ITUEvents

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium

22–24 January 2019
Cairo, Egypt

#financialinclusion

Hosted by

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and
Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Authentication Work stream FIGI Security Infrastructure and Trust Working Group

Abbie Barbir, Chair

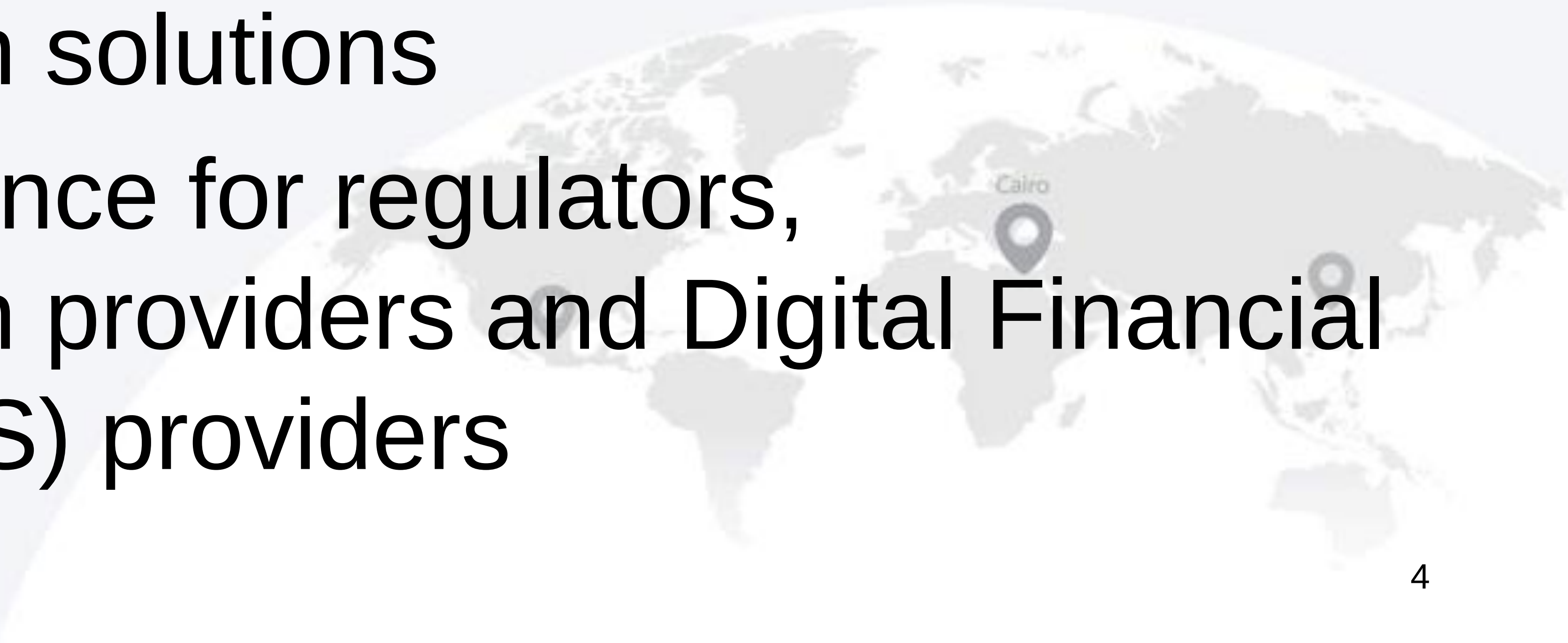
Security, Infrastructure, Trust Working Group

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

- To enhance confidence in using Digital Financial Services (DFS)
- To address DFS security issues and mass digital fraud in developing countries
- To assess new technology impact on security & consumer protection

Authentication Workstream

- To provide use cases, requirements, definitions and examples of strong authentication solutions
- To offer guidance for regulators, authentication providers and Digital Financial Services (DFS) providers



Scope and Focus

- Strong interoperable authentication to support DFS
- Use cases (web/Mobile)
  - National solutions (e.g Aadhaar in India. AliPay)
- Means of evaluating authentication assurance (ITU-T X.1254)
- Digital Lab setup
  - APIs for interoperable authentication Supporting FIDO Standards (ITU-T X.1277 / ITU-T X.1278) including API for:
    - End point validation, subscription and registration
    - Device Registration enabling service provider to register an Authenticator with user account and policy.
    - Device authentication.
    - Transaction Confirmation: Support for user to confirm a specific transaction is provided.
    - Deregistration: Relying party can trigger the deletion of the account-related authentication key material

