Finda Systems (Asia) Pte Ltd
51 Goldhill Plaza #07-10/11
Singapore 308900

DIGITAL KYC PROOF-OF-CONCEPT WHITE-PAPER 1

Overview of the Digital KYC authentication system

1. INTRODUCTION

“Fraud Management Insight 2017” reported that consumers in Indonesia experienced Financial Service Fraud at least once over 12 months, at 49.8% against the Asia Pacific average of 34.7%. Singapore consumers have the highest trust towards the government at 75.5% against the Asia Pacific average of 51.7%. The trust of personal data protection is centered on government agencies. Most Thai consumers believe business entities severely lack fraud detection capabilities and speed in response to fraud incidents at 60.5% against the Asia Pacific average of 47.7%.

The worldwide Anti-Money Laundering (AML) compliance landscape has changed enormously over the past years, with increasing layers of regulation added in many jurisdictions to strengthen the financial system against money laundering, terrorist financing and other financial crimes. Regulations and regulatory enforcement have continued to become more stringent, with substantial fines being levied where breaches have been identified.

In response to this continuing regulatory change, regulated institutions have built substantial operations to enable compliance and mitigate the risk of financial crime. These activities have consisted of changes to processes, new supporting IT systems and the development of entirely new operational areas. Collectively, this has resulted in a considerable overhead for regulated institutions.

We have also seen an enormous amount of technological change. This has accelerated in recent years with the growth of the compliance technology sector in many mature Financial Services markets. These disruptive and additive technologies have enormous potential in transforming Financial Services, with many having prominent use cases impacting financial crime compliance, particularly AML.

The regulated institutions are taking diverse approaches, both in the area of AML lifecycle and the technologies they are investing in. Many are taking priority of Risk Aversion and clear preference for proven capability when possible.

2. KYC CHALLENGES

The KYC process, which protects against Money Laundering (ML) and Terrorism Financing (TF) violations, have seen inconsistent levels of adoption amongst regulated institutions due to:

a) Limited Budget. Cost remains a key consideration for regulated institutions. A new technology would be adopted if it could provide financial and compliance benefits, at the existing stage the quality of Customer Due Diligence (CDD) could be compromised due to cost impact.

b) Lack of internal capabilities. Internal challenges were another barrier for adopting complex emerging technologies such as blockchain or machine learning due to perceived lack of internal technology capabilities.

c) Lack of shared utilities. Each CDD is conducted in isolation by each regulated institution. There was no sharing of CDD information.

d) Onboarding cycle. Long processing time to onboard a customer as CDD process involving manual documentation scanning could take a long time but quality of CDD remains low.

e) Need for regional standardization. The larger regulated institutions that operate over different jurisdictions would require a degree of standardization across those jurisdictions. Technology providers that lack the regional reach were unlikely to be considered.

In summary, there are prioritizations and challenges faced by the regulated institutions towards AML technology adoption.

3. DIGITAL KYC LIFE-CYCLE

Physical identity was designed to enable face-to-face transactions among entities. It aims to provide the means to determine whether an entity is who/what it claims to be through a set of attributes such as a driver's license, company ID, device serial number and through visual, line-of-sight means.

Digital identity enables transactions in the digital world and offers improved functionality for its user as well as efficiency for the institutions. Through a set of electronic attributes such as biometric templates, online browsing records and phone numbers, digital identity aims to allow identification of an entity online or remotely through electronic means.

Digital KYC lifecycle could be broken down into FOUR fundamental questions as table 1 defining how an entity should know their customer.

Identity	Question	Description
I1	Who are you?	Determining and verifying an identity e.g. passport, driving license, identity card

I2	What do you want to do?	Monitoring transactions for suspicious activities, identifying source of funds.
I3	Are you identified in the “blacklist”?	Uncovering politically exposed persons (PEPs), sanctions or terrorists and profiles, criminals and others
I4	Are you identified as who you are?	Performing Customer Due Diligence (CDD) during onboarding, and ongoing CDD as identity and client activities may change over time.

