KYC models

Ragnar Toomla
TalTech / SEB
Landscape

**Customer**
- Multiple and duplicated information requests and points of contact
- Long onboarding process
- Time consuming renewals

**Financial institution**
- Increasing KYC costs
- Data quality
- Changing regulatory targets
- Risks of KYC failure
- Scrutiny by regulators
- Sub-optimal customer experience

**Regulator**
- Difficult to oversee individual FI approaches and processes
- Complex international standards
- Recent top tier banks’ KYC failures

Source: PWC
Financial crime becoming more sophisticated
De-risking trend

- FI's opting to exit entire categories of customers
- Whole segments of consumers and entire product lines are being abandoned
- Safer to avoid high-risk clients altogether than to manage the associated compliance costs

- May lead banks to outlaw entire lawful industries
- Could force some of these entities and individuals to turn to service providers with limited AML capabilities or to the shadow banking system

In order to help ensure the future health and security of the financial system, it will be imperative for all players to work together
Typical customer on-boarding process

Application → Verification → Collection → Management

Source: Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU, 2018.
Example process in case of shared KYC utility

Customer approaches bank
- Individual
- Corporate

Bank queries the shared KYC platform
- Customer consent to access data

Validation with trusted sources
- Government registries
- Tax authorities
- Credit bureaus

Data is updated in shared KYC platform
- Info from validation process is updated on shared platform

KYC process can be completed

Source: Infocomm Media Development Authority of Singapore (IMDA). 2017
Industry Collaboration

Jurisdictional

Utility Service Providers

Self-Sovereign Digital Identities

Utility Services
- data services and identification (ID) information storage

Managed Services
- outsourced utility services, plus transaction tracking and CDD

Source: Adl and Haworth 2018; Sengupta 2017
The SWIFT KYC Registry
A single source to share & collect your KYC data for Correspondent Banking

- Standardized baseline
  Extensive information including legal entity data, ownership, client and product segments, detailed AML questionnaire, tax/FATCA/CRS information

- Up-to-date information
  Time-stamped data. Any changes are communicated in real-time to correspondents

- Data verification by SWIFT
  All data verified by SWIFT compliance professionals

- Cooperative business model
  Unlimited number of users, volume-based pricing and guaranteed maximum spend

- Secure, user-control access
  User Approved sharing of KYC data

5500 banks registered

60% coverage in terms of SWIFT-connected banks
75% coverage in terms of SWIFT transactions volume
SWIFT KYC registry for corporates

1. Bank X requires access and approaches the Corporate via the KYC Registry.
2. The Corporate receives notification that Bank X requests access to their KYC data.
3. The Corporate approves basic or extended access of Bank X.
4. Access to data is unlocked on the KYC Registry.
5. A notification is sent to users at Bank X that KYC data has been made available by the Corporate.

The permission is valid until pro-actively revoked or surrendered.
D.KYC (Deloitte Know Your Customer)

About

- Launched in 2018
- Provided by Deloitte Luxembourg
- Integrated managed service that combines numerous KYC/AML/CTF services, expertise, and workflow management.

Features

- Counterparty onboarding - Initial risk scoring and due diligence
- Ongoing monitoring and due diligence
- Watchlist and adverse media screening
- Documents verification/qualification
- Oversight & Reporting
- Data hosted in Luxembourg
D.KYC operating model

Clients' counterparties
Natural persons, legal entities
Supplies static data & documents

Clients
Financial & non-financial institutions
Decisions on counterparty acceptance, monitoring and oversight of KYC operations

Deloitte Solutions Sàrl
PSF
Set of predefined KYC/AML/CTF Managed Services

External data
Singapore MyInfo Personal Data Platform

http://www.myinfo.gov.sg

What data items are in MyInfo?

- NRIC
- Name
- Sex
- Date of Birth
- Nationality
- Country of Birth
- Race
- Dialling
- Name of Employer
- Occupation
- Highest Education Level
- Name of School
- Year of Graduation
- Relationship
- ID Type
- ID Number
- Marital Status
- Marriage Date
- Divorce Date
- Yearly Assessable Income
- Year of Assessment
- Monthly Household Income
- CPF Account Balances
- CPF Contribution History (14 Months)
- Mobile Number
- Home Number
- Email Address
- Mailing Address
- Billing Address
- Registered Address
- Type of Housing
- Ownership of Private Residential Property
- Vehicle Number

Source: https://www.slideshare.net/ISS-NUS/myinfo-product-journey-govtech-Singapore
Consent based data sharing

