FATF Guidance on Digital ID

Fredesvinda Montes, May, 2020

WORLD BANK GROUP

FATF RECOMMENDATIONS FOR IDENTIFICATION OF CLIENTS AS PART OF THE CDD

R 10 FATF

- Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names
- Fis should conduct CDD under the following circumstances
  - (i) Onboarding of new clients;
  - (ii) Occasional transactions above 15,000 USD-Euros; or (ii) Electronic Transfers based on R16;
  - (iii) Suspicious illegal activity of ML or TF; or
  - (iv) When the FI has doubts about the veracity and reliability of the clients' data

R 10 FATF

- Identify the client and the ultimate beneficiary **using data, documents and reliable information from independent sources.**
- Ultimate Beneficiary and Client
- CDD must be done with an risk based approach (RBA)
- (R10 a and R10 d)
- R17 on third party reliance
- R11 on record keeping apply also

DIGITAL ID GUIDANCE (2019)

- Framework for adequacy of Digital ID Systems to R10
- Financial Inclusion
- Final document approved by FATF in Feb 2020.
- FATF Statement in response to COVID-19
- FATF non-paper in April 2020
- Country Examples

WORLD BANK GROUP

FATF DIGITAL ID GUIDANCE , February 2020

Key Terms

- The Guidance is limited to customers that individuals not to legal entities or beneficial owners.
- **Official Identity** for access financial services. Specification of a unique natural person that is based on (i) attributes of the person and (ii) is recognized by the state for regulatory and other official purposes.
- **Proof of official Identity** depends on some form of gov provided or issued registration, certification or documentation that constitutes evidence of core attributes.
- **Digital ID systems** use electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels (identity **proofing**, **enrolmen**t and **authentication** are essential steps and a third one when feasible is desirable **interoperability**.

Benefits

- Facilitate customer onboarding
- Support on-going due diligence
- Facilitate other CDD measures
- Reduce costs and enhance efficiency
- Foster financial inclusion and reduce informality by enabling remote onboarding of clients

Risks

- Cybersecurity
- Privacy
- ID Theft
- Exclusion risks
- Connectivity

RBA

- Digital ID systems should rely upon technology, processes, governance and other safeguards, that provide an appropriate level of trustworthiness.
- Framework based on questions
  - (i) Digital ID authorized by government to be used for CDD?
  - (ii) Do you know the LoAs of the system?
  - (iii) Is the Digital ID appropriate for ML/FT risk situation?
- 1- Flexible approach in establishing the required identity attributes, evidence and processes for proving official identity
- 2- Include risk mitigation measures – Tiered approach to CDD
- 3- Low ML/TF risks – lower levels of assurance for identity proofing are appropriate

FATF DIGITAL ID GUIDANCE , February 2020

Authorities

1. Develop clear guidelines allowing the risk-based use of reliable and independent Digital ID systems by entities regulated for AML/CFT purposes.
2. Assess existing regulations so that non-face to face onboarding may be standard or low risk when a Digital ID with appropriate levels of assurance are used for remote identification/verification.
3. Adopt principles, performance, and/or outcomes-based criteria
4. Develop an integrated multi-stakeholder approach to understanding and mitigating risks.

Regulated Entities

1. Take informed RBA to relying on Digital ID systems for CDD that includes;
   - •Understanding LoAs for identity proofing and authentication
   - •Ensuring that the LoAs are adequate to the jurisdiction, product, customer etc.
2. Consider if ID systems with lower LoA may be appropriate for SCDD in cases of low ML/TF risk.
3. Review policies if non-face to face onboarding or transactions are always considered high risk even when relying on Digital ID.
4. Adopt anti-fraud and cybersecurity measures
5. Enable a process for authorities to obtain, the underlying identity information needed for identification and verification of individuals.