Table 1: Digital KYC fundamental questions

4. CURRENT DIGITAL KYC AUTHENTICATION PROCESS

Table 2 lists the current digital KYC authentication process and our assessment in addressing KYC lifecycle.

	Method	Description	I1	I2	I3	I4
1	PIN or Password	As one of the most traditional and widespread methods of verifying user identities, passwords are the de-facto mode of digital KYC today. The biggest benefit of a password-based system is that it is cheap to implement. All that is needed is a simple form where a username and the password is created when registering, and a database for storing the username and password (in encrypted format). The simple and straightforward implementation of a password-based authentication system is its biggest benefit. However, password is not strong by any means. Even if the registration process is rigorous, the method itself is too	Y	Y	N	N

		vulnerable.				
2	One-time Passwords (OTP)	Banks started to issue OTP lists to their customers already in the 90’s. Today OTPs can be seen in many forms from these printed OTP lists, SMSs, tokens generating OTPs to mobile apps. There is existing standards on how to generate OTPs. As the name suggests OTPs are for one-time use which makes it a stronger alternative compared to passwords. A typical OTP is a string of random numbers (4-8 long). During authentication the user needs to lookup (from the list) or generate an OTP using a token or an app that is then written to the web authentication form. Generated OTPs are usually valid for a short period of time allowing some time for the user to write it to the form and minimizing the possibility of a replay attack. SMS based OTPs are sent to the registered mobile phone number of the user. The convenience of an OTP system is lower than passwords and the fact that the user has to carry the list or specific token is a disadvantage. Tokens are also fairly costly for the service provider. In the long run, it is necessary to replace them (battery, broken) or issue a new one (lost token). OTPs are almost always combined with a password, lowering the convenience even further. To reach the highest level of Authenticator Assurance Level of the new NIST guidelines, a single-factor OTP authenticator must be combined with at least multi-factor device or software, or additional single-factor and a memorized secret (PIN, password, passcode). On the security front OTPs have a few issues. SMS-based OTPs are no longer recommended by the NIST guidelines as e.g. a smart phone malware can capture it, or the gateway used to send the message can be hacked (SS7 vulnerabilities). The other issue is that like the password, the user can unintentionally reveal the OTP.	Y	Y	N	N

3	Biometrics	The emergence of fingerprint reader equipped smart phones has raised biometrics as one of the strong alternatives to authenticate a user. There are plenty of different options for biometrics starting with the fingerprint, facial, voice, iris to even behavior. If it can be measured and a template can be created and repeated for comparing purposes, it can be used as a biometric identifier. The best part of the biometric authentication method is in the usability. If the biometric authentication scheme can leverage e.g. the fingerprint reader on a modern smart phone, it outshines most other methods in terms of convenience. Other, perhaps more obscure, methods can have questionable convenience, but the proliferation of smart phones with biometric capabilities should ensure that they are the main devices where biometric authentication will be implemented. Relying solely on biometric authentication is much more complex effort and can result into biometric database breaches as the templates need to be stored somewhere centrally. Another downside of a biometric factor is that it's almost impossible to change once the biometric data is stolen.	Y	Y	Y	Y
4	Multi-factor authentication (MFA)	It means that more than one factor is used to verify the identity. The main categories of these factors are • Something that you know (password, PIN code, answer to a secret question) • Something that you have (token, smart card, phone) • Something that you are (fingerprint, face, eye, blood vessel pattern, heartbeat, DNA, behavior) By combining these factors we get a multi-factor authentication scheme. Multifactor does not automatically mean that you have a strong authentication method. A good multi-factor authentication integrates at least one strong factor (such as biometrics) into the method. Note that the NIST Authenticator Assurance Level 3 requires that at least part of the multi-factor authentication scheme be implemented using a device.	Y	Y	Y	Y

5	Shared Utilities	Shared Utilities can involve the use of a secured distributed ledger such as blockchain technology to build Know Your Customer utilities. A KYC Utility provides a centralized location where customer identification and verification can be performed once for a customer, rather than several times by different regulated institutions for the same customer.	Y	Y	Y	Y

