YOTI

WHITE PAPER

Project Endeavour

A shared digital identity platform for UK retail customer mutualised KYC

September 2019

The purpose of this paper

Project Endeavour ("Endeavour") is a UK-focussed collaboration aiming to disrupt existing **Know Your Customer ("KYC")** standards and practices across regulated financial institutions, through an innovative proof of concept. This White Paper describes the high level use case, in order to promote interest in the proof of concept which is planned for late 2019 and running into 2020. It is written for executives of UK financial institutions who are keen for their participating teams to work collegiately, apply thought leadership and pursue an innovative and enhanced solution in a key area of regulatory compliance. Endeavour seeks to deliver a strong use case for the UK, based upon a unique architecture and approach, with a view to developing a scalable and global capability.

The objective

A shared platform which **regulated UK financial institutions ("firms")** can mutually access, and which employs the use of accurate and rich data, can deliver a utility of consistent and high quality **identity verification ("ID&V")** and **anti-money laundering ("AML")** data on individuals. This innovative approach is referred to as *mutualised KYC.* Endeavour proposes that **a digital identity platform ("DIP")** can be used as a shared platform for new-to-bank mutualised KYC.

The specific use case addressed in this paper will allow for firms to trust in the verified identity attributes held in *an individual's digital credentials wallet*, which is itself a secure app provided by a DIP. The digital credentials wallet can hold sufficient personal information, as custodian on behalf of an individual, which can be used for KYC due diligence on that person, before they may be onboarded as customer.

For firms, the solution can be scalable for a large and strategically important UK customer base, allowing firms to onboard *low risk*[1] or 'good' customers speedily without having to duplicate costly background searches, under a prescribed scenario.

1. The financial crime risk profile of a potential customer is determined as a result of a regulated firm's own financial crime risk assessment and will generally attempt to categorise that eventual customer as an inherent risk category or class based upon a variety of factors including their identity, product or service which they are trying to access and the channel of delivery. The risk category of the individual will generally then drive a treatment strategy for the ongoing monitoring checks and controls that should be undertaken on the customer.

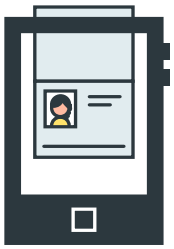
The use case

Endeavour focusses on an innovative proof of concept, that a secure DIP can be used as a shared platform for new-to-bank mutualised KYC for UK retail customers.

a) Fundamentals

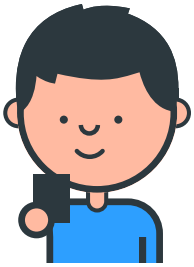
The Endeavour use case is based on five fundamental pillars:

1



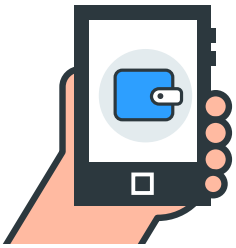
Individuals hold their personal information within a digital credentials wallet. The key to unlock this information is held securely and privately on the individual's mobile device. Only the user (and not even the DIP) can access their personal information.

2



The individual is in full control of their digital credentials wallet and they must consent to share it (in line with GDPR) with any *relying party*[2] of their choice. The digital credentials wallet is shared with firms under a decentralised model on a trusted network and on a mutualised basis.

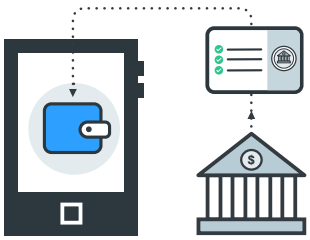
3



The digital credentials wallet must contain *sufficient verifiable* credentials for each and collectively all of the relying parties to be able to make an informed decision on the customer's financial crime risk profile. Verifiable credentials can be revoked at any time, which is important should either a firm or customer wish to terminate their relationship, or the financial crime risk profile of the customer changes.