ID Providers

1. Understand the AML/CFT requirements for CDD
2. Seek assurance testing and certification by the government or an approved expert body
3. Provide transparent information to AML/CFT regulated entities and foster federation and interoperability

FATF GUIDANCE ON DIGITAL ID- ID PROOFING/VERIFICATION

Requirement	AL 1	AL2	AL3
Presence	No requirement	In person	In person-Supervised remote
Resolution	No requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence	Same as AL2
Evidence	No evidence is collected	• One piece of SUPERIOR or STRONG evidence on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence, OR • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, OR • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as AL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements	Required	Required. Notification of proofing to postal address
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	Moderate Baseline	High baseline

FATF GUIDANCE NOTE ON DIGITAL ID: AUTHENTICATION

Reduce Risk of Fraud

Assurance that the at the individual asserting identity for account authorization controls an authenticator(s) bound to the subscriber's account

AAL 1

Provides some assurance

- Credential stuffing, phishing, PIN code capture and replay, forged logging attacks
- MFA is optional
- Biometrics alone maybe used as single-factor authenticator

AAL2

Provides high confidence

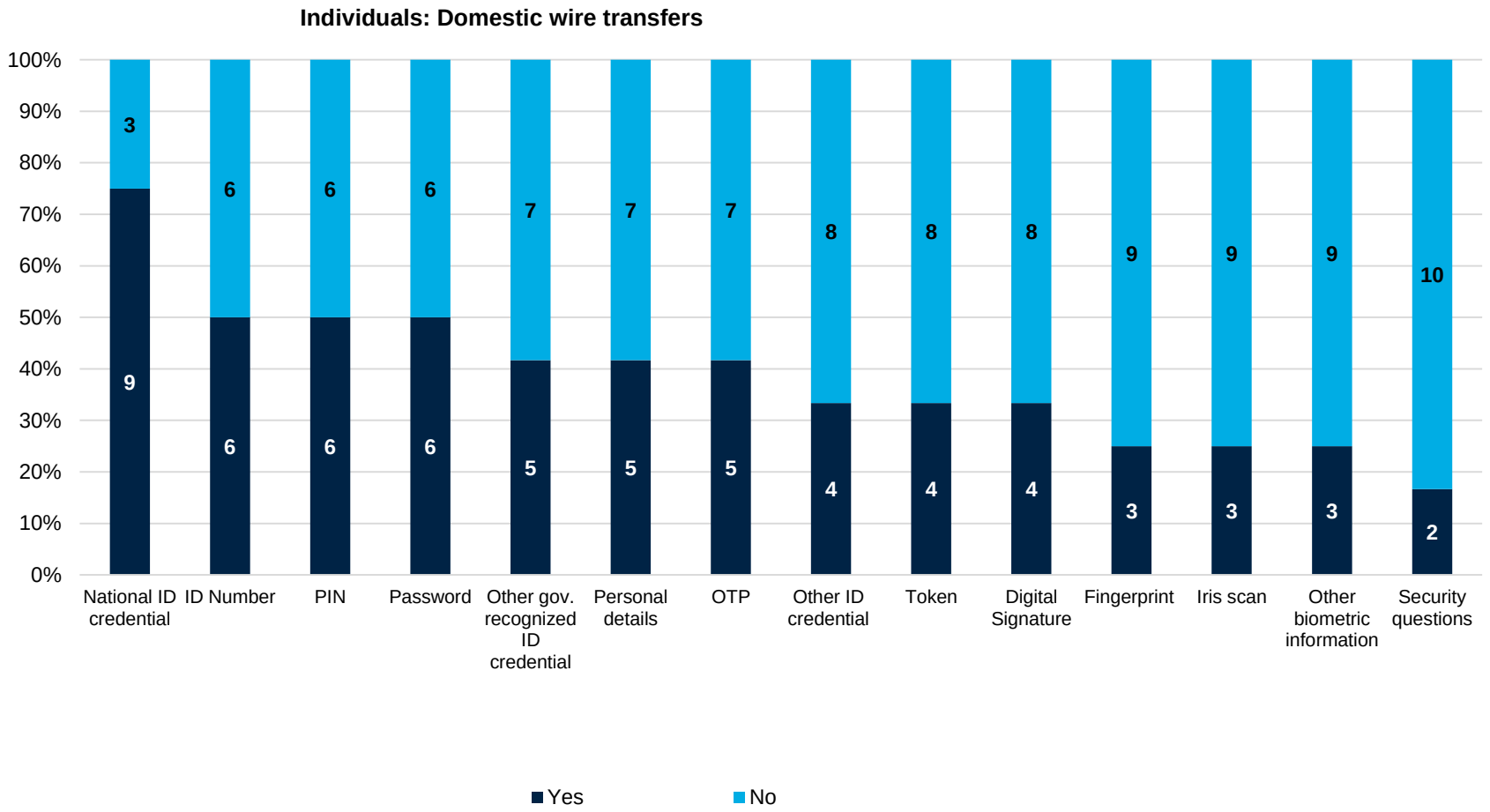
- MFA is mandatory
- Lack of biometrics, or specific groups that facial recognition might encounter failures
- Information security controls at moderate baseline
- Biometrics + device

