payments strategy forum

July 2017

Trusted KYC Data Sharing – Framework Implementation

Supporting Document

Contents

Preface

This document has been produced by the Financial Crime, Security and Data Working Group (FCWG) as part of the consultation paper 'Blueprint for the Future of UK Payments' developed and published by the Forum in July 2017. It describes our suggested implementation approach to be followed by the future delivery body in order to create the framework outlined in Section 6.3 of the consultation document.

This document is expected to be of particular interest to those with a role in the prevention of financial crime, including Payment Service Providers (PSPs), trade bodies, solution vendors, regulators, law enforcement agencies and the government.

The establishment of a data sharing framework is recommended (see Figure 1) to provide a method of sharing a core set of SME[1] customer data between organisations acting as data providers where the customer already has an account (e.g. a bank or insurance company) and other organisations who use that data with the customer's consent (data consumers).

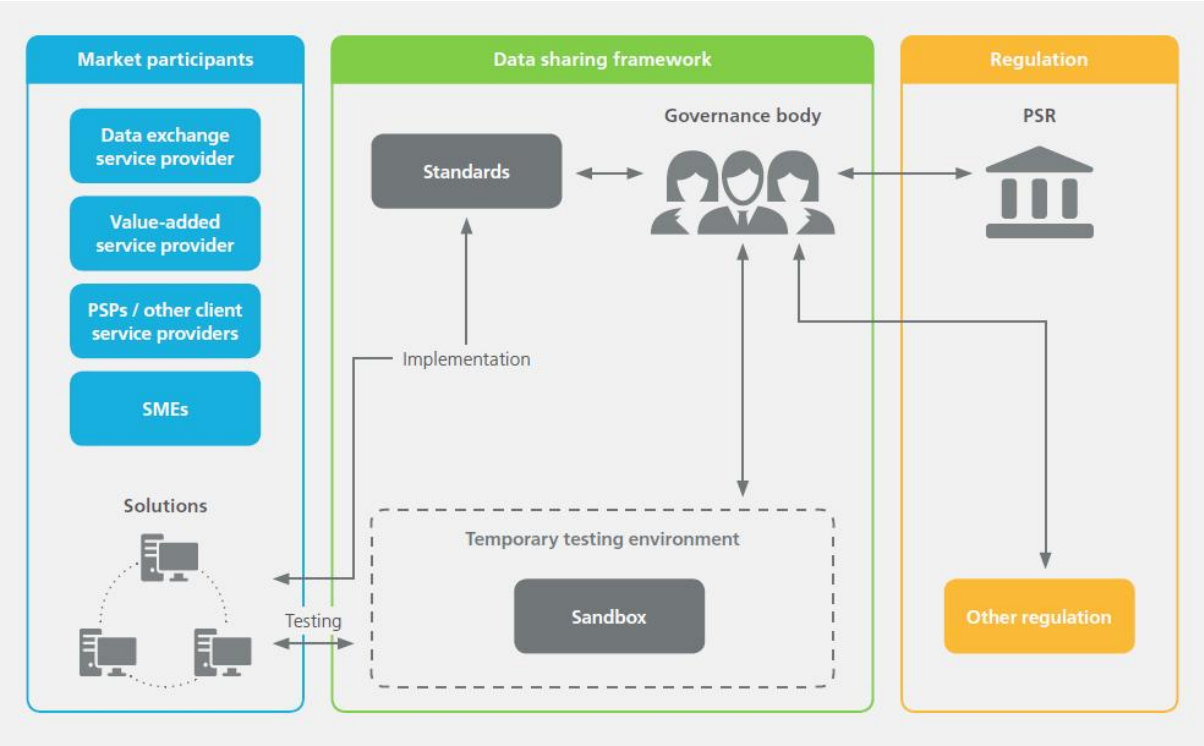

Figure 1 Schematic picture of data sharing framework

The framework will consist of a set of standards for the sharing and exchanging of a core set of SME customer data overseen by a governance body, and supported by a temporary testing environment. The lack of industry-wide standards, rules and governance might have limited the market adoption of data sharing solutions in the past. It is expected that the data sharing framework will resolve this and lead to a range of competitive value-added Know your customer (KYC) services using the evolving data sharing capability.