2. A relying party is a third party who is requesting data on individuals, ie. firms who are seeking ID&V and AML data on individuals who are attempting to onboard with them and establish customer relationships.

4



If a new-to-bank relationship is established between an individual and a firm on the trusted network, then a further verifiable credential is returned to the customer's digital credentials wallet which the customer may then present to another firm on the trusted network, in seeking out a further relationship.

5

Absolute trust exists between the firms on the network, manifested through agreement of:

a. a consistent AML framework and unified standards;

b. the definition and approach to onboarding low risk customers;

c. the AML screening search and refine methodology employed; and

d. the content of the digital credentials wallet which holds the customer's verifiable credentials.

b) Customer product

The specific product under the use case shall be determined through deep-dive discussions with the participating firms at roundtable workshops. The initial focus could centre on onboarding for a standard current account which is ubiquitous as a financial services product. Additionally, many UK customers have already become accustomed to a digital channel for current account onboarding, as pioneered by several fintech banks who operate solely through user downloaded apps. It would be cleaner for the proof of concept scope to be focussed on KYC, without traditional credit scoring[3].

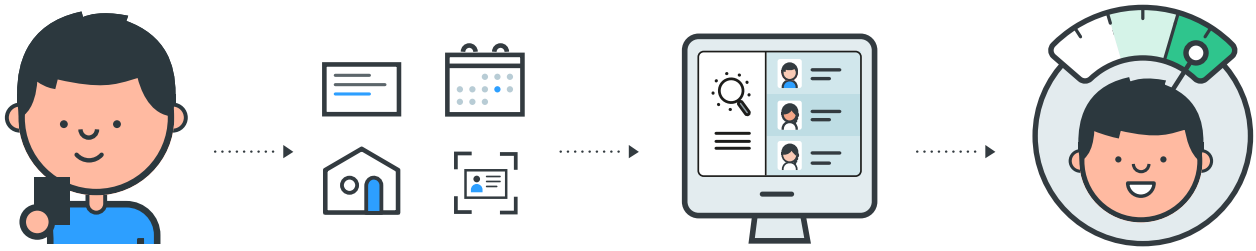
3. Credit scoring may initially be considered out of scope as it could require an expanded set of credentials versus what is required for KYC.

c) AML platform

The DIP will need to rely upon a partnership with an AML screening platform with access to extensive data, strong search methodologies and intelligent refinement algorithms. The methodologies and algorithms will need to be approved and trusted by the participating firms. The key technological requirement is the ability to intelligently refine the search results to sift out false positives and return *a point-in-time* index score (timestamped) against the unique identity of that individual. The index score can then be held as a verifiable credential in the individual's digital credentials wallet for the purpose of data sharing with the relying party at the point of onboarding.

The third party AML screening platform(s) will be determined by a Request For Proposal by the firms who choose to participate in Endeavour at the earliest opportunity. Key high level considerations will be the quality of their enriched data sources, ability to create intelligent algorithms to push out false positives and to generate a returning index score based upon robust probabilistic assumptions.

As a result, if brought to a full scale production environment, a competitive marketplace will be established for AML platforms to provide enriched data sourcing, intelligent name screening and robust index scoring on individuals for the new-to-bank customer proposition.



User shares their ID&V attributes using the DIP's app

AML Screening

Index score

d) Onboarding protocol

If an individual chooses to share their digital credentials with a firm on the trusted network, the onboarding protocol should revert to a predetermined view of what a low risk customer looks like. Based on the content of the digital credentials wallet information shared with the relying party, if the individual appears to be low risk then an immediate determination can be made as to whether the individual can be onboarded as a customer.

Crucially, the same firm then returns a new credential[4] to the customer's digital credentials wallet, confirming that a new-to-bank relationship has been created. This credential can then be shared with another firm on the network who trusts that the previous firm (undisclosed and anonymised) was satisfied that the customer presented appropriate and satisfactory credentials at a specific point-in-time previously.

e) Consistency of framework, standards and risk assessment

The key requirement of the participating firms is to agree a consistent, shared and trusted AML framework and set of standards, such that the approach to risk assessing and defining what a low risk customer looks like can be agreed in principle.