Table 2: Current Digital KYC authentication matrix

5. DIGITAL KYC AUTHENTICATION SOLUTIONS

As depicted in figure 1, KYC involves three major parts: Customer Onboarding and Maintenance, Transaction Monitoring and Filtering, and Reporting and Management Information.

a. Customer onboarding and maintenance

The current onboarding processes at many financial institutions are anachronistic. How can you prove who you are? This rather existential question sits at the heart of regulated institutions’ fight against the risk of financial crime and is the main challenge for the future of client onboarding. Particularly in an age where financial institutions rarely interact with their customers face-to-face, how can these institutions really know their customer? Technology provides a solution to this conundrum, provided that regulations can keep pace with technological developments. Having visibility across the market of the full range of Know Your Customer (KYC) identification and verification innovations that are out there enables us to see how they are driving divergent approaches to customer onboarding.

Current processes for client onboarding employed by many financial services organizations in Customer Due Diligence (CDD) involves collecting documents or individually engaging credit reference agencies to verify customer identity against other independent data sources on their behalf. This poses a number of challenges as below:

i. Access - we are seeing pressure from society for immediate services. Customers' expectations nowadays demand easy access to financial services and certainly no longer include physically coming into a branch.

ii. Time consuming - numerous reviews that we have performed at financial services institutions have illustrated that the time it takes to onboard a customer can be very long. This is costly for the bank and frustrating for the customer.

iii. Variable quality - the remediation exercises that we have performed have shown that compliance officers set due diligence standards to varying degrees of rigor, resulting in varying strength of KYC documentation obtained.

Customer onboarding and maintenance is one of the parts of AML lifecycle where regulated institutions already make use of technologies solutions. They are:

i. Services from third party data providers, including AML/KYC firms and credit rating agencies. However, the underlying data needs to be regularly updated, otherwise resulting in inaccurate decisions about customers.

ii. Performing enhanced due diligence and adverse media searches, both were labor-intensive.

iii. The use of biometric has become prevalent in the customer maintenance purposes. These include voice-based biometric for telephony contact centers. This has shown improvement in customer experience and reduces fraud. Device based biometrics for digital interaction with customers, particularly the use of fingerprint scanning. This was perceived as low cost, and provided additional security and frictionless interaction (than having to enter

PIN or equivalent). More complex biometric including facial recognition, iris recognition were an area for consideration.

iv. Utility technologies and KYC/AML data sharing across regulated institutions would become reality eventually. This could be accelerated through the intervention of regulators.

v. Data analytics and machine learning within utilities could have enormous impact in terms of identifying and preventing fraud, AML and terrorist financing. Advanced analytics technologies such as Natural Language Processing (NLP) would offer enormous operational benefits, particularly in automating existing manual processes such as scanned documents, adverse media searches.

vi. Shared Utilities involves the use of blockchain technology to build Know Your Customer utilities. A KYC Utility provides a centralized location where customer identification and verification can be performed once for a customer, rather than several times by different regulated institutions for the same customer.

vii. The use of banking chatbots that leverages on artificial intelligence (AI) in the hopes of automating responses to client queries online is a bold step. Automation has swept through the banking industry in recent years, convincing firms to embrace digitalization and reap the efficiency gains it brings.

b. Transaction Monitoring and filtering

This was considered an area as having the most potential for the adoption of new and emerging technologies. Technologies in this area are used to monitor and filter transactions, preventing those that might go to the sanctioned countries, entities and individuals and identifying those with a high risk of fraud or money laundering. The existing technology consists of decision-tree based system, which works with defined rule sets to identify outliers and trigger alerts. This includes transaction of unusual amount and in an unusual location. The nature of the rule sets and data quality issues might lead to enormous volume of alerts that require laborious manual review. This often results in true suspicious transaction only detected sometime after the transaction has been completed. Emerging technologies in transaction monitoring and filtering are:

a) Big data analytics – this involves consolidating of data into data lakes, with associated analytics.

b) Real-time transaction analysis together with device-based recognition system and data analytic to reduce the false alerts.

c) Machine learning within the data analytics option is common consideration.

d) Blockchain or distributed ledger technologies have been considered to meet regulatory requirements, for its ability of processing power and theoretical ability to meet traceability and auditability.

c. Reporting and management information

New and emerging technologies could offer considerable advantages and operational improvements to regulated institutions in this area. In particular, data analytics and machine learning technologies has the potential to rapidly reduce the number of potential Suspicious Activity Report (SAR) needing human review or intervention.

