FIGI Security Clinic

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Implementation of Secure Authentication Technologies for DFS

Abbie Barbir
Chair – Authentication WS

4-5 December 2019
#financialinclusion

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

Technical Report: Implementation of Secure Authentication Technologies for DFS

Andrew Hughes, Editor

The Report

- Contributions from working group members for over the last 22 months
- Additional contributions from industry consortia and standards development bodies
- Download the report

The Contents

- Requirements for strong authentication in regulation
- Strong authentication specifications and technologies
- Emerging technologies and approaches
- Implementation examples for use cases

‘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 a DFS 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 behavior 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 800-63-3-3
- 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

Emerging Approaches

- W3C Verifiable Credentials and Decentralized Identifiers
  - Shift towards personal ‘wallet’ for secure storage of cryptographic keys and secrets
- Cognitive Continuous Authentication
  - Dynamic evaluation of authentication and sessions to detect abnormal activities

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

- Acceptto-FIDO mobile payment
- 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

Closing Remarks

- Keep watching this space for innovation – the rate of invention is very high & technologies and approaches are maturing