An agreed threshold will be required to be determined against the returning index score, such that low risk customers can be identified and onboarded in a fast and automated way. Equally, it should also be determined to what extent a returning index score can be relied upon for a qualified low risk customer by another relying party. This might be for a specified finite time duration (ie. within X days of timestamp) or it may be determined that refreshed index scores are required per onboarding attempt.

The framework, standards and approach to risk assessment must be agreed by all parties to be aligned to the **Joint Money Laundering Steering Group Guidance for the UK Financial Sector (2017) ("JMLSG guidance")** minimum standards or above.

4. This credential shall be time and date stamped but can be revoked, if required, as a result of ongoing monitoring checks which lead to concern for a customer's risk profile.

f) Blockchain

Endeavour will utilise a permissioned **Distributed Ledger Technology ("DLT")** as a platform for the following reasons:

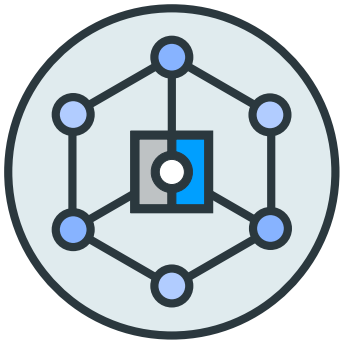
1. The ledger[5] is fully transparent and every share in the ledger is timestamped providing an immutable and auditable history of transactions.

2. The ledger is tamper-proof and provides a secure vehicle to share information.

3. Only trusted, authorised relying parties who are members of the network will have access to write on the ledger.

4. The technology is decentralised which means that individuals can receive credentials from any trusted relying party to enrich their profile and this information can be shared with other relying parties. Participating firms can grant a new credential to each new customer, for example sort code and account number.

5. No **Personal information[6] ("PI")** is written to the ledger in order for the solution to be GDPR compliant. PI is only stored in a (i) secured identity container, which is deployed in the individual's digital credentials wallet of the DIP, and (ii) the encrypted databases owned by relying parties who are authorised to access the PI.



5. Endeavour will use the Corda blockchain network, owned by R3, which has been chosen due to its strong levels of privacy and security.

6. Personal information is any data that could potentially identify a specific individual.

g) Effective outcome

In the way described above, a mutualised KYC framework will be designed in order to onboard rapidly and securely the vast majority of UK customers, who might be considered to be low risk as a result of a well defined, agreed and consistent financial crime review methodology. The solution will comply with UK AML regulations to the satisfaction of the participating firms.

Endeavour will aim to validate the results of a live trial run on a pool of UK customers, such that the proof of concept can be taken forwards into a production environment as it demonstrates tangible value for UK regulated financial institutions and showcases their position as leaders in regulatory technological innovation on a global stage.

It is anticipated that the FCA will show a keen interest to oversee the progress made under Endeavour.