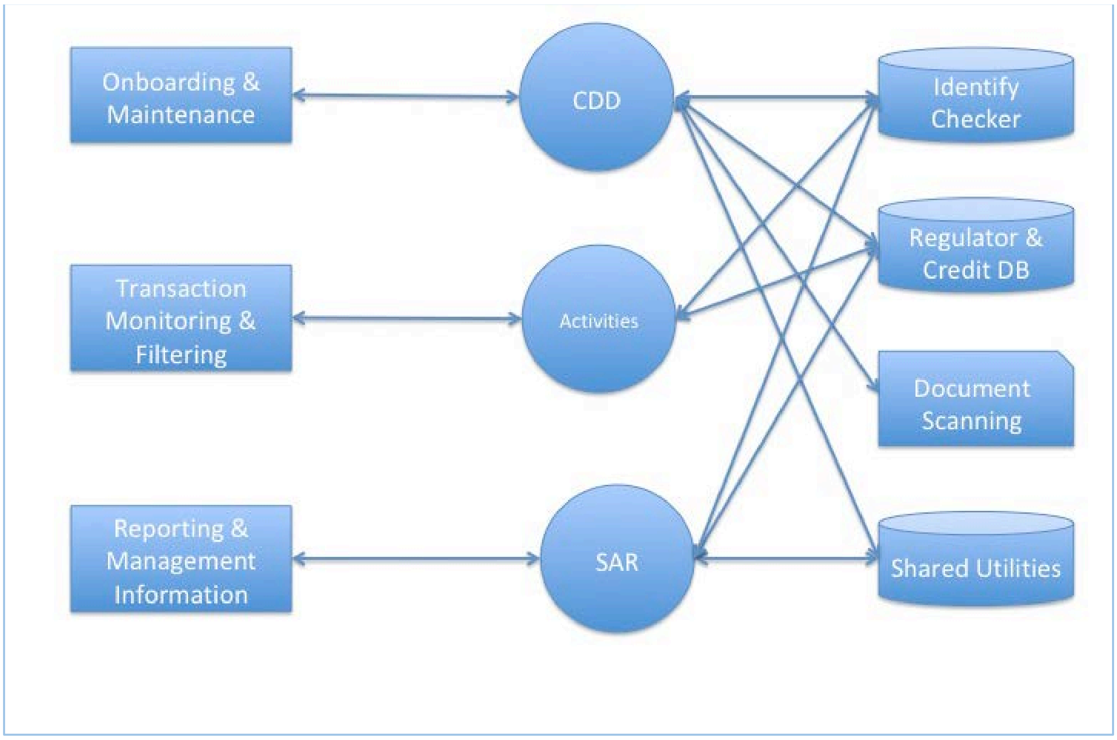

Figure 1: Digital KYC Authentication Solutions

6. CHALLENGES FACED BY KYC TECH FIRMS

Despite the huge potential in digital KYC, tech firms continue to face challenges in offering the solutions to institutions. The following are the reasons:

a) Larger regulated institutions have established arrangement with large providers and unwilling to work with new provider

b) Regulated institutions have low appetite in the space with the possible high risk of using unproven emerging technologies, both from regulatory and operational perspective.

c) Changing regulatory environment is fundamentally a challenge. Smaller providers lack the bandwidth to perform robust horizon scanning for regulatory change.

d) Ability of scale for smaller providers is a key barrier of entry.

e) Disconnection between IT and operations staff within regulated institutions.

f) Lack of regulated standards across data security and identity verification requirements.

g) Increased data privacy consideration is restricting the development of efficient and cheaper options for analyzing data.

h) Lead-time for designing, developing and testing new regulatory technology remains lengthy due to the need to continually assure compliance.

i) Data remains a thematic issue, both in terms of security / protection inherent in any sharing of data, as well as challenges of working with volumes of data.

j) Without a functioning government digital identity service, adoption in Financial Services would be slow.

k) Without clear standards and definitions being laid down by a government body or a regulator, it is a difficult area in which to build technology.