Trouble With Passwords

Most people use less than 5 passwords for all accounts

50%

of those haven't changed their password in the last 5 years

Reuse makes them easy to compromise

39%

of adults use the same password for many of their online accounts

They are very difficult to remember

25%

of adults admit to using less secure passwords, because they are easier to remember

There are lots of places to steal them from

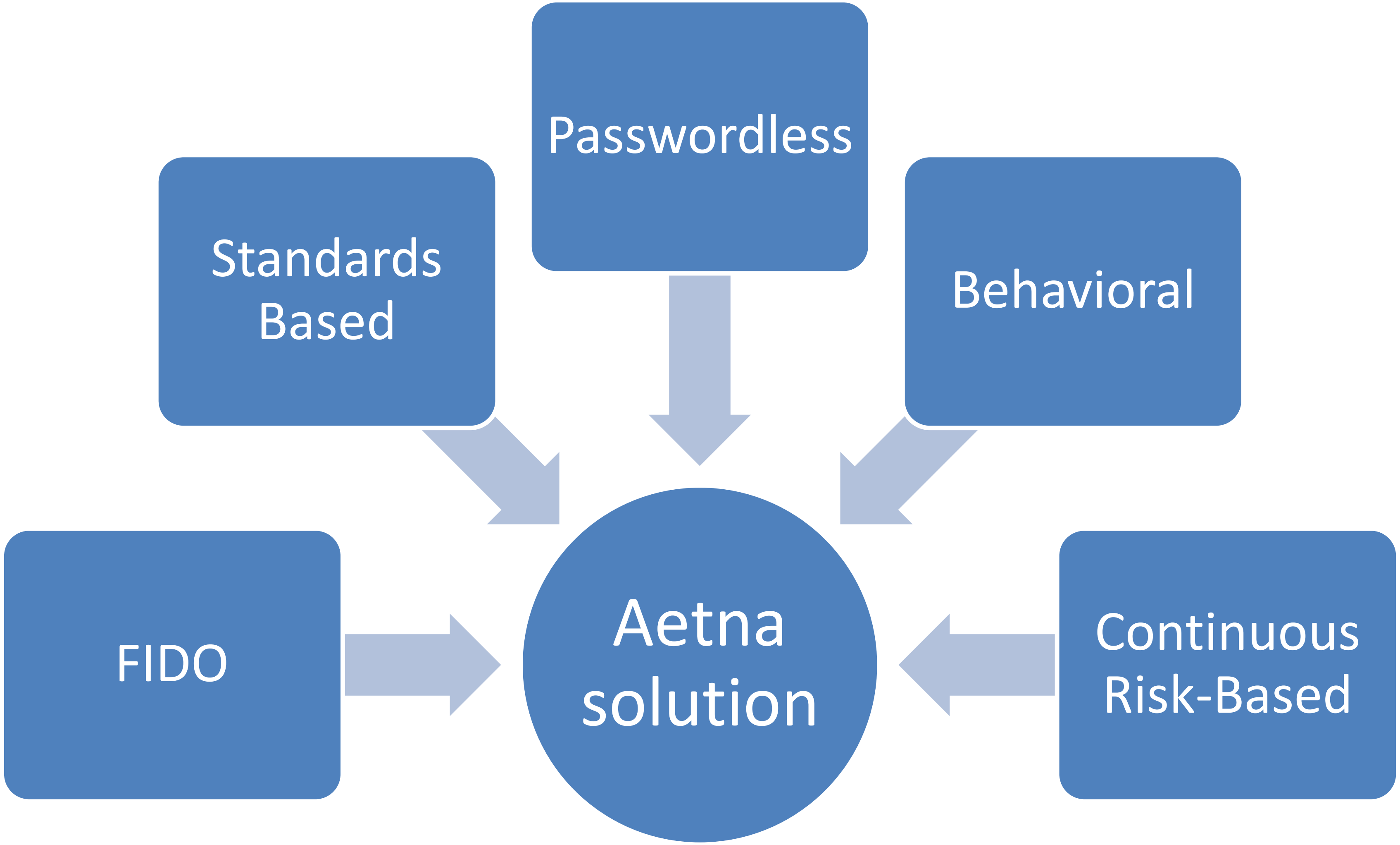
49%

of adults write their passwords down on paper

Over 3 billion user IDs and passwords were stolen in 2016

Sources: Pew research; Telesign research

Aetna Next Generation Authentication



Passwordless

Standards Based