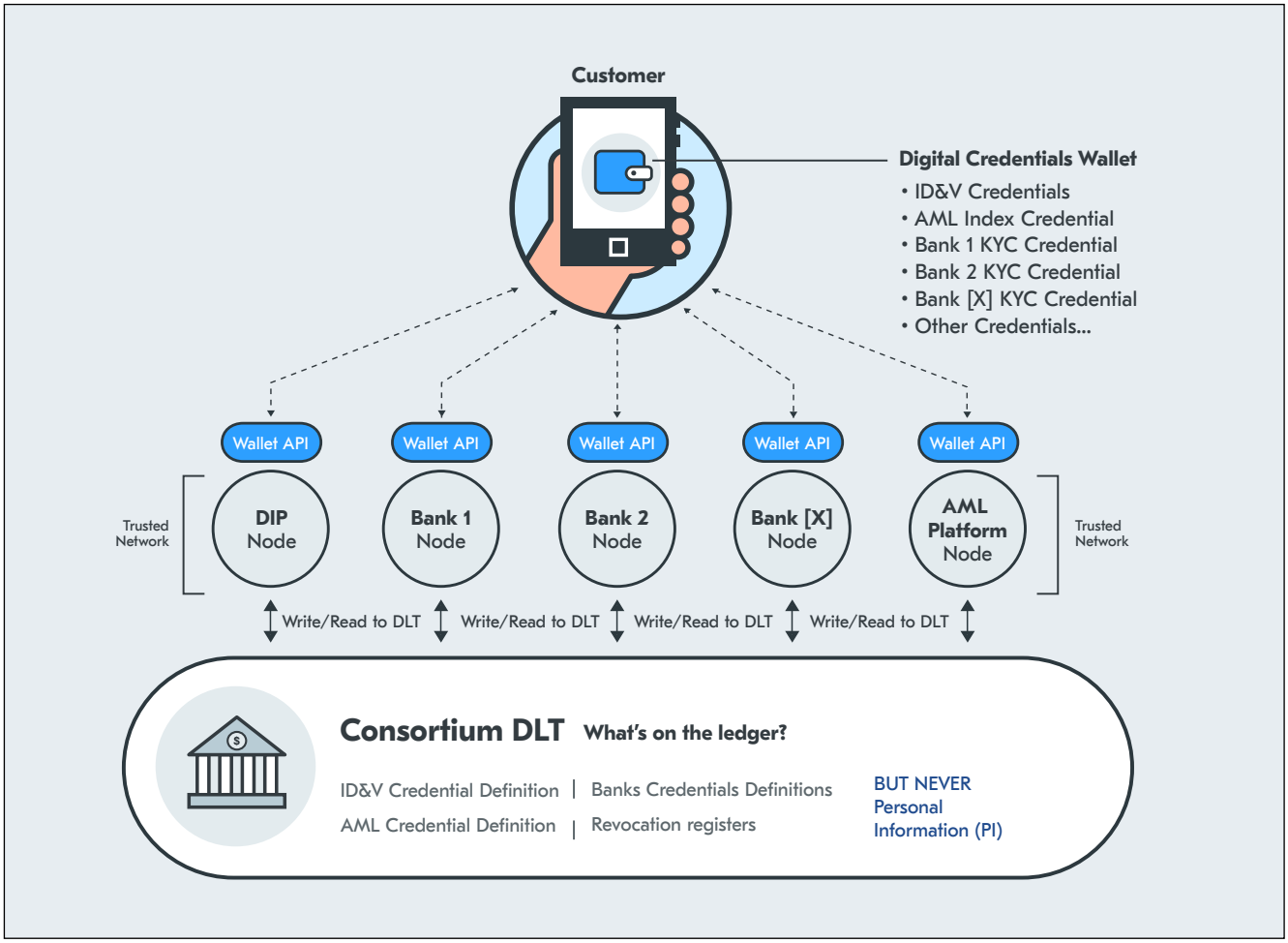


Figure 1: schematic representation for how Endeavour envisages that a mutualised KYC shared platform could function on DLT