Data sharing is intended to be on a point-to-point basis between PSPs, or via data exchange service providers which offer a single point of connectivity between data providers and consumers. Data will only be shared with the customers' consent. For example, an insurance company (data consumer) can

[1] Small and Medium sized Enterprises (SMEs)

only receive customer data from a bank (data provider) about a customer (data owner), with that customer's consent. In this example, the insurer could also purchase services from a data analytics company (KYC service provider) to further enhance and validate the data being shared.

The whole network and the wider public will benefit from improved (i.e. corrected, verified and timely) customer information through updates during each interaction. Results will include improved customer experience, reduced KYC operational costs and increased ability to identify 'bad actors'[2] and reduce financial crime.

The data sharing framework is expected to enable the development of a market for the provision of KYC services as well as a wider range of services supporting other business activities. Data exchange service providers will be able to participate by complying with the standards set by the governance body. Value-added service providers will be able to test their KYC services against the specific needs of individual PSPs and client service providers in the temporary testing environment.

1 Objective of this Document

The 'Trusted KYC Data Sharing' solution introduced in Section 6.3 of the consultation document is further detailed in two documents (see Figure 2). This document describes the suggested implementation approach for the data sharing framework. The following components are required to allow active involvement by participants in customer data sharing:

1. Baseline standards for sharing a core set of SME customer data, accepted within and beyond the payments industry, to support SME KYC processes.
2. A permanent governance body monitoring adherence to standards and rules, including responsibility to mitigate the risks of abuse, fraud, privacy and security issues.
3. A temporary testing environment encouraging the development of a market for value-added KYC services.

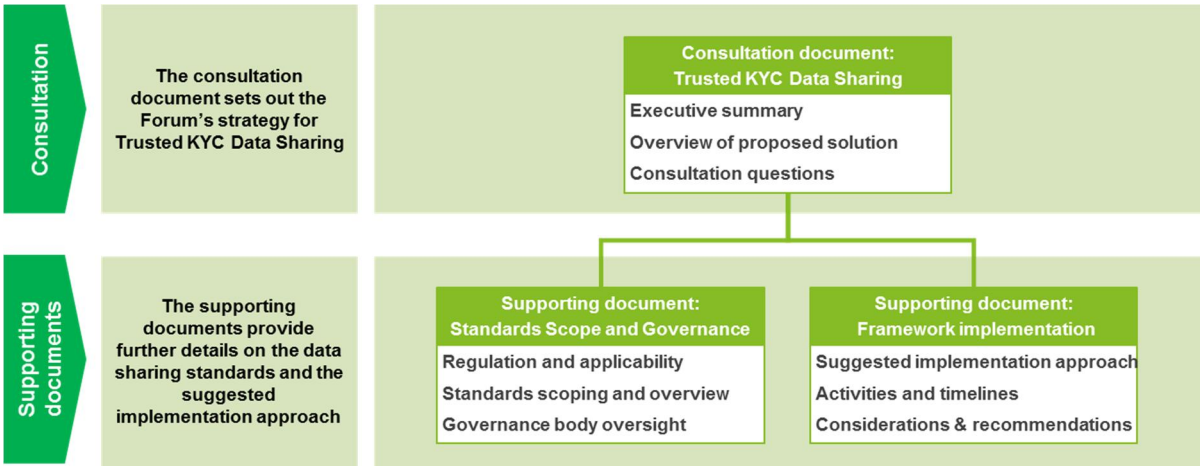

Figure 2 Schematic picture of document structure

The delivery body will need to identify and / or establish a governance body before the development of the temporary testing environment. When establishing the framework, the following illustrative steps should be considered (see Figure 3). Please note that these activities and timelines are only indicative; they must be validated and confirmed by both bodies once established.

[2] Bad actors are those individuals or organisations who intend to use the services of a PSP or Financial Institution to commit fraud or other financial crime.