AAL3

Provides very high confidence

- MFA (hardware and VIR)
- SCA under RTS of the PSD2 (Strong Customer Authentication)

Survey Responses: Authentication Methods



KEY ASPECTS OF THE FATF STATEMENT, April 2020

Risk based approach as a flexible framework to address emerging needs

Identify Increased risks to ML (fraud, cybersecurity)

Measures

- SCDD for contingency accounts (Gov payments, facilitate access to digital/contactless payments)
- Legitimate reasons for usual process of KYC for on going due diligence might not be appropriate
- Acceptance of lower levels of assurance of IDs
- Delayed verification of ID for account onboarding, accept digital copies of documentation and scanned documents
- Use Digital ID solutions for customer on boarding when feasible.

CONSIDERATIONS FOR COUNTRY IMPLEMENTATION

SCENARIO	IDENTIFICATION/ VERIFICATION	AUTHENTICATION
G2P	Apply Tiered approach to SCDD (Proof of ID + Proof of address could be waived) Selfies and Videoconference + ID scan	MFA but maybe no need for biometrics if not available
Internet Banking	Alternative ways and information could be used if available Verification of information through third parties (e.g. telecommunication operators)	Biometrics alone MFA but selection of factors avoid contact
Occasional Transactions	Walk in or remittances (exemptions to verification based on thresholds)	
E-wallets	Delayed verification of ID	Biometrics through cell phone credentials

MEXICO TIERED APPROACH TO SCDD

	Level 1	Level 2	Level 3
Data from the consumer	▪ No data required	▪ Name, ▪ Date of Birth ▪ Address ▪ Sex ▪ Place of birth for remote onboarding.	▪ Same as Level 2 + ▪ Nationality ▪ Occupation ▪ Telephone Number
Interview	No need	Face to face or remote (requires verification of National ID	Face to face
Type of Consumer	Individuals	Individuals	Individuals /Legal Entities
Límits[1]	▪ Maximum balance of 1,000 Udi ($5,883 MXN) ▪ Maximun month deposit 750 Udi ($4,412 MXN)	▪ Maximun month deposit de 3,000 Udi (17,650 MXN) ▪ Maximun month deposit for beneficiaries of Social programs 6,000 Udi (35,300 USD).	▪ Maximun month deposit 10,000 Udi (58,833 MXN).

COVID 19- RESPONSES FROM AUTHORITIES

Egypt

Enroll customers to internet banking services

Limits raised on pre-paid cards

→

Information available on client's profile

No signature required

No password required

→

Telephone Number +NID are sent to Telecommunication Authority for verification

India https://www.finextra.com/pressarticle/81941/npci-urges-india-to-use-digital-payments-to-reduce-social-contact-and-contain-covid-19-outbreak

Foster non-cash digital payments

→

Fast track on-boarding of UPI and UPI QR

→

UPI ID

Ghana https://www.bog.gov.gh/wp-content/uploads/2020/03/MPC-Press-Release-March-2020-3.pdf

Enrolment of Basic Accounts

Increased limits

(3 month period)

→

Use existing mobile phone registration data

→

RESPONSES FROM COUNTRIES (APRIL 2020)

EBA

Delayed implementation of SCA	E-commerce card transactions • 50 Euros or total of 150 • 5 transactions	