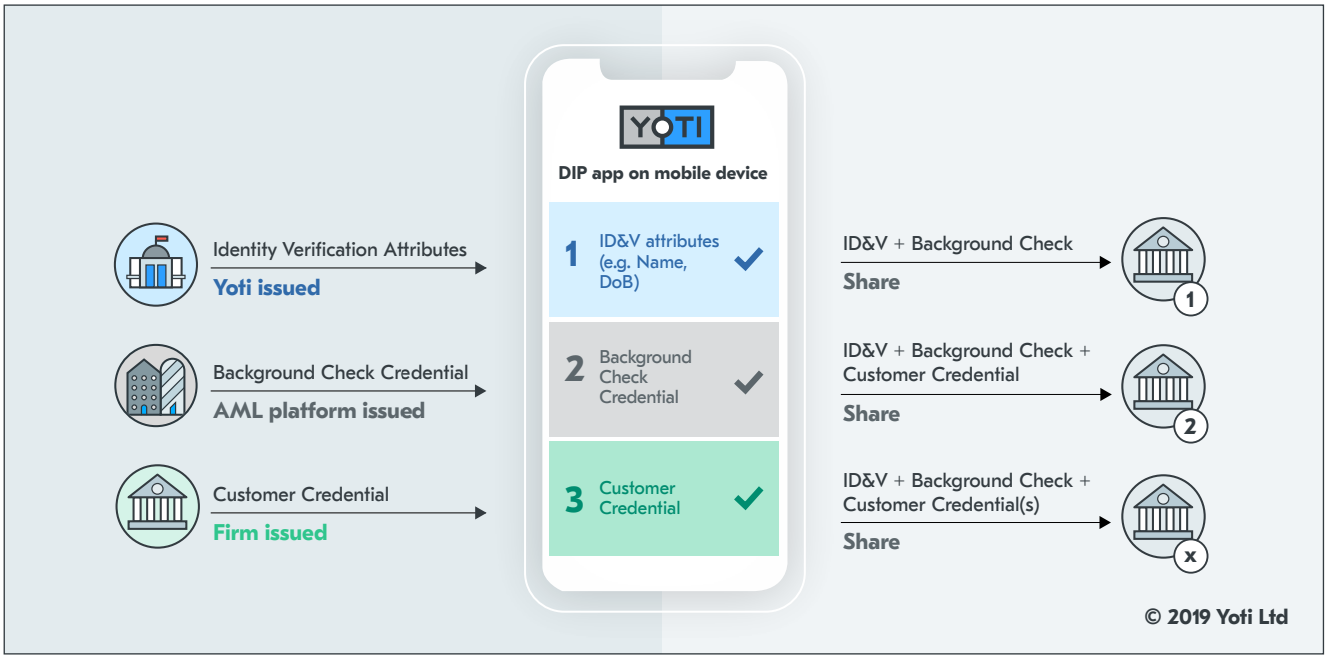


Figure 2: Digital credentials wallet summary

Why is this important?

Money Laundering and terrorist financing continue to be major concerns for the global finance sector. According to the National Crime Association, over £100 billion is laundered in the UK every year[7]. The Home Office concurs with this value[8]. These funds are being channelled from a range of exploitative and violent crimes, including people trafficking and drug dealing.

KYC is a fundamental requirement for firms in the fight against money laundering and terrorist financing. KYC, in general terms, requires a firm to be both confident in the identity of an individual and have enough knowledge of that person to be able to determine how much of a money laundering or terrorist financing risk they might present, before being onboarded as a customer.

As part of a KYC check, a **Client Due Diligence ("CDD")** file is required to be created on an individual (i.e. someone who does not have an existing relationship with the firm), which needs to be approved by both the customer-facing business and compliance function of the firm, before accepting that person as a new customer. However, from a customer's perspective, KYC can be slow and frustrating. Each firm has to perform its own KYC check per individual customer, often duplicating the same search that another firm may have done very recently.

An outcome of the KYC review is a need to determine whether the true identity of an individual is matched against relevant money laundering, terrorist financing, Politically Exposed Persons and sanctions searches, criminal and fraud databases, and adverse media reports.

7. https://nationalcrimeagency.gov.uk/news/national-economic-crime-centre-leads-push-to-identify-money-laundering-activity

8. https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/

Convergence of Fraud within Economic Crime

The Government's Economic Crime Plan for 2019-2020 specifically calls out public-private collaboration as a key driver in both understanding the threat of economic crime and helping mitigate the ongoing risk created by both fraud and money laundering. This need is driven by multiple trends across the industry, including the convergence of fraud and wider economic crime.