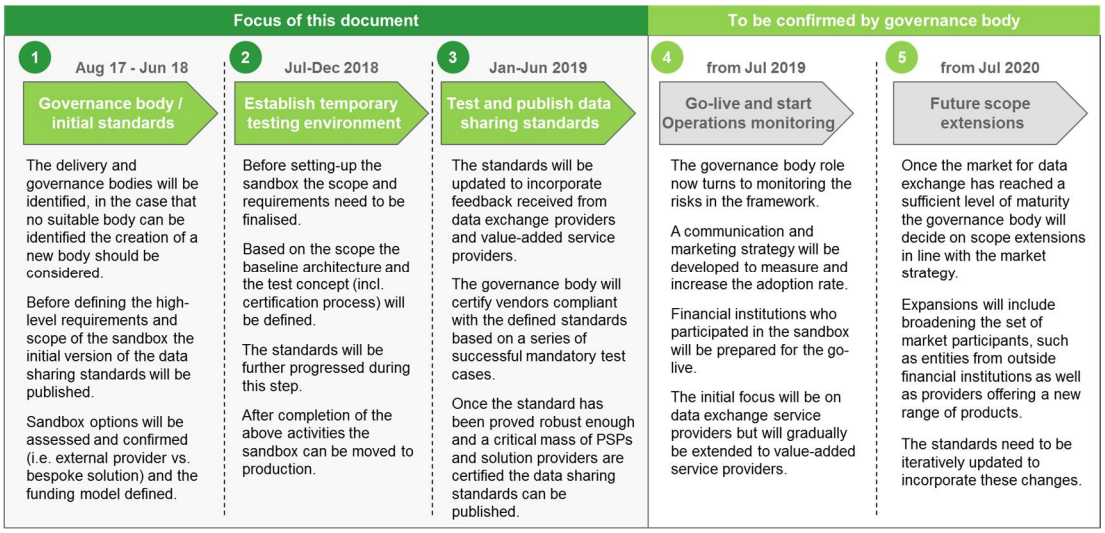

Figure 3: Suggested implementation approach

2 Evolving Benefits Provided by the Data Sharing Environment

The greater the number of participants utilising the exchanging mechanisms, the more often the data is refreshed, verified and updated with the SME customers' consent. This results in participants having efficient access to the most complete, recent and highest quality data. This will increase the chance to detect 'bad actors', whilst streamlining the KYC process between SMEs and PSPs. They will receive tangible benefits from the beginning, including reduced barriers for PSPs to enter the SME market segment and SMEs subscribing to new products and services as a result of more efficient due diligence processes.

Figure 4 provides an overview of the expected adoption by solution providers and the subsequent benefits in addressing inherent detriments.

	Introduction (by mid- 2019)	Growth (mid-2019 - mid 2020)	Maturity (from mid- 2020)
Anticipated benefits	• Focus on data sharing and exchanging. • Standardised interaction mechanisms between SMEs and financial services. • Greater level of assurance and trust in customer information through increased collaboration and sharing. • Better customer experience at higher speed and with higher quality outcomes.	• More KYC value added service provider entering the environment. • Improved market competition and account switching capability. • Broader number of service providers is expected to further improve the sophistication and speed of the services, e.g. usage of data passport.	• Inclusion of non-Financial Institutions such as telecommunication and utility services providers. • Access to more dynamic data (by linking to a broader range of services used by the customer on a regular basis). • Access to additional and varied data sources to supplement the standard core set of data (e.g. telco geo-positioning data).

Figure 4 Evolution of solutions and anticipated benefits

Introduction (by mid-2019)

The initial implementation of the standards will be limited to cover the exchange of a core set of SME customer data between PSPs and/or third party service providers (TPSPs). The standards can subsequently be extended in future phases to cover additional services and include participants from other sectors to expand the range of benefits offered to SMEs. The initial data exchange environment will help PSPs to improve customer experience by:

- Maintaining higher data accuracy as a result of more frequent data collection across the network.
- Making the access to core customer data easier and less costly thereby reducing form filling activities.
- Having access to more comprehensive data by directly linking to PSP source systems.

Growth (mid-2019 – mid-2020)

From mid-2019 till mid-2020 it is envisaged that the data exchange environment will evolve further, and new services will be offered by third party providers covering a wider range of services across the whole KYC value chain (such as data validation and customer screening). In addition, the participation by a broader set of Financial Institutions (such as Insurers and Asset Managers) could lead to these additional benefits:

- More accurate data (as a result of value-adding services which validate the data quality).
- Greater competition in the market and innovation for value-adding KYC services.
- Improved account switching capability.