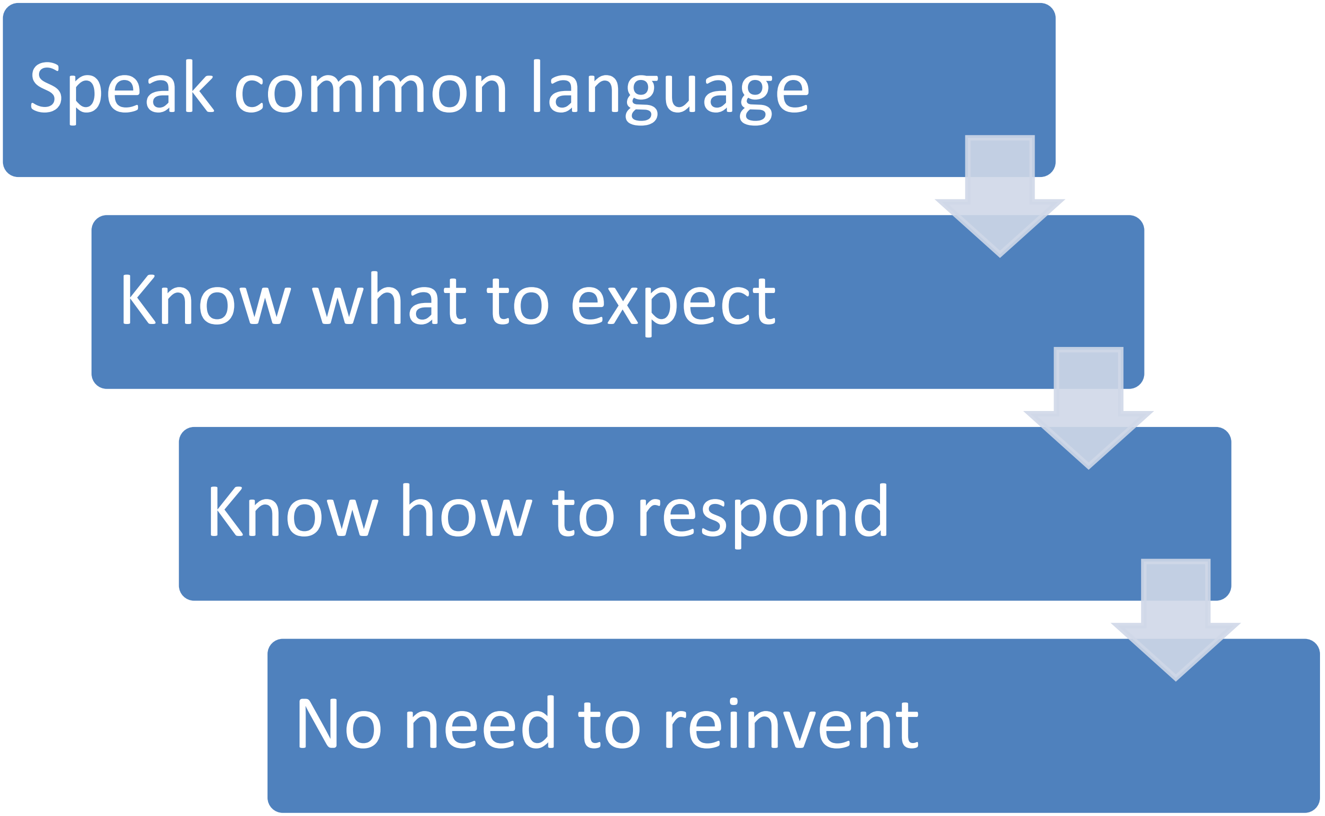
Behavioral

FIDO

Aetna solution

Continuous Risk-Based

Standards = Interoperability


Speak common language

Know what to expect

Know how to respond

No need to reinvent

- ITU X.1252 (Revision)
- ITU X.1254 (Revision)
- ITU X.509
- ITU-T X.1276
- ITU-T X.1277, ITU-T X.1278
- ISO 29115 (Revision)
- ISE FICAM
- NIST 800-63-3
- FIDO 2.0 WebAuthN (w3C)
- Oauth 2.0
- OIDC

ITUEvents

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium

22–24 January 2019
Cairo, Egypt

#financialinclusion

Hosted by

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Discussion Paper: Secure Authentication Use Cases for DFS and Guidelines for Regulators and DFS Providers