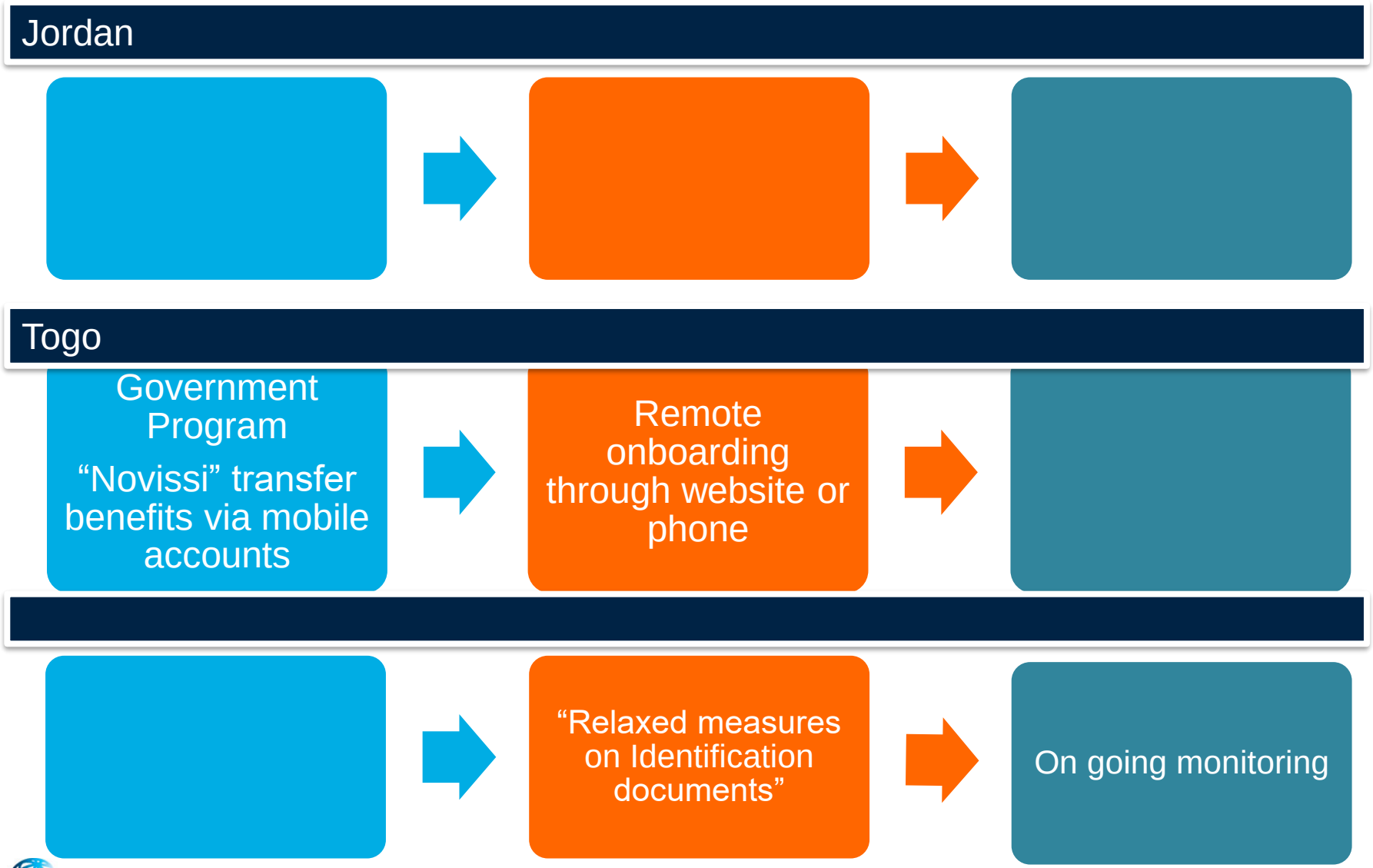
Pakistan http://www.sbp.org.pk/psd/2020/C2.htm

Foster Digital Payments (internet and mobile financial services)	Biometric verification to activate internet and mobile accounts is suspended	(i) Measures for customer authentication and verification (ii) Security and safety measures

Philippines http://www.bsp.gov.ph/publications/media.asp?id=5342

	"Relaxed measures on Identification documents"	On going monitoring

RESPONSES FROM COUNTRIES (APRIL 2020)



FIGI TOOLKIT FOR ID IN THE FINANCIAL SECTOR

Legal & regulatory

Oversight

Private Sector Role

New Technologies

Integrated Framework

Questionnaire

FATF DIGITYAL ID GUIDANCE

Pilot the Toolkit

Present Results June 2020

RELEVANT MATERIALS ON DIGITAL ID

- https://www.gpfi.org/publications/g20-digital-identity-onboarding

- FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence*, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html
- World Bank (2018), Private sector economic impacts from identification systems, http://documents.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf

- https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html
- Forthcoming FIGI toolkit on Digital ID (The World Bank)

RELEVANT MATERIALS ON DIGITAL ID

- https://www.gpfi.org/publications/g20-digital-identity-onboarding

- FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence*, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html
- World Bank (2018), Private sector economic impacts from identification systems, http://documents.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf

- http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
- Forthcoming FIGI toolkit on Digital ID (The World Bank)
- https://id4d.worldbank.org/

Fredes Montes
Senior Financial Sector Specialist
fmontes@worldbank.org
+1 202907644