digital Service (GDS), which operates GOV.UK Verify, is running a project with the private sector to understand the first stage of the Verify Private Sector On-boarding process. The results of this project will be published by GDS.

4. Self Certification and Listing Process

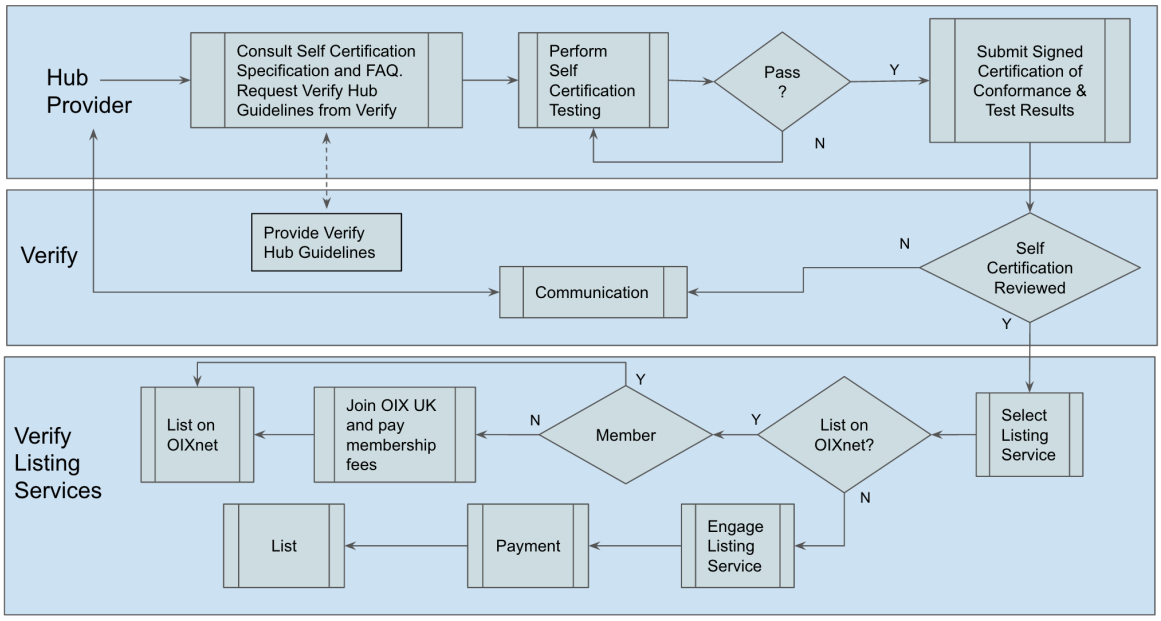
Private sector Hub Providers need to be certified and have their certifications listed in order to be able to offer their services to the market. However, for the Verify Sandbox Environment this will be a self-certification activity that assures potential Relying Parties that the Hub Providers are aligned to minimum standards for Verify.

Self-Certification

There is significant advantage to a self-certification & listing process (see section on Listing Service and Payments below) compared to an independent 3rd party certification process. This is primarily low cost and low overhead that has the result of encouraging new Relying Parties to explore how they would adopt Verify. The Hub Provider presents evidence of compliance with Verify standards that is simpler, quicker, less expensive and more scalable than 3rd party certification. Evidence of compliance is made available for public scrutiny and organisations put their reputation on the line by making a public declaration that its implementation conforms to the required standard.

Process

The diagram below shows the self certification process for Hub Providers to go through and then list their accepted services.



The details of the process are as follows:

- The Hub Provider starts the process by reviewing the self certification requirements and FAQs to understand what is required of them to become certified. These documents will be published on the listing service. The Hub Provider will also need to contact the Verify team to request the Verify Hub Guidelines document at verify-sandbox@digital.cabinet-office.gov.uk. The Self Certification requirements can be seen in Appendix A.
- Optionally, if the hub provider wants to engage with public sector services they will need to have a SAML interface that aligns to the Verify standard. The Hub Provider will test their own interface and provide evidence of conformance through their test cases and test results.
- Once the Hub Provider has completed its own conformance test, it submits the self certification request to the Verify team including the test cases and results and a signed declaration that the organisation conforms to the defined requirements.
- The Verify team reviews the self-certification and related evidence for completeness and assures it is ready for listing.
- Once the Hub Provider's self-certification has been accepted they will select their listing service. They will need to engage with that listing service and pay listing fees as appropriate. If the listing service selected is OIXnet then the Hub Provider will need to be a member of OIX UK before they can list.