Regulatory compliance and customer due diligence is costing in excess of £650million per year in staff costs alone according to recent figures from the FCA[9], notwithstanding the duplicate costs in data, systems and processes when understanding fraud risk compared to AML/CTF risk.

There is significant overlap between the fraud risk associated with an individual and their propensity to engage in money laundering and/or terrorist financing. Organised criminal groups funded by nation states are using fraud as a key revenue generation stream and banks are starting to tackle this by consolidating resource between the previously disparate areas of fraud and AML/CTF.

In a world where auto-decisioning is becoming the norm rather than the exception, there should be a greater focus on gathering as much information as possible during the KYC process from best-in-class third party data sources to further understand underlying customer risk.

Customer risk assessment

It is apparent from the firms' own customer risk assessments that low risk customers account for the vast majority of the UK retail banking customer base. It is therefore beneficial for firms to be able to agree a unified and consistent framework for the approach to identifying low risk customers (Endeavour will focus on a prescribed onboarding use case), through a digital channel. Such a framework would need to comply with the specific guidance under the published JMLSG guidance.

In order to determine whether a customer is low risk, the various relying parties need to be assured of the individual's i) truly verified identity and ii) associated financial crime risk profile as a result of detailed screening. Fast and robust identification of low risk customers can reduce a vast amount of time and cost spent on performing due diligence on a large proportion of any firm's retail customer book. This in turn will allow customer-facing business units and compliance functions to focus more time and resources on higher financial crime risk individuals, who are more likely to be bad actors.

9. FCA paper "Financial crime: analysis of firms' data" (November 2018)

The role of the Digital Identity Platform

DIPs provide a secure way for individuals to prove who they are to access products and services. This is an important development for a digital economy, where consumers prefer to transact in a trusted manner through digital channels, such as websites and mobile apps.

DIPs can read specific personal information details about an individual (first name, surname, date of birth, etc.) from authentic government issued sources, verify that they are true and that they belong to the individual, and ultimately permit the individual to share them with requesting third parties over digital channels. Individual identity details are often referred to as attributes, and requesting third parties are often referred to as relying parties.

Endeavour will make use of information about the individual. In this case the DIP will incorporate records of individuals' unique physical characteristics through creating a facial template, based on a successful liveness test[10]. The DIP will then review government-issued photographic identity documentation submitted by the subject to match the photograph of the individual against their facial, which has been previously validated by the liveness test. Submitted government-issued photographic identity documentation can be checked against specific security features for authenticity.

10. A liveness test will determine whether an individual is a true individual and must employ robust anti-facial spoofing techniques. It must be quick and easy to use and provide a level of assurance that the relying party can accept.

Individuals with an E-Passport and a **Near Field Communication ("NFC[11]")** enabled device can be cryptographically verified by using public keys sourced from the International Civil Aviation Organization's Public Key Directory. This is aligned to global standard used for international border checks[12]. DIPs can utilise NFC enabled device capability for this purpose on both Android and iPhone devices from September 2019.

Innovative methodologies, such as that described above, give rise to high quality ID&V assurance for a *Generation Z* UK customer base, who are typically early adopters of mobile device technology and will expect to be able to share data and transact in this way. This permits firms to establish and build deep credentials with a strategically important UK customer base who have traditionally had *thin files.*

Once the identity of the individual has been verified, images of the documentation and relevant identity attributes can be remitted as data files to the relying party to establish the basis of a CDD file.

The DIP needs to be trustworthy. All parties involved should be able to rely upon the ID&V methodology employed with confidence, in order to be able to trust in the identity of an individual beyond reasonable doubt. At the very least, the methodology needs to be demonstrably stronger than the majority of the processes employed by many firms today.

It is expected that there will be a rapid increase in DIP adoption in the UK given the increasing number of use cases required by legislation (ie. age verification for an increasing number of retail goods, most recently now including energy drinks). This will mean that within the next year DIPs will begin to be able to build up a significant behavioural profile of their users through their identity sharing patterns, although data protection and privacy rules may limit this to metadata.