Maturity (from mid-2020 onwards)

When the first complete version of the data exchange standards is published, the core set of SME customer data will be shared more frequently (e.g., SMEs contracting new services/products from different institutions), leading to increased data accuracy. An ongoing evolution of the standards is expected after this point, particularly given consideration of how and when non-UK PSPs should be included.

An example of this evolution could be the inclusion of non-Financial Institutions such as telecommunication and utility services providers. This will bring further benefits such as:

- Access to more dynamic data (by linking to a broader range of services used by the customer on a regular basis).
- Access to additional and varied data sources to supplement the standard core set of data (for example telco geo-positioning data).

There will be room for multiple solutions based on different business models. These solutions may be designed to target different customer segments. New service providers will benefit from the open landscape created where data sharing is already possible between different participants. This will allow them to provide their services in a more efficient and effective way, giving them the chance to replace or provide new alternatives to the existing sharing mechanisms.

The above development path is based on a conservative adoption rate by participants of the data sharing framework. Should PSPs with a large market share be more proactive than predicted the development curve will be faster leading to more services being offered as the data exchange volume increases.

3 Implementation Steps and Activities

The approach described in the overview can be further broken down into the following key activities which are outlined in Table 1 and are described in the following sections.

Schedule	Step	Activity
Aug 2017 – Dec 2017	**Step 1**: Handover to delivery body	1. Identify delivery body and define project plan
Jan 2018 – Jun 2018	**Step 2**: Establish governance body and develop standards	2. Establish governance body 3. Select testing environment provider and define funding model 4. Publish initial standard and translate into sandbox requirements
Jul 2018 – Dec 2018	**Step 3**: Establish temporary testing environment	5. Stakeholder management 6. Finalise scope and requirements 7. Define baseline reference architecture 8. Define test concept and certification process 9. Move testing environment into production
Jan 2019 – Jun 2019	**Step 4**: Test baseline standards and update for publication	10. Perform tests 11. Iterative updates to solutions and standard 12. Move certified solutions to production and publish baseline standard
Jul 2019 ongoing	**Step 5**: Go-live and start Operations monitoring	13. Communication strategy 14. Market strategy 15. Operations monitoring
Jul 2020 onwards	**Step 6**: Future scope extensions	16. Expansion strategy 17. Certification of new entrants 18. Further development of standards

Table 1 Recommended implementation approach.

3.1 Step 1: Handover to Delivery Body

After the consultation phase the Forum will facilitate handover to a delivery body which will be responsible for the development of the data sharing framework, the engagement with a governance body or establishing a new oversight body for the framework.

3.1.1 Activity 1: Identify Delivery Body and Define Project Plan

Workshops will be initiated in October and November 2017 to discuss and agree the approach to establishing the most appropriate entity, or entities, to lead and take responsibility for implementing the KYC Data Sharing framework.

Once identified and agreed, the Forum will hand over responsibility for all further activity to this body, who will be accountable for establishing the data sharing framework. It will create a detailed project plan spanning the activities outlined in this document. In the first step all activities until end of 2018, i.e. until the testing environment is established, should be itemised in detail and prioritised.

3.2 Step 2: Establish Governance Body and Develop Standards

From the beginning of 2018, delivery body activities will include the establishment of a governance body, the selection of a testing environment provider, the definition of a funding model and the publication of initial standards and requirements.

3.2.1 Activity 2: Establish Governance Body

The delivery body will set up a series of workshops to validate the core requirements of the governance body. These requirements should cover the following topics:

- Governance body objectives
- Members
- Responsibilities
- Authority
- Governance body administration
- Relationship to other bodies

During the workshops a potential governance body will be selected from existing bodies (industry or other) that may already satisfy the requirements outlined above. In the case that no suitable body can be identified the creation of a new governance body should be considered. The governance body should incorporate members from a wide variety of organisations representing different participant categories in the new data exchange environment potentially including PSPs, client service providers, SMEs, sponsors, technical providers, data privacy experts, contributors and observers.

Once established, the governance body will set up and sign-off the governance scope requirements, define the mechanisms to oversee the environment, and define the process for updating the data sharing standards (now controlled by this body). It will supervise the certification process for participants that are compliant against the defined data sharing standards, and will have the authority to revoke the certification for participants that no longer meet them.