Listing Service and Payments

The Verify Sandbox Environment needs to have a public facing channel for communications to industry to promote their service and also act as a point of trust for their alignment to the self certification requirements. There may be multiple Listing Services of which OIXnet, which is owned by the Open Identity Exchange, is one. Hub Providers that undertake the self certification process may need to pay to have their services listed. An example of the type of information required for OIXnet listing, including costs, can be seen in Appendix B

5. Governance

Users will expect a consistent experience when they use their digital identity under Verify and will wish to know that the integrity of their digital identity is protected wherever they use it. The market will need to develop a consensus on which areas are defined by agreed standards in order to achieve the trust of users and which areas are open to competition and innovation. This will necessitate a degree of transparency even in the Verify Sandbox Environment. Therefore the Verify team will define the governance of the Sandbox Environment to ensure that there is the appropriate level of transparency across all projects. The goal is for this transparency overhead to be as light as possible to help projects and is not expected to be a day-to-day involvement. Verify will appoint a Verify Sandbox Manager who will engage with projects to achieve the following:

- Define and agree use cases and test data with project participants
- Report on high level outcomes of tests to stakeholders
- Providing support to the Hub Providers for client engagement
- Assist in project kick offs
- Introduce other potential value adding partners where appropriate
- Provide awareness of other projects (where appropriate to disclose) that can accelerate testing and understanding
- Cross Hub Provider communications for 3rd parties that want to engage (such as attribute providers)
- Understanding Verify level risks and issues and help to mitigate them
- Communication to the Verify Management team
- Capture of pre-agreed meta data about projects to enhance the development

6. Costs

Testing through the Verify Sandbox Environment incurs costs for all parties and these costs will need to be funded. Hub providers cannot be expected to provide a free service if there is no commitment for their services to be procured for a production service.

All pricing and contracts for projects need to be agreed between the engaging parties and Verify does not need to be involved. If projects want to be conducted under OIX project rules then there is a project overhead fee of 10% with a minimum spend of £2.5k + VAT.

7. Customers

Customers of the Sandbox Environment can be from either the public, private or the 3rd Sectors and they will need to engage with Hub Providers to commence and run projects.. Public sector organisations should initially engage with the Verify engagement team as their likely route will be to connect to the GOV.UK Verify hub provided by GDS. The procurement route for public sector organisations with private sector hub providers will be through the Digital Outcomes and Specialists framework. For hub consultancy and testing, please apply to the digital outcome and specialists 2 framework, closing date 14 December 2016. After this date, to offer a test environment hub service to the public sector, please apply for the new G-Cloud framework next year.

For private sector Relying Parties, or private sector suppliers supplying to the public sector, the primary route to testing in a Verify environment will be through private sector hub providers in the Verify Sandbox Environment. The customer and the Hub Providers will be able to choose whether they want to run the project as an OIX project. The Verify project manager will be able to help make customers aware of the value that comes from the OIX process but customers do not need to be members of the OIX or OIX UK to participate in projects.

Under OIX projects there is a standard OIX UK project process and all parties will be asked to sign the OIX Participant Agreement which can be found here (all parties have the rights to protect their IP through this agreement and can selectively disclose any information publicly though OIX white papers and any information that they wish to retain as private).

The route to a production environment is different depending on whether the customer is a Relying Party (or a technology / service supplier) in the public or private sectors. The Public Sector, including central and local government, will progress to production via the GOV.UK Verify hub whereas private sector will progress via their choice of private sector hubs.

8. Further Information

For further information about the Verify Sandbox Environment please contact the Verify team via verify-sandbox@digital.cabinet-office.gov.uk

9. Conclusion

Creating the Verify Sandbox Environment will enable Relying Parties and their technology suppliers to develop and test their services in a flexible environment to achieve a detailed technical and functional understanding of Verify and the use of trustworthy digital identities. All organisations that use the Sandbox Environment will be able to provide feedback to the Verify team of any risks, issues or recommendations that emerge at the Verify level. Once a detailed business and technical understanding of the implications of integrating Verify with a Relying Party's service has been achieved it will enable it to create the necessary business cases to agree the commitment and resources required to move into an Alpha phase of a delivery project. Hub Providers will also be able to test their services and begin to understand what is required to bring these services into a live environment for the private sector.

10. Appendix A – Hub Provider Self-Certification Document

DRAFT

Certification of Conformance to the following Hub Provider standards for the Verify Sandbox Environment

Organisation Name ……...