Visit bank’s Web site

Apply with MyInfo option

Login with SingPass & 2FA

Consent to share MyInfo profile

Complete and submit

Now available at: DBS, OCBC, UOB, Maybank, Standard Chartered

Source: https://www.slideshare.net/ISS-NUS/myinfo-product-journey-govtech-Singapore
Streamlining private sector services

Legacy Process
Regulatory Requirement
- Proof of Identity
- Income statements
- Other supporting docs

With MyInfo
Verified Data From Authoritative Source through APIs

Outcomes
Seamless bank account opening
KYC And compliance efficiencies
Convenience for citizens and Productivity and cost savings for businesses

Pilot banks have reported:
- Average usage by 50% of eligible customers.
- Up to 80% reduction in application time for customers.
- Up to 15% increase in approvals from better data quality.

Source: https://www.slideshare.net/ISS-NUS/myinfo-product-journey-govtech-Singapore
MAS working with group of banks in Singapore to build joint KYC utility for countering money laundering and terrorism financing

Methods of detecting and preventing the abuse of the financial system cannot remain static, as criminals are constantly finding new creative ways to perpetrate crimes.

By Pratiksh Bhatia — 27 October, 2017 in Cyber Resilience, Fintech, News, Singapore

Recommended

Technology
Singapore's Bank Intel-Sharing Plan in 'Coma' on Cost Concern

By Chanyaporn Chanaaroen and Andrea Tan

October 12, 2018, 3:44 AM GMT+3

Utility is meant to save costs of opening corporate accounts
Costs of the plan exceeded expectations, MAS's Ravi Menon says

Most Read

How Much Money Do You Need to Be Wealthy in America?

Stocks Rebound as Trade Comments Ease Concerns: Markets Wrap

Trump Tower is Now One of NYC's Least-Desirable Luxury Buildings

MARKETS

Stocks, Commodities Tumble as China Strikes Back: Markets Wrap

Oil Gives Back Gains as API Sees Big Jump in U.S. Crude Supply
Design desicions

1. **Mutualisation** - one single KYC record
2. **Centralisation not decentralisation**
3. **Exclusion** of private individuals and private banking
4. **Harmonised policy and operating model**
5. **Customer interaction by bank not Utility**
6. **Ownership model** - separate company, with independent management. Banks will not have any ownership.
7. **Adoption strategy**
   - ensuring ecosystem connectivity with other data sources
   - ensuring the ability to ingest and output many different types of data formats
   - exploring ways to increase adoption rate of the Utility, e.g. regulators mandating the use of the Utility
Evolution of digital identities

- **Centralized Identity**: Identity is centrally assigned by authority. Example: Assigning IP addresses in early 90s by IANA.
- **Federated Identity**: Usage of multiple services with a single account. Example: Microsoft Passport.
- **User-centric Identity**: Focusing on the control of personal data by the user. Example: OpenID, OAuth, Facebook Connect.
- **Self-sovereign Identities**: Every person creates and manages their own digital identities. Example: ID2020.

Source: Allen 2016
1.1bn people are unable to prove their identity.

WORLD BANK, ID4D Dataset
Ten Principles of Self-Sovereign Identity

1. **Existence.** Users must have an independent existence.
2. **Control.** Users must control their identities.
3. **Access.** Users must have access to their own data.
4. **Transparency.** Systems and algorithms must be transparent.
5. ** Persistence.** Identities must be long-lived.
6. **Portability.** Information and services about identity must be transportable.
7. **Interoperability.** Identities should be as widely usable as possible.
8. **Consent.** Users must agree to the use of their identity.
9. **Minimalization.** Disclosure of claims must be minimized.
10. **Protection.** The rights of users must be protected.

Source: Allen 2016
Self-Sovereign Identity model

Source: Ankur Patel, Principal Program Manager, Identity, Microsoft 2019
Opportunities

- person ultimately has full control
- increases the freedom of the individual
- trustworthiness no longer directly tied to local governments
- protection of privacy as an important design objective (GDPR)
- selective sharing of personal data with service providers follows the idea of data economy and privacy by default/design
- transparency created by self-governance could also strengthen the European digital single market by removing barriers of missing trust

Challenges

- challenge to offer solutions that help persons to manage the additional administrative efforts sufficiently comfortable
- protection of the privacy of persons
- difficulty of prohibiting profiling by third parties
- data formats and standardized interfaces for securely exchanging evidences and digital identities
- distributed ledger technologies have limitations in terms of speed and volume
Conclusion

• Less corruption, tax evasion, money laundering, and other criminal activities
• More consistent information
• Better information management
• Reduced risks
• Cheaper and easier to create new relationships