Overall responsibilities of the governance body will include the following activities:

- **Define the standards** on the sharing and exchange of a core set of SME customer data through the environment.
- **Evolve the standards** to meet the needs of the full range of participants (SMEs, PSPs and KYC service providers).
- **Enforce compliance** of the defined data exchange standards.
- **Oversee participation take-up and utilisation by PSPs and SMEs** in the data sharing environment.

3.2.2 Activity 3: Select Testing Environment Provider and Define Funding Model

The delivery body will define technical and functional criteria (e.g. sandbox and technical infrastructure, logistics, project management skills, etc.) to identify a suitable testing environment provider (sandbox) through a competitive tender. These requirements will be signed-off by the governance body. It is recommended that at least three providers should be considered during this selection process. In the unlikely event that no provider would be able to fulfil the sandbox requirements, a bespoke solution should be considered.

The base assumption is that the temporary testing environment is operated on a not-for-profit basis, making the environment affordable for all participants thus not limiting the competition in the market. Therefore the delivery body needs to define an appropriate funding model. To ensure that the temporary testing environment is used and supported by the maximum number of participants.

The final funding option is likely to depend upon the decision to use an industry sandbox, or to create a bespoke environment. It must also be decided whether participants will start funding prior to the go live of the testing environment. This would reduce the initial investment to be covered by the environment provider.

3.2.3 Activity 4: Publish Initial Standard and Translate into Sandbox Requirements

June 2018 is recommended as the deadline by which the core standards must be agreed; this will ensure an appropriate period of time is available for the sandbox setup. The delivery body should use industry best practice when defining the lower level details contained in the standard, and should agree the standards through close engagement with the future framework participants.

The high-level demands articulated in the standards – see supporting document 'Trusted KYC Data Sharing - Standards Scope and Governance Oversight' - need to be translated into requirements for the temporary testing environment, e.g. availability of the environment, expected parallel users; reporting and Management Information requirements; possibility to use existing industry standards[3]; and integration with other sources like Company House. These requirements need to be developed by the delivery body and be signed off by the governance body.

3.3 Step 3: Establish Temporary Testing Environment

The objective of the temporary testing environment is for an early adopter community of PSPs, client service providers and technical providers to exchange data in a safe environment, and to test and refine the interoperability between the different data exchange methods. This will provide a hosted environment to evaluate and iterate the data sharing standards. The sandbox will support the development of the certification process used to ensure participants comply with the data exchange standards.

The sandbox will also provide an environment for third party KYC service providers to position, market and refine their value adding service offerings. The sandbox provides a mechanism to aggregate and manage the demand for KYC services from PSPs and other client service providers by:

- Forecasting the solutions' success by tracking the adoption rate and by monitoring the data sharing volumes.
- Simplifying the vetting process by using the testing environment for proof of concept and certification.
- Negotiating and standardising service terms (including quality, price and setup fees) and payment mechanisms.

To facilitate the exchange of services between the sandbox participants a central registry will be provided during the duration of the sandbox; however no industry-wide common infrastructure outside the test environment will be available. Figure 3 lists the high-level design principles of the sandbox.

High-level sandbox design criteria:

- It will allow the testing of the standards designed for the customer data exchange.
- It will provide an environment for KYC service providers to test and demonstrate their offerings to Financial Institutions using the provided data sharing environment.
- It will be flexible enough to test future requirements across the whole KYC end-to-end value chain including data validation, customer screening and other functionalities.

Figure 3 High-level sandbox design criteria

The temporary testing environment will help to improve market competition and is expected to lead to a wider development of solutions resolving common industry problems, particularly ones driven by

[3] Like the CMA business current account opening standard information set

upcoming regulatory change such as GDPR or PSD2. Multiple exchange providers and peer-to-peer networks can coexist in the sandbox and allow TPSPs to use existing data foundations to demonstrate their value-added services to potential PSP customers.

Figure 4 illustrates the data sources used by the sandbox, and gives an overview of example test cases to ensure compliance with the data sharing standards.