11. Near-field communication capability enables devices to perform contactless functions such as interrogating a chip on a passport or making a contactless payment.

12. https://www.icao.int/Security/FAL/PKD/Pages/default.aspx

Next steps

A select group of UK authorised firms will be invited to participate as part of the Endeavour proof of concept. Workshops with relevant and appropriate stakeholders from interested firms will be arranged in order to provide further details about Endeavour. This includes an introduction to the detailed use case, initial discussion of the commercial model and technical solution architecture. Workshops are scheduled to take place throughout October 2019.

Roundtables with confirmed participant firms are scheduled to be held over the remainder of 2019 and into early 2020 to work on the mutualised KYC framework, standards and protocols, the approach to risk assessment and index scoring, ID&V methodology, solution architecture design, and testing and audit plan. This will all be set out under a formal programme management plan and governance structure.

The building of the solution architecture and full integration with participant banking platforms will take place before the pilot trial which will take place from mid 2020.

Annex 1 - Importance of Digital Identity Platforms in financial services

The UK banking industry is going through a crucial period of transformation as it embraces the digital revolution under a myriad of IT transformation programmes. Technological innovation is now being explored seriously and the practical application of many use cases are being considered where there is a perceived benefit from a cost and efficiency perspective, or notably where solutions can offer enhanced compliance with regulatory requirements.

Digital identity and the associated extension of an individual's identity, can and should be explored to manage and reduce financial crime risk, notably new-to-bank KYC onboarding processes are ripe for review in this context. DIPs offer regulated firms the opportunity to:

1. Reduce the cost of labour
2. Dispense with paper trails and physical CDD files
3. Digitalise a key process underpinning customer facing activities
4. Speed up execution of customer onboarding services
5. Tighten up the control environment and enhance regulatory standards
6. Improve the customer experience and onboarding journey
7. Improve GDPR practices with the digitalisation of ID&V document images
8. Automate KYC data capture for better reporting and governance oversight

Traditionally, new-to-bank customers have used paper-based documents to prove who they are. This commonly requires the customer to present their identity documents in-person to staff, who may not be highly skilled in checking security features to ascertain the authenticity of identity documents, particularly when documentation is issued from an overseas jurisdiction. There is a clear risk of identity fraud under this method and it is inconvenient for individuals to attend in-person meetings as part of the legacy customer journey.

AML controls and KYC risk assessments still present considerable risk management issues for financial institutions all over the world and regulators continue to press enforcement actions where they have found evidence of malpractice in this regard. This leads to financial crime risk management being a common point of concern for consumer-facing businesses and compliance functions at firms.

The Senior Managers & Certification Regime bestows a legal *Duty of Responsibility* on executives, which in turn confers personal liability. Being able to evidence that reasonable steps have been taken to ensure appropriate risk management is in place for systems and controls is paramount. Those with executive responsibility for customer-focussed businesses are required to be able to articulate and detail specific risk mitigation factors related to AML and KYC.

DIPs will therefore be of considerable interest to (regulatory-approved) Senior Manager Functions who bear the full weight of regulatory responsibility for managing their businesses and the inherent customer risks.

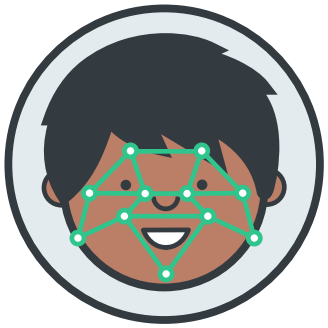
It is cost-efficient to be able to accept electronic proof-of-identity rather than have branch network staff manually check and process identity documents. DIPs have already been embraced as a proof of concept, as can be seen by the wave of newly authorised fintech banks (without physical presences) who are onboarding increasing numbers of UK customers, by making use of consumers' growing reliance and affiliation with mobile devices. Many firms are unwilling or unable to develop their own bespoke DIPs in the short-to-medium term, with the technological and security challenges, as well as the cost barrier-to-entry that this entails, when they could instead integrate quickly, securely and cheaply with an existing, proven and available DIP solution.