Category	Detail	Means of Assurance. Additional Details
Functionality	Brokering of identity and attribute requests from test Relying Parties to test Verify Identity Providers and the return of a matching data set and attributes to a Relying Party. The presentation of the Identity Provider selection page to allow a user to select an Identity Provider. Integration to at least 2 Verify Identity Providers and / or the creation of 2 Verify representative Identity Providers that align with the UX of those Identity Providers. The Identity Providers will enable a credential Authentication and the return of the matching data set. Hub Providers must contact all the Verify Identity Providers to offer the ability for them to connect to their test environment. The Identity Providers can provide a list of blacklisted markets that they do not want the hub providers to work with. Only the Verify Identity Providers or representative IDPs can be displayed on the IDP Selection Page.	
Tech Standards	Compliance to the Verify Hub Guidelines (Document provided on request). For engagement with public sector services provide evidence of compliance with the Verify SAML profile. The evidence could simply be in the form of test cases and results. Exceptions Hub support for the PKI in the Sandbox is optional.	

	Additions Where the Hub Provider offers the OpenID Connect protocol it is best practice to align with the self certification requirements defined by the OpenID Foundation defined via the OIXnet website Where the Hub Provider offers the International Government Assurance Profile (iGov) reference should be made to the iGov Working Group through the OpenID website	
Security	The Sandbox Environments will use test data and hence the level of security required will depend on the projects being conducted.	
Process	Viable on-boarding process for Identity Providers and Relying Parties that should be self defined and aligned to business need.	
User Experience Design	Under the current government framework, the GOV.UK Verify logo and identity are owned and managed by the Government, for use in Government only. As Verify expands to include the private sector, Verify design assets will be licenced for use by companies and organisations. The private sector re-use project will explore and design user journeys, and identify some of the associated challenges and solutions for private sector Relying Parties. Hub Providers will be expected to implement against the guidelines, and make Relying Parties aware of them, as they become available.	
Non Functional	Make the Verify Matching Service Adaptor (MSA) available to public sector Relying Parties (when the open source code is made available). Awareness of the existing documentation on matching in the Verify Technical Guide and the OIX White Paper on Data Matching in the Identity Ecosystem. Must be able to operate a PKI if required by partners	
Verify Reporting	Agree to engage with the Verify team in order to understand what level of reporting is appropriate to both protect commercial sensitivities and provide Verify level insight. At a minimum bi-monthly reports on the high level status of all projects must be completed.	

Communications	Publishing of the Hub Provider service offering and self certification documentation on a listing service	
Operations	Operational availability for UK business hours	
Principles	Must be aware of the PCAG Identity Assurance principles	

Organisation Address Information

Address	
Country	

Organisation Authorised contact Information

Name	
Title	
Email	

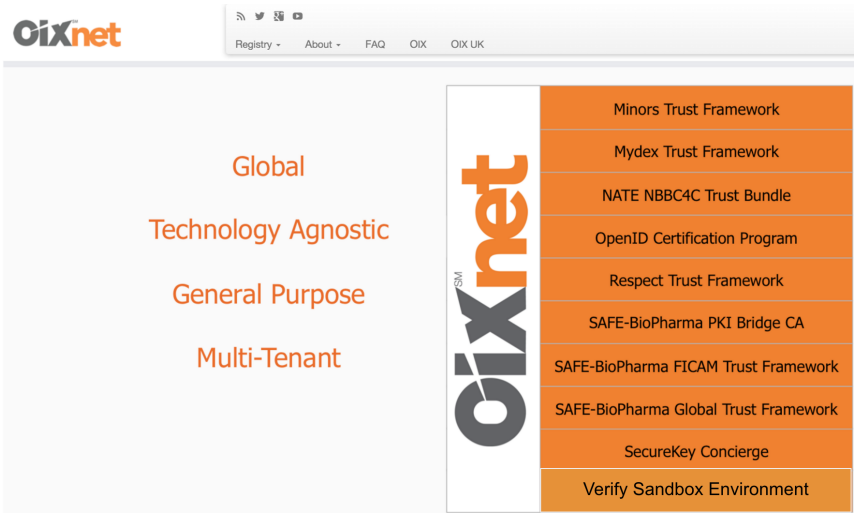
Signature ……..

Date ……..

Appendix B – OIXnet Listing

This appendix shows an example of how the Verify Sandbox can be registered on OIXnet. For members of OIX UK, the costs of listing on OIXnet are included in their membership fees. This reflects the current OIX Board decision and is expected to be the case for the foreseeable future but the OIX Board reserves the right to change that decision. Non OIX UK members Hub Providers will need to join OIX UK before they can list their services. The content in this appendix is example content only as well as an example structure.