7. ALLIANCE FOR FINANCIAL STABILITY WITH INFORMATION TECHNOLOGY (AFS-IT)

As the digital revolution in finance accelerates across the wider Asian region and beyond, the Alliance for Financial Stability with Information Technology (“AFS-IT”) seeks to provide a non-governmental platform for international collaborative efforts by central banks and monetary authorities, financial regulators, professionals and technology experts to strengthen systemic financial stability and market security. In particular, one of the Alliance’s key roles is to propose and establish a set of Digital Know Your Customer (KYC) Standards collectively with partner countries in the region.

Guiding Principles for the Digital KYC Standards

a) Conformity with International standards and fundamentals: the Digital KYC standards should ensure conformity with the standards, recommendations and fundamental principles of major international financial standard-setting organisations such as Financial Action Task Force (FATF), International Monetary Fund (IMF) and Basel Committee on Banking Supervision (BCBS) etc.

b) Respecting local legal and regulatory circumstances: for regional or international standards to be applicable to multiple jurisdictions, the Digital KYC Standards should respect the local legal and regulatory circumstances of the relevant markets and should not seek to create new legal obligations or hindrances. The standards should provide guidelines to effectively address the problems for the region while allowing flexibility for each local regulator to customize and tailor based on local requirement and circumstances.

c) Respecting Personal Data Privacy: with the immense benefit of the personal digital data collected, the standard should ensure that personal data is secure and protected and that the use of such information will not be abused. Any risks should be carefully mitigated and addressed in accordance with local regulatory requirements.

d) Inter-operability and Compatibility: the Digital KYC Standards should ensure inter-operability and compatibility with international major financial transaction systems and information operating systems, approved by professional financial bodies. The Standards should also endeavor to work and collaborate with Fintech/Regtech companies, 3rd party payment platforms and local finance communities in the areas of knowledge-sharing and research.

e) Ensuring efficiency: a set of effective Digital KYC Standards should be commercially viable and practical to be implemented with quality, and without causing significant impact on the efficiency of the relevant operations. If a standard introduces certain checking or validation in the operations, it should also focus on the issue of efficiency from the end-to-end perspective for better customer experience. The verification of standards should be considered in a practical and consistent manner as the ability to recognize compliance to standards will not only reduce the need for duplicating the verification efforts, but also promote confidence in implementing the standards.

f) Data-Analytics and Intervention Capabilities: the Digital KYC Standards should ensure that technology solutions have the capability to support digital analytics on the transaction data and KYC database, when deemed necessary by the regulatory bodies, to effectuate timely intervention measures.

g) Independence and Neutrality: to prevent any unnecessary conflict of interest, effective Digital KYC Standards should be developed using a technology-neutral approach and should not be built around certain specific technologies, application systems or service providers. The standards should be established by neutral third party and independent of any bank card issuing organization, banks or service providers in accordance with local regulatory requirements. It should be built with an approach that will facilitate flexibility in implementation and healthy competition among banks and technology solutions, leading to further innovation and development.

h) Comprehensiveness, Robustness and Reliability: to successfully achieve the regulatory objectives of financial stability and safety, the Digital KYC Standards should ensure technology robustness and soundness, particularly in terms of information security with the ongoing and escalating cyber threats, and a strong deterrence against financial criminals. The standards should include key measurements for robustness and soundness, as well as reliability so that technology solutions can effectively and comprehensively address the problems.

i) Transparency: the standards formulation process should be transparent to relevant stakeholders, including industry practitioners and service providers in the relevant jurisdictions. They should be actively and regularly engaged during the process to ensure their practical concerns and other observations are discussed and addressed. A high degree of stakeholder involvement is especially important for Fintech and technology standards because of the need to include the expertise of all the underlying technologies.