Annex 2 - Verifiable credentials

Credentials are part of our daily lives and they are often used to attest individuals' abilities to perform particular activities or to prove that they have certain experience. Driving licences are issued to prove that someone is capable of driving an automobile, passports prove someone's identity for cross-border travel and diplomas evidence that students have a level of education.

Verifiable credentials are identity attributes that are assured by a trusted third party reference source and can be used to evidence the true identity of an individual, as well as specific aspects of that individual's identity.

DIPs can evidence verifiable credentials by returning searches from credible databases or through confirming that identity attributes have been taken from authenticated government-issued identity documents. Verifiable credentials are therefore created where identity attributes can be proven as trusted from source.



For example, an individual's first name, surname and date of birth can be used by a relying party to identify who that person is. These identity attributes are displayed on the individual's passport, so if the passport can be authenticated (for example, as discussed earlier by cryptographic reading of the passport chip and matching the face in the passport photo to the sourced facial of the individual) then it can be concluded to a strong level of assurance that it belongs to the individual in question. The first name, surname and date of birth can then be considered to be verifiable credentials, which a relying party can trust.

Known third party organisations within a trusted network can issue verifiable credentials to individuals, for that DIP to hold in a digital credentials wallet on their behalf. This has positive implications for utility providers, educational institutions, government departments, employers and even landlords, to provide verifiable credentials for individuals. The individual can then choose to share any or all verifiable credentials with a relying party, which may then be accepted as a source of truth.

Importantly, verifiable credentials can also be revoked. This means that if, for example, an individual has a change in circumstance and the credential or the specific data held as that credential no longer applies or exists, then that person should not be able to share it anymore until it has been re-verified.

Verifiable credentials can be stored in the digital credentials wallet, as part of an individual's digital identity. Under an agreed and trusted framework which is aligned to the JMLSG guidance, an individual should then be able to present appropriate and satisfactory verifiable credentials to a firm as a relying party, in order to prove that they might be considered appropriate to be granted quick and easy access to a product or service.

In order for new B2C relationships to be created in this manner, through digital channel KYC onboarding, the sharing of identity attributes as verifiable credentials will need to be deemed acceptable under an agreed framework of KYC standards and practices.

Annex 3 - Data security and privacy

It is imperative that DIPs are designed in a way that aligns with global privacy regulations in order to protect the customer's identity. DIP solutions should follow a privacy and security-by-design approach to ensure that the technology architecture protects the confidentiality and security of individual customer data.

This implies that an individual may only share their identity attributes with a relying party if they can confirm that it is the firm who they expect it to be. They may then proceed to consent to that share of their data in real time.

Furthermore, DIPs can assist firms to comply with privacy regulations. They can enable increased transparency, making clear to customers what identity data is being requested before the consent to share is granted.

DIPs can also allow firms to readily comply with the data minimisation privacy principle, as they may only request personal data which is absolutely necessary for the relevant transaction. DIP solutions can also ensure the accuracy and reliability of the data, taking that responsibility off the firm entirely.

Contact detail

To find out more details about Endeavour and how to get involved please contact:

Gareth Narinesingh

Yoti Commercial Director - Financial Services,
Project Endeavour Director
gareth.narinesingh@yoti.com

Ana Salazar

Yoti Business Development - Financial Services,
Project Endeavour Manager
ana.salazar@yoti.com

Miguel Jimenez

Yoti Blockchain Engineer,
Project Endeavour,
Technical Lead
miguel.jimenez@yoti.com

To find out more visit

yoti.com

Download on the App Store

GET IT ON Google Play