Andrew Hughes, Editor

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

The Discussion Paper

The Sources

- Contributions from working group members over the last 12 months
- Additional contributions from industry consortia and standards development bodies

The Contents

- Describes standards and regulations for strong authentication
- Implementation examples for use cases
- Guidance for regulators, authentication providers and DFS providers
- Standardization objectives

‘Authentication’

Authentication Systems

- Used in two ways:
  - Establish that the person is who they claim to be when enrolling for an account
  - Verify that a returning customer is the same one that previously opened an account

For Account Creation

- Ask for and verify identification information
  - – For DFS – ‘Know Your Customer’ (KYC) procedures
  - – “e-KYC” examples are given in this report
  - – Obtain from previously-established accounts based on regulatory obligations

For Returning Customers

- For returning customers, ask for evidence that they are the same person as seen before
    - Ask for a secret only known to them
    - Have them demonstrate possession and control of a credential or device previously issued
    - Compare a biometric sample to one ‘on file’

Multi-factor Authentication Approach

- Combine multiple authentication factors to strengthen overall authentication mechanism
  - – Knowledge-based factor
  - – Possession-based factor
  - – Factor based on physical or inherent characteristic

Advanced Authentication Techniques

- Convenient and easy to use
- Eliminate or reduce reliance on passwords
- Examine real-time behaviour to detect anomalies
- Dynamic risk scoring of authentication confidence
- Background authentication throughout transaction
- Broadly similar to anti-fraud techniques

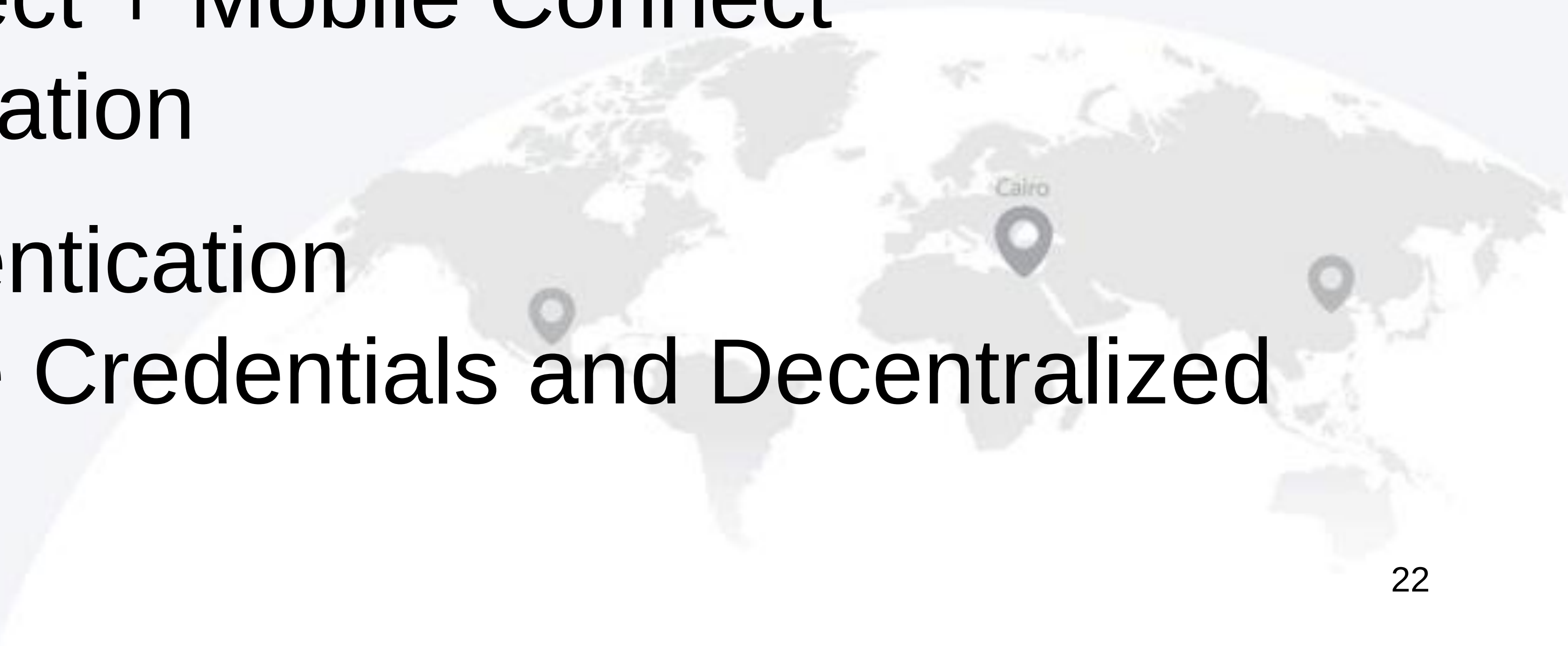
The Standards and Specifications

Standards and Regulations

- These contain ‘levels’ and requirements
- ITU-T Recommendation x.1254
- NIST SP 800-63-3
- eIDAS Regulation
- Payment Services Directive 2