8. EXPECTED REGULATORY AND COMMERCIAL BENEFITS

There is unlikely that any commercial digital KYC solution would address all the challenges today, neither into the future. With evolving technologies, the appropriate solution today must continue to transform to address the ever-changing regulatory landscapes and ever more sophisticated AML/CFT operations.

The regulator needs a supportive environment where public and private sectors finance players can engage in open discussion. With an established and structured digital KYC platform, this would lead to quicker customer due diligence (CDD), reduce compliance costs and improve financial inclusion. For example, regulator could endorse various Utility technologies, KYC/AML data sharing, and common reporting standard (CRS) across regulated institutions could provide a simple, convenient and secured CDD during the onboarding process.

The commercial benefits as depicted in figure 2 are in many folds with full Digital KYC Lifecycle implementation.

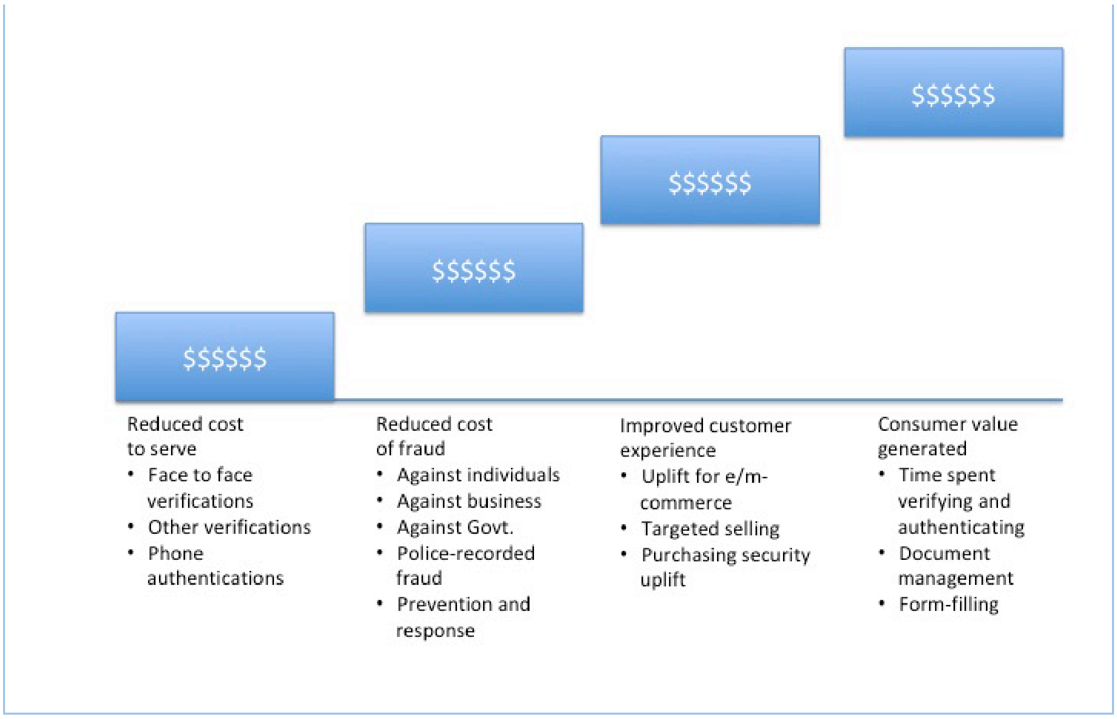

Figure 2: Commercial Benefit of Digital KYC

9. CONCLUSION

While Digital KYC is not completely new, evolving data acquisition technologies combined with machine learning and more powerful data analytics have generated the potential to create commercial and regulatory value for the government, institutions as well as the end-consumers. Tech firm continues to face challenges in pushing the adaption of Digital KYC solutions, but with strong support from government agencies, open dialogues with the eco-system, and industry led regional standardization, the future of digital KYC is promising and would transform the way KYC is conducted.

Submitted by:

POC applicant: Finda

Participating bank: OCBC