Example OIXnet home page:



Verify Sandbox Environment Page

Registrant

GOV.UK Verify
Address

GOV.UK Verify is run by the Government Digital Service. It is the way to prove who you are online so you can access digital services securely and safely and at your convenience and without having to use postal or face-to-face services. Verify is building a new market of identity services that will continue to grow and improve over time, whilst designing user privacy and control into the system from the start. Verify provides one consistent, safe service that all of government can use, rather than each department inventing and paying separately for its own separate approach which would be wasteful for government and more complex and difficult for users. Verify is more than just a new service, it's also building a new market for identity services, in the UK, in Europe and globally. This means that there are clear rules of the game, a substantial demand for services meeting those rules from government and other sectors, and a clear incentive for the market to invest to build new solutions. This market will be able to meet the needs for identity assurance not just for central government services, but also for local authorities, health services and private sector services like banks, mobile network operators, airlines and retailers. The benefit of this market to the UK economy has been estimated at close to £3 billion, just in savings against the cost today of assuring people's identities using old, analogue methods.

Privacy and consumer control are designed into the service – GOV.UK Verify has been working with a Privacy and Consumer Advisory Group since 2012. There is no central database or persistent identifier.

Primary Contact:
Verify Contact

Alternate Contact:
Verify

Information being listed

Verify Sandbox Overview

The Verify Sandbox Environment enables organisations to conduct initial testing projects so that they can achieve an understanding of how to leverage Verify and trustworthy digital identities within their organisations. Any organisation that wants to test Verify can do so by engaging with a certified hub providers which can be seen in the list below.

Certification means that these providers have reached a minimum set of standards for Verify and can therefore be trusted by other organisations.

Verify Sandbox Links

Frequently Asked Questions
Hub On-Boarding Process
Self-Certification Process

Verify Sandbox Self-Certified Hub Providers

The following organizations have self-certified compliance to the OIX UK Sandbox specifications and are registered:

Certified Party	Hub Service	Self-Certification Date
Org 1	Org 1 hub service for Verify	07 November 2016
Org 2	Org 2 hub service for Verify	10 November 2016
Org N	Org 3 hub service for Verify	12 November 2016

Certified Parties

Organisation Name
Name and Address

Primary Contact:
Eg: Chief Technology Officer

Services offered
Description of the service being offered

Verify Sandbox Self-Certifications
Hub Provider Service for Verify (this would be a link to a PDF of self-certification results)

Indicative Rate Card
Description of pricing for services being offered

Appendix C – Glossary

Term	Description
attributes	Data that's sent from one entity to another in a SAML assertion, for example, the matching dataset for use by the matching service.
authentication request	The request that a service sends to the hub, or the hub sends to an identity provider, to request the identification of a user trying to access a digital service.
credentials	An identity provider issues credentials to a user to allow the user to be authenticated when accessing a government service. Examples of credentials are usernames, passwords and security codes.
cryptography	A set of techniques for guaranteeing the integrity and confidentiality of data transmitted over a public network. This is done by a combination of encryption and signing
data matching	The process of finding a local identifier through matching that's useful to a service when completing a transaction, for example confirming a National Insurance number so the user can amend their tax records.
hub	The infrastructure that manages interactions between users, services, identity providers, and matching services for the purpose of authenticating a user who wants to use a service. The hub protects privacy and ensures security during authentication.
identity	In the case of identity assurance, this is the description of who or what an entity is, defined by a collection of attributes.
identity assurance	The ability to prove, to a certain level of confidence, that a user trying to access a digital service is who they say they are.
Identity Assurance Principles	The principles that set out how the government's identity assurance approach should be configured to meet the privacy and consumer expectations of its users. They are published by the Privacy and Consumer Advisory Group and are amended or replaced from time to time.
identity provider	Private sector organisations, to verify that a user is who they say they are and assert verified data that identifies them to a government service. The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and the National Cyber Security Centre.
Matching Service Adapter	A software tool provided by GOV.UK Verify that's installed within the government service's security domain. The Matching Service Adapter handles SAML requests for matching queries and sends responses to the GOV.UK Verify hub. The Matching Service Adapter and the local matching service together comprise the matching service.
onboarding	The process through which new government services integrate with GOV.UK Verify. The onboarding process is divided into 6 stages. Each stage has a defined set of outputs which a service must meet before moving to the next stage. Onboarding ends with access to the full production environment where the

	government service deploys their live service.
public key infrastructure (PKI)	The purpose of a public key infrastructure is to implement secure electronic transactions over insecure networks such as the internet. It is used to authenticate identities for the purposes of data encryption and signing.
relying party	An entity in a system of federated identity that relies on a response from another entity, such as a successful authentication request. A relying party is also referred to as a service provider when it provides a service that the end user directly interacts with. Relying party is a term used in SAML specifications. In the GOV.UK Verify federation, relying parties are government services.
SAML (Security Assertion Markup Language)	An Extensible Markup Language (XML) open standard for the exchange of authentication and authorisation data between parties such as identity providers and government services. OASIS governs the SAML standards.