Technical Specifications

- FIDO Alliance specifications
  - ITU-T Recommendations x.1277, x.1278
- OpenID Connect + Mobile Connect
- IFAA Authentication
- Aadhaar Authentication
- W3C Verifiable Credentials and Decentralized Identifiers



The Use Case Examples

The Use Cases

- Use cases
  - Enrolment and account opening
  - Authentication to access a DFS

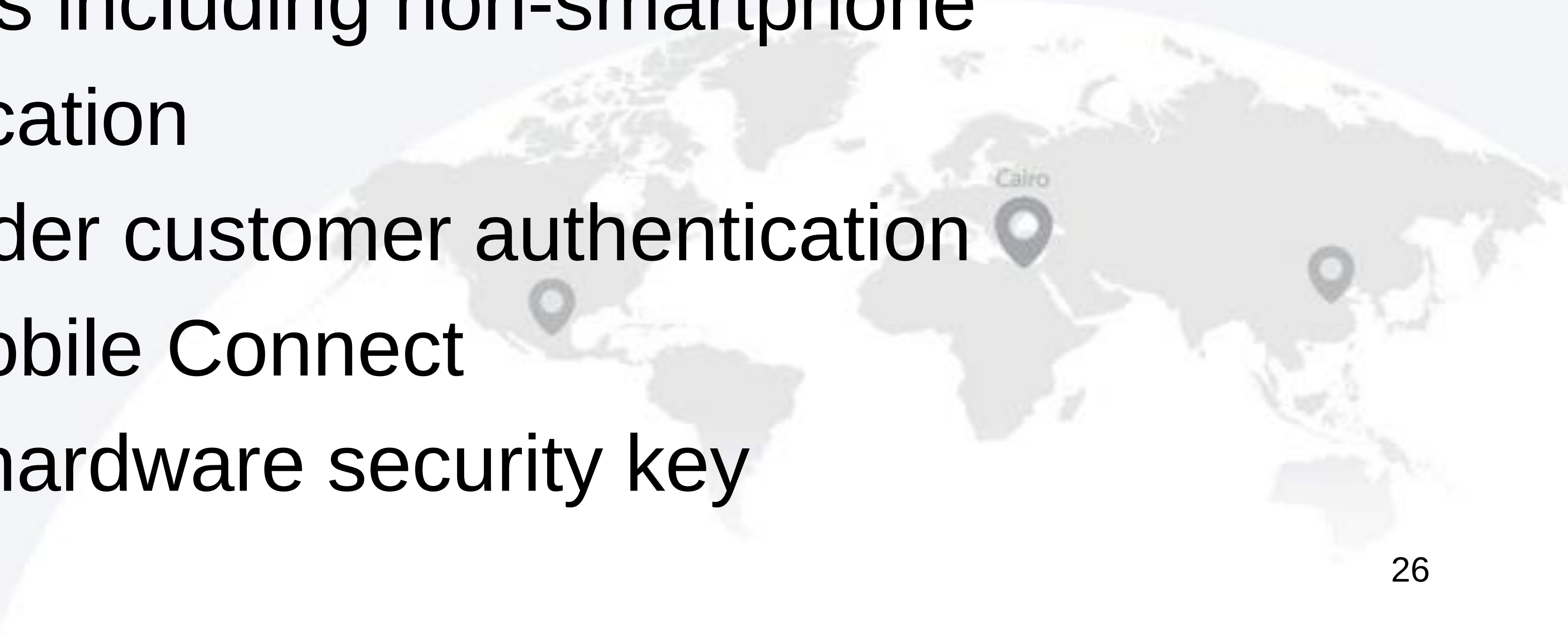
Account Opening

- Aadhaar eKYC – from national ID
- K-FIDO Enrolment – from national ID
- City of Zug eID – from citizen register
- FIDO account enrolment
- Healthcare provider – member enrolment