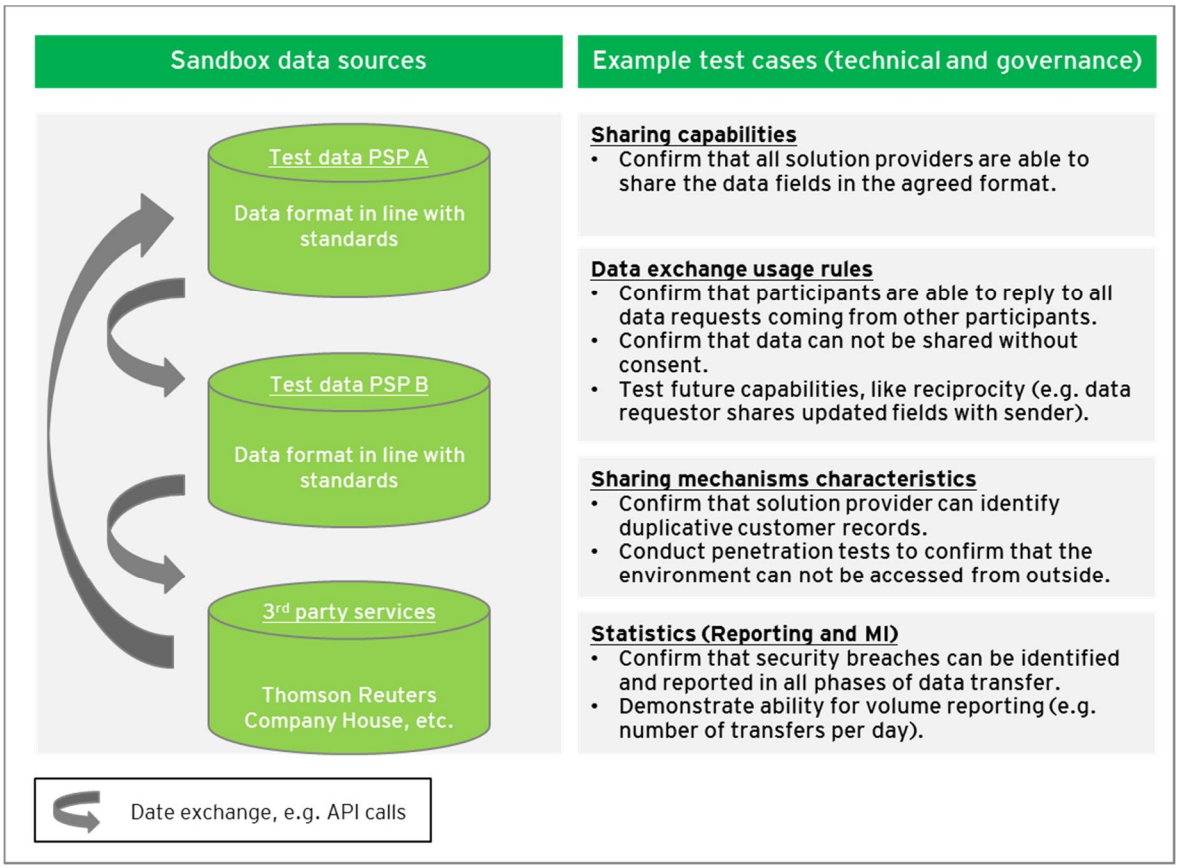

Figure 4: Sandbox: data sources and example test cases

3.3.1 Activity 5: Stakeholder Management

The delivery body will define and identify the users, observers and suppliers to the sandbox, e.g. service providers, SMEs and Financial Institutions. Although the initial phase will focus on PSPs and other client service providers, participation will not be limited to them alone.

While the governance body oversees the establishment of the sandbox in line with the strategy the day-to-day participation in the sandbox requires a number of forums:

- User forum: consisting of PSPs, client service providers and SMEs - recommends changes to the testing environment and the data sharing standards based on industry needs.
- Standards forum: allows contributors and observers to evaluate the standards.
- Cost/benefit forum: allows the relative costs and benefits of further standardisation to be explored carefully, through mutual collaboration.
- Regulatory forum: allows regulators to join conversations on regulatory issues raised in sandbox testing.
- Economic modelling forum: defines the future pricing mechanisms for the sharing capability, e.g. price point per transaction.

3.3.2 Activity 6: Finalise Scope and Requirements

The high-level requirements defined in Activity 4 need to be articulated in a formal business requirements document, ensuring the sandbox fulfils the needs of all participants. If the standards are further developed during this step the revised version will be taken as a baseline. All framework participants and forums should be involved in the creation and sign-off.

At a minimum it is recommended to cover the following topics:

- Likely contributors to the sandbox – entities providing assets, technology or services (e.g. providers of SME information).
- Solutions to be included, and which should be covered by the test concept.
- Reporting and MI - data fields, data exchange usage, data privacy and security.
- Possibilities to utilise other industry standards.
- Operating principles and protocols.

3.3.3 Activity 7: Define Baseline Reference Architecture

The business requirements need to be translated into a baseline reference architecture and technical requirements. This will accelerate delivery and provides a basis for governance to ensure the consistency and applicability of technology usage within the environment. The following advantages are expected by conducting this activity:

- Improvement of the interoperability of the environment by establishing a standard framework and sharing best practice.
- Reduction of development costs through a common vocabulary to provide a quick start for all participants.
- Improvement in communications by sharing the same architectural mind-set.
- Taking important design decisions early on.

3.3.4 Activity 8: Define Test Concept and Certification Process

A test concept including test scope and goals, test plan, test cases and the certification process needs to be created and signed-off before moving the testing environment into production. Considerations could include:

- Establishing a test case inventory to ensure that all relevant section of the data sharing standards are covered.
- Establishing communication protocols, including process for making requests and collecting data, capturing issues and vetting issues with the delivery body.
- Desired testing and resource schedule /timeline requirements with prioritised testing activities based on criticality for going-live.
- Defining the period of validity for the certificate, e.g. refresh intervals and trigger events (e.g. major changes to the standard) requiring a solution to be re-certified.

Test cases should cover all categories of the initial standards mentioned in Activity 4. For more details on possible test cases please refer to Appendix 1.

3.3.5 Activity 9: Move Testing Environment into Production

Once the sandbox environment is operationalised and fulfils the requirements set out in Activities 6 and 7, it can be moved to production. It is recommended that user acceptance tests are performed in order to confirm that all requirements are met.

3.4 Step 4: Test Baseline Standards and update for Publication

In this step an assessment is made as to the readiness of the standards and technical solutions, having reached a maturity and level of support to justify moving to production. This will be measured through a sign-off process following a series of successful mandatory test cases. Consent must be sought from the appropriate forums (see Activity 5) prior to production.

Participants with solutions outside the scope of the baseline standards (e.g. future functional areas) can be allowed to participate if all forum members give their consent by assessing possible impacts, e.g. extension of the timeline, updates to the initial standard, additional test cases, etc.

3.4.1 Activity 10: Perform Tests

To be certified solutions need to follow the test concept outlined in in Activity 8. Test cases may need to be updated to incorporate new requirements, changes in standards, or newly developed functionality. The test results will specify the tested component and test outcome (successful test, partially successful test or test failure). Required/recommended changes to the solution or standards will be discussed based on test results.

3.4.2 Activity 11: Iterative Updates to Solutions and Standard

Solutions and standards will be updated in an iterative process based on test results. Any changes should be discussed in the forums as appropriate.

3.4.3 Activity 12: Move Certified Solutions to Production and Publish Baseline Standard

In order to certify a solution the following requirements need to be met:

- The solution passed all mandatory tests successfully.
- The relevant observers and forums approved the solution.

Once the baseline standard has been proved robust enough and a critical mass of PSPs and solution providers are certified the data sharing standards can be published.

3.5 Step 5: Go-live and start Operations Monitoring

Early users of the temporary testing environment will be able to offer certified SME customer data exchange mechanisms and other value-added solutions from day one of the published standards. In this phase it is assumed that PSPs will be operating in the exchange of data for SMEs that wish to move bank accounts or take out a new banking product with a new provider.

Technical solution providers will already be able to support the early adopting institutions. These vendors will operate a proven solution compliant with the standards. Financial Institutions that want to participate at this point can select one of the vendors with confidence, or look at other vendors who are developing additional solutions (see Step 6).

3.5.1 Activity 13: Communication Strategy

As the success of KYC sharing will be mainly dependent on the level of participation by PSPs and the consent of their SME customers to share data, a communication strategy should be developed by the delivery body and owned by the governance body. The strategy should be tailored to articulate the advantages for SME customers (including online presence and publications in professional magazines). Trade bodies could also inform their members of the benefits and address any concerns they may have.

A separate communication strategy for PSPs and service providers should be developed to increase the adoption rate and ensure a continuous feedback loop between the data sharing framework participants.

3.5.2 Activity 14: Market Strategy

The governance body should develop a market strategy which defines the underlying business models, cost distribution models and incentive systems to encourage new market entrants, market forecasts and analysis.

In the event that necessary entrants to the market do not emerge as expected, the governance body must take remedial next steps e.g. encourage the development of core functionality that could be later offered by a commercially viable utility in the SME KYC environment.

3.5.3 Activity 15: Operations Monitoring

At this stage, the governance body priority will change to monitoring the risks in the data sharing environment and adoption. A communication and emergency plan needs to be developed for major security breaches in order to keep data safe at all times.

The governance body and all market participants will get access to reporting and MI data provided by the delivery body as part of the testing environment. The reporting requirements will be updated over time, based on feedback from the recipients and a constantly changing environment.

3.6 Step 6: Future Scope Extensions

At this stage the governance body will decide on the further role of the delivery body. One option is that the delivery body ceases to exist and that the governance body takes over the remaining responsibilities. In the case of a large expected number of future participants it is more likely that the delivery body will still be supporting this step. During this phase more Financial Institutions are expected to engage and develop their business case for participation and select their providers to support access to the data exchange environment.

3.6.1 Activity 16: Expansion Strategy

By mid-2020 it is envisaged that this data exchange initiative will evolve and new services will be offered by the TPSPs covering services across the KYC value chain (including data validation and customer screening). During this phase a decision will be made by the governance body as to whether the sandbox is still required to allow new technical providers to develop their solutions. This may increase participation fees. Continued access to the sandbox would allow new entrant PSPs to select vendors and establish connectivity with the market. If extended, the ownership and governance of the sandbox should be determined by the governance body and the forums.

3.6.2 Activity 17: Certification of new Entrants

If extended, the sandbox could be used by existing and new entrants to further test and certify their services. In the event that the operation of the sandbox does not continue, the process for validation and certification of new participants without the testing environment must be specified in the data sharing standards.

3.6.3 Activity 18: Further Development of Standards

On an ongoing basis the standards will be updated by the governance body based on feedback from the SME community and other participants, thus facilitating the extension of the range of services available – such as KYC Utilities, Digital identity, Identification and Verification, KYC data storage etc. The scope could be expanded to include:

- Liability transfer for the accuracy of the data shared.
- Liability for the accuracy of validation of data, where conducted by a third party.
- SMEs using their validated digital identity to validate other SMEs they do business with.

Appendix

Appendix 1: Test Cases

The following test cases are examples and need to be confirmed at a later stage, by both the governance body and the delivery body. The test cases are intended to confirm the technical capabilities as well as the establishment of the required governance structure in conformance with the defined framework.

Category	Potential test case (examples)
Sharing capabilities	A. Confirm that PSPs are able to share data based on the CMA business current account opening standard information set format. B. Confirm that participants are able to share evidentiary documentation (soft copies). C. Confirm that sharing capabilities can be monitored (e.g. #PSPs sharing whole CMA data set, #PSPs not sharing at least 50% of the fields).
Interoperability	D. Confirm that every PSP is able to request and receive information from other peers through the network established between the different data sharing solutions. E. Confirm that the interoperability issues can be monitored (e.g. between PSPs and service providers).
Operating Model	F. Confirm that PSPs respond to all data requests within an agreed SLA (outside the scope of the initial standard). G. Confirm reciprocity functionality, e.g. PSPs reporting back to the originating PSP in case of changes of customer data detected (outside the scope of the initial standard). H. Confirm that PSPs are able to register their participation in the environment.
Data	I. Confirm that the data exchange mechanism is meeting the format and completeness requirements required by the standard. J. Confirm that the future requirement of providing the target/beneficiary PSP with the last updated/validation date is possible.
Security and Privacy	K. Confirm that reporting of experienced security and privacy breaches can be reported to the delivery body. L. Confirm that data encryption is possible.
Compliance	M. Confirm that PSPs are able to report data inconsistencies to originating PSP. N. Confirm that the data exchange environment provides the ability to fully comply with all relevant regulations.
Customer awareness	O. Confirm that PSPs have set up the required processes and procedures to only share personal data when they receive consent from their customers.

Table 2: Potential test cases (examples)