Access A Service

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

- IFAA – mobile payment – fingerprint or face
- Aadhaar Authentication & Universal Payments Interface – several modalities including non-smartphone
- K-FIDO Authentication
- Healthcare Provider customer authentication
- SK Telecom – Mobile Connect
- FIDO Alliance – hardware security key

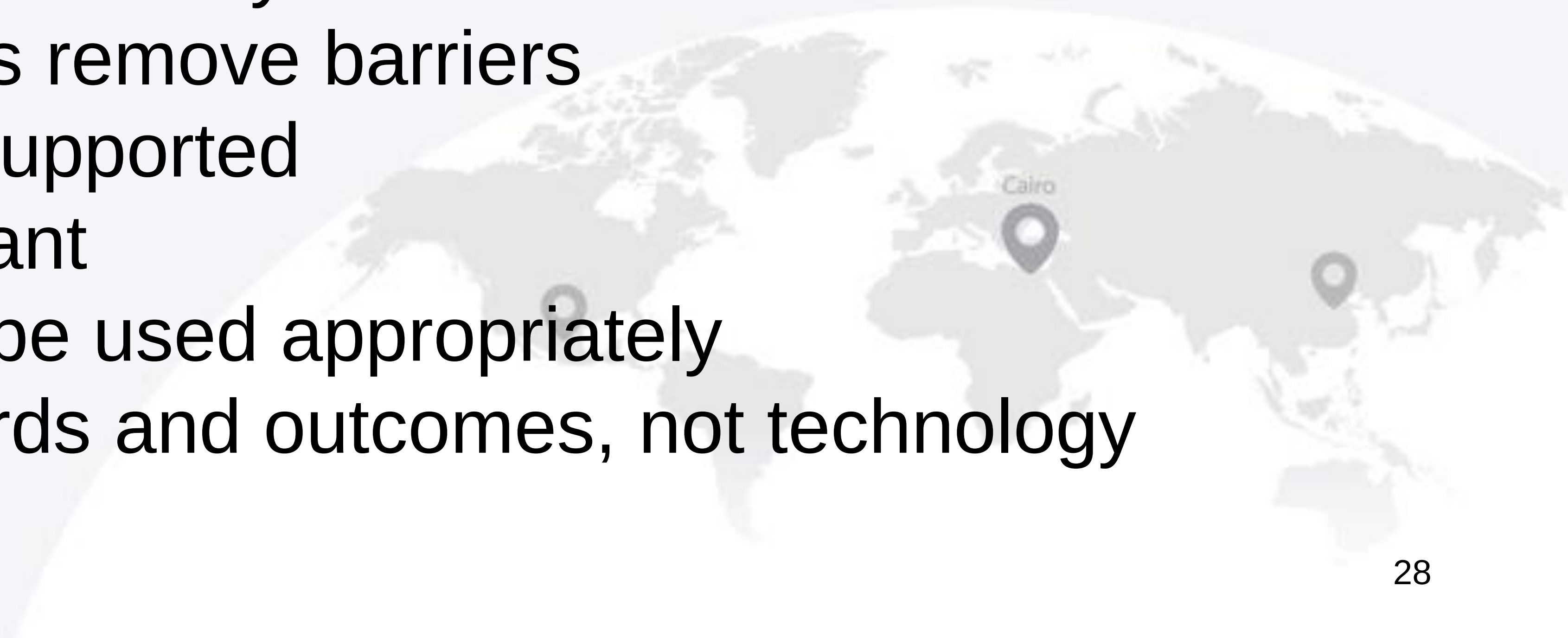


The Guidance

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Guidance for Regulators

- Require strong authentication
- Recognize limitations of shared secrets
- Make authentication easy to use
- New technologies remove barriers
- Mobile must be supported
- Privacy is important
- Biometrics must be used appropriately
- Focus on standards and outcomes, not technology



Biometric Authentication

- Design considerations
  - Accuracy, universality, stability/permanence, collectability, resistance to circumvention, acceptability, usability, cost

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Standardization

- More work is needed for
  - Behavioral biometrics
  - Relative strengths of authentication
  - Mobile security capabilities and authenticator strengths
  - User experience

Closing Remarks

- Keep watching this space for innovation – the rate of invention is very high & technologies and approaches are maturing
- Please review and provide feedback
- Don’t be the next weak link in the chain!

To Provide Feedback

- Download the report

  https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Secure%20Authentication%20Use%20Cases.pdf

- tsbfigisit@itu.int

ITUEvents

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium

22–24 January 2019
Cairo, Egypt

#financialinclusion

Hosted by

NTRA National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU