International Telecommunication Union

FINANCIAL INCLUSION GLOBAL INITIATIVE (FIGI)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(12/2018)

Security, Infrastructure and Trust Working Group

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

Report of the Authentication Workstream

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

A new global program to advance research in digital finance and accelerate digital financial inclusion in developing countries, the Financial Inclusion Global Initiative (FIGI), was launched by the World Bank Group, the International Telecommunication Union (ITU) and the Committee on Payments and Market Infrastructures (CPMI), with support from the Bill & Melinda Gates Foundation.

The Security, Infrastructure and Trust Working Group is one of the three working groups which has been established under FIGI and is led by the ITU. The other two working groups are the Digital Identity and Electronic Payments Acceptance Working Groups and are led by the World Bank Group.

Secure Authentication Use Cases for DFS and Guidelines for Regulators and DFS Providers

Authentication Workstream

About this Report

This report was written by the following authors, contributors and reviewers:

Andrew Hughes, Abbie Barbir, Arnold Kibuuka, Vijay Mauree, Harm Arendshorst, Tiakala Lynda Yaden, Mr. Mayank, Vinod Kotwal, Jeremy Grant, Brett McDowell, Adam Power, Sylvan Tran, Ramesh Kesanupalli, Chunpei Feng, Hongwei (Kevin) Luo, David Pollington.

Section 5 of this report includes content adapted from an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfigisit@itu.int

Table of contents

List of Figures

List of Tables

Executive Summary

This Discussion Paper is the result of contributions and deliberations of the Financial Inclusion Global Initiative Security, Infrastructure and Trust Working Group Authentication work stream.

The Digital Financial Services (DFS) ecosystem requires standardized, interoperable, strong authentication technologies as enablers to reduce risk and protect assets. Weak authentication approaches based on web browsers and passwords are no longer sufficient to support safe DFS use. This report describes technologies and standards that can be used to implement strong authentication systems for DFS and provides examples of implemented strong authentication systems.

Previously, the ITU Focus Group on Digital Financial Services, a multiparty consultative body for fostering the development of safe DFS ecosystems, produced recommendations on security, identification and authentication for DFS. This report addresses several of the Focus Group recommendations, including:

- The use of mobile devices that allow for the use of strong authentication mechanisms to demonstrate ownership of the device is recommended.
- At time of registration, A DFS operator should create a digital identity for its customers, for use in both DFS transactions and (where relevant) in identity assertion with external service providers.
- DFS Operators should ensure an intuitive and straightforward customer experience for registration and subsequent authentication.
- Policy makers and regulators should be encouraged to use national identity systems, or other market-wide identity systems, to help with opening transaction accounts, addressing payments, and, in some instances, improving transaction security.
- App developers should ensure that DFS applications are designed and implemented in accordance with industry and Standards Setting Bodies (SSB) best practices for secure software development, including encrypted and authenticated communication and secure coding practices.
- Where a customer is unable to provide a foundational document of digital identity, a dynamic, self-asserted digital identity should be issued.
- Regulators should standardize digital identity registration, and ensure interoperability between DFS operators and service providers relying on the digital identity.

A primary goal of authentication systems is to increase confidence that a previously-enrolled user is actually that user. Access control and authorization policy can then be applied to that authenticated user.

Design decisions and technology choices for each authentication system element affect how ‘strong’ an authentication system is: how resistant to attack and compromise due to common threats. ‘Strong’ authentication systems are designed to mitigate weaknesses that ‘weak’ authentication systems do not.

Typical authentication systems in use today were designed for the pre-mobile-device internet. They are based on a single authentication event, typically performed at application start up, and assume that the user, device and session do not change after that single authentication event. These elements have proven to introduce weaknesses into authentication systems.

In addition to ‘strong’ authentication system elements, advanced authentication systems are designed to address today’s threat models and design patterns. Compared to ‘strong’ authentication systems, there is an increased emphasis on detection and authentication of human users versus the client software used by people through environmental and behavioral analysis. New approaches are being implemented to minimize friction for mobile and multi-factor use cases: many systems are now built with ‘mobile first’ designs. Authentication now happens at many points during a user-system interaction: at identification time, at times when increased privileges are invoked (so-called ‘step-up’ authentication), and even continuously during the entire session.

This report describes several widely-adopted technical and policy standards that support strong authentication mechanisms.

The examples of strong authentication and advanced authentication systems are categorized as either enrolment of authentication for use of DFS. These two use case categories primarily impact users of DFS.

The examples presented for the Enrolment use case describe how previously-established identity information can be used to create new service accounts and to satisfy KYC requirements. The key aspect in the examples is that the person has been enrolled previously with an authority: their identity information collected, verified and stored. This stored identity information is then available for later presentation to service providers, controlled by the person’s authentication to release that identity information.

The examples for the Entity authentication use case describe how next generation authentication mechanisms are used to authenticate an individual for authorization to consume services.

The remainder of the report offers guidance to regulators and solution providers for policy development, system design and implementation.

The guidance for regulators includes:

1. Require strong forms of authentication.
2. Recognize the security limitations of shared secrets.
3. To gain widespread adoption, authentication must be easy to use.
4. Understand that the old barriers to strong authentication no longer apply.
5. Authentication solutions must support mobile.
6. Privacy matters.
7. Biometrics are making authentication easier – but must be applied appropriately.
8. Don’t prescribe any single technology or solution – focus on standards and outcomes.

The report describes several examples of strong and advanced authentication systems for access to financial services. Further standardization work is needed to ensure that technologies are made to be fit for purpose and that different approaches can be evaluated for relative strengths and capabilities.

In conclusion, it is clear that there exist effective solutions addressing today’s enhanced threats to DFS. Through careful planning, strong direction and sustained effort, access to DFS can be safe, low-barrier and effective.

1 Acronyms

AAGUID	Authenticator Attestation GUID
ASPSP	Account Servicing Payment Service Providers
AUA	Authentication User Agency
CIDR	Central Identities Data Repository
CTAP	Client to Authenticator Protocol
DFS	Digital Financial Services
eKYC	Electronic Know-Your-Customer
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standards
FRR	False Rejection Rate
FTE	Failure to Enroll
GUID	Globally Unique Identifier
ID GW	Identity Gateway
IdP	Identity Provider
IFAA	Internet Finance Authentication Alliance
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ITU FG DFS	ITU Focus Group on Digital Financial Services
KUA	KYC User Agency
MSISDN	Mobile Station International Subscriber Directory Number
NPCI	National Payments Corporation of India
OIDC	OpenID Connect
OOB	Out of Band
OTP	One Time Password
PSD2	Payment Services Directive 2
RP	Relying Party
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SSB	Standards Setting Bodies
TPP	Third Party (Payment Service) Providers
U2F	Universal Second Factor
UAF	Universal Authentication Framework
UIDAI	Unique Identification Authority of India
UPI	Universal Payments Interface

VPA	Virtual Payment Address

2 Introduction

The Digital Financial Services (DFS) ecosystem requires standardized, interoperable, strong authentication technologies as enablers to reduce risk and protect assets. Weak authentication approaches based on web browsers and passwords are no longer sufficient to support safe DFS use. This report describes technologies and standards that can be used to implement strong authentication systems for DFS and provides examples of implemented strong authentication systems.

2.1 Overview of ITU FG DFS

The Financial Inclusion Global Initiative was formed as a follow-on activity of the ITU Focus Group on Digital Financial Services (hereinafter, "ITU FG DFS" or "Focus Group") which was established as a multiparty consultative body for fostering the development of safe, enabling DFS ecosystems. The overall objectives of the Focus Group were to: (i) increase and formalize the collaboration between financial and telecommunications authorities with respect to DFS; (ii) identify key issues limiting the development of safe, enabling DFS ecosystems; (iii) analyse how these issues have been addressed in practice and exchange information on best practices; and (iv) develop policy recommendations for authorities and other stakeholders on how to approach these issues in their countries. The Focus Group brought together financial and telecommunications authorities, private-sector stakeholders, consumer advocates, DFS technical experts, development partners, and other key DFS stakeholders to collaboratively explore these issues and develop consensus recommendations. [1]

This report addresses several of the Focus Group recommendations, including [1]:

- The use of mobile devices that allow for the use of strong authentication mechanisms to demonstrate ownership of the device is recommended.
- At time of registration, A DFS operator should create a digital identity for its customers, for use in both DFS transactions and (where relevant) in identity assertion with external service providers.
- DFS Operators should ensure an intuitive and straightforward customer experience for registration and subsequent authentication.
- Policy makers and regulators are encouraged to use national identity systems, or other market-wide identity systems, to help with opening transaction accounts, addressing payments, and, in some instances, improving transaction security.
- App developers should ensure that DFS applications are designed and implemented in accordance with industry and Standards Setting Bodies (SSB) best practices for secure software development, including encrypted and authenticated communication and secure coding practices.
- Where a customer is unable to provide a foundational document of digital identity, issue a dynamic, self-asserted digital identity.
- Regulators should standardize digital identity registration, and ensure interoperability between DFS operators and service providers relying on the digital identity.

This report describes strong authentication technologies, standards, and techniques to aid in DFS account opening and customer ease-of-use.

2.2 Overview of the DFS Ecosystem

The Digital Financial Services ecosystem consists of users (consumers, businesses, government agencies and non-profit groups) who have needs for digital and interoperable financial products and services; the providers (banks, other licensed financial institutions, and non-banks) who supply those products and services through digital means; the financial, technical, and other infrastructures that make them possible; and the governmental policies, laws and regulations which enable them to be delivered in an accessible, affordable, and safe manner. [2]

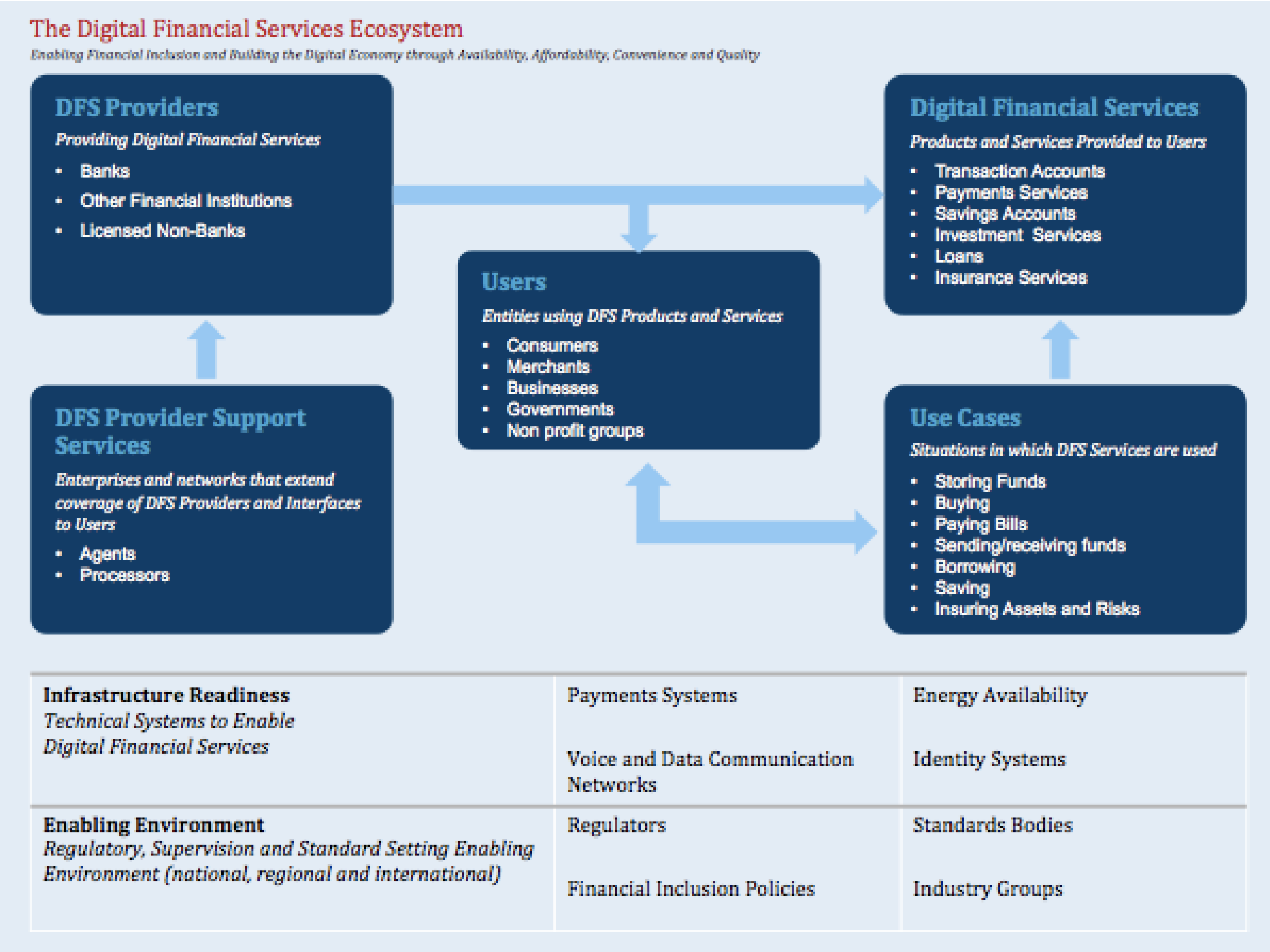

Figure 1: The Digital Financial Services Ecosystem

This report describes aspects of the Identity Systems infrastructure that enable digital financial services: account opening (eKYC) and strong electronic credential authentication.

3 Strong Authentication Techniques and Standards

A primary goal of authentication systems is to increase confidence that a previously-enrolled user is actually that user. Access control and authorization policy can then be applied to that authenticated user.

Authentication systems involve individuals, credentials issued to those individuals, and authenticators used by the individual to prove they are the original registered credential receiver. Authentication protocols define how each element interacts to authenticate the individual. Each element has observable or measurable behaviors in the environment which can be compared to previously-measured 'normal' behavior.

Design decisions and technology choices for each authentication system element affect how ‘strong’ an authentication system is: how resistant to attack and compromise due to common threats. ‘Strong’ authentication systems are designed to mitigate weaknesses that ‘weak’ authentication systems do not.

For example, a weakness for individuals is having to deal with password systems. Passwords are hard to remember, easy to steal, reused across services and very inconvenient to use. Stronger authentication systems might choose to use a biometric to unlock a local secure encryption key vault, which gives the individual a lower-friction, password-less experience.

Authenticators such as SMS-delivered one-time codes that are subject to phishing could be replaced by hardware cryptographic authenticators such as a Secure Element or Trusted Execution Environment in mobile devices.

Authentication protocols that use shared secrets or unencrypted transmissions could be replaced with asymmetric key cryptographic protocols, encrypted channels and different keys for each service. Multi-factor authentication protocols have additional attacker resistance than single-factor protocols.

The threat landscape changes regularly and design decisions must be made to address new or commonly-used threats. For example, threats to web site access from desktop computers are different from mobile-only apps and services which have been invented in recent years.

3.1 Characteristics of Advanced Authentication Systems

Typical authentication systems in use today were designed for the pre-mobile-device internet. They are based on a single authentication event, typically performed at application start up, and assume that the user, device and session do not change after that single authentication event. Authentication tends to be a high friction activity with a poor user experience, especially when password or multi-factor authentication are used. Current-generation authentication systems are not easy for mobile users to interact with: on mobile devices, authentication events are infrequent and rely on device security locks that may not be effective.

Advanced authentication systems are designed to address today’s threat models and design patterns. Compared to ‘strong’ authentication systems, there is an increased emphasis on detection and authentication of human users versus the client software used by people through environmental and behavioral analysis. New approaches are being implemented to minimize friction for mobile and multi-factor use cases: many systems are now built with ‘mobile first’ designs. Authentication now happens at many points during a user-system interaction: at identification time, at times when increased privileges are invoked (so-called ‘step-up’ authentication), and even continuously during the entire session.

The objective of advanced authentication systems is to provide a low-friction experience for users, while reducing risk and increasing security assurance.

Characteristics of advanced authentication systems	**Description**
Elimination or reduced reliance on passwords	Use of passwords to authenticate is hard for users, particularly on mobile devices. Password systems are increasingly vulnerable to database breaches and phishing.
Multi-modal user authentication	The authentication step is designed using more than one authentication mode to minimize user friction. Modes could include push to mobile app, web-based form, device biometric matching, passwords, or voice response.
Real-time analysis of user behavior to detect anomalies	Detection of anomalies that are inconsistent with the mode of access, such as having a user session jump between distant geographical locations, use of an unregistered device, or change in web browser mid-session.
Continuous authentication of user, software and device	Continuous authentication techniques challenge the user, software or device throughout the session, seeking valid responses. Some continuous authentication techniques are invisible to the user, especially at the device and software levels.
Dynamic risk scoring of authentication confidence	Authentication confidence takes several factors into account, such as: device capabilities, the requested transaction, use of weaker or stronger authenticators.
Consistency across all devices and channels a user chooses to use	Authentication systems are designed for user experience and security. Users are connecting to services using whichever channel is convenient for the user. Authentication systems must ensure that the authentication confidence is maintained no matter which channel is used.

Table 1: Advanced Authentication System Characteristics

3.2 Overview of Standards and Specifications for Strong Authentication

This section describes standards that cover strong authentication and authentication technologies that support strong authentication mechanisms. Authentication systems using these technologies can deliver strong user authentication plus low-friction user experience and dynamic risk evaluation.

3.2.1 ITU-T Recommendation X.1254

Recommendation ITU-T X.1254 *Entity authentication assurance framework* [3] describes an authentication assurance model which can be used by service providers and authentication providers to communicate about expectations and available authentication mechanisms. The authentication assurance model includes four levels of increasing assurance. There are many inputs used to determine the level of assurance achieved by an authentication method.

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Table 2: X.1254 Levels of Assurance

In the entity authentication phase, the entity uses its credential to attest its identity to a Relying Party (RP). The authentication process is concerned solely with the establishment of confidence in the claim or assertion of identity, and it has no bearing on or relationship with the actions the relying party may choose to take based upon the claim or assertion.

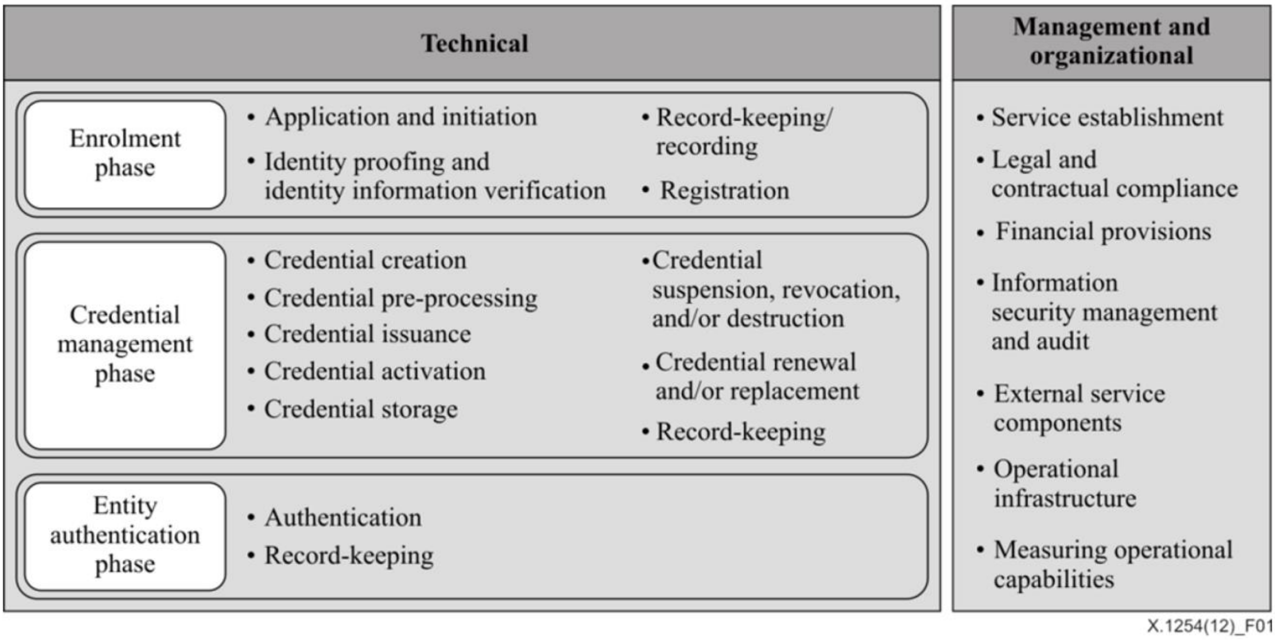

Figure 2: X.1254 Entity authentication assurance framework elements

ITU-T X.1254 section 10.3 describes threats to and controls for the authentication phase.

3.2.2 NIST Special Publication 800-63-3

NIST Special Publication 800-63B *Digital Identity Guidelines Part B* [4] addresses how an individual can authenticate using an authentication system. Similar to ITU-T X.1254, the NIST document uses levels of assurance to indicate relative effectiveness of authenticators and authentication protocols.

The publication lists the authenticator types and authentication protocols capabilities that are acceptable at each level of assurance.

3.2.3 eIDAS Regulation

The Regulation (EU) N°910/2014[1] on electronic identification and trust services for electronic transactions (eIDAS Regulation) provides a regulatory environment to European Union members to enable secure electronic interactions between businesses, citizens and public authorities. An important aspect of the eIDAS Regulation is that it describes electronic identification assurance levels. Assurance levels in eIDAS fulfil the same function as those in Recommendation X.1254 and NIST SP 800-63-3.

3.2.4 Payment Services Directive

The Payment Services Directive (PSD2) is in force in Europe, and Strong Customer Authentication (SCA) will be required to access bank accounts for information aggregation or payment initiation. The "Regulatory Technical Standards on strong customer authentication and common and secure communication" (RTS), published by the European Banking Authority, describe the principles and requirements of multi-factor authentication and authentication code generation.

The RTS include the following requirements:

- Users must be authenticated using a minimum of two-factor authentication
- The authentication of a user should result in the generation of an authentication code, a cryptographic signature of the transaction. The authentication code must, in the case of remote payments, be linked to the amount and payee approved by the user
- The user's cryptographic material must be protected from unauthorized disclosure

3.2.5 FIDO Alliance Specifications

The FIDO Alliance protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user called "user verification". User verification can take the form of any number of user–friendly and secure action such as swiping a finger, performing facial recognition, entering a PIN, or speaking into a microphone. Private keys are bound to a device and prove that users are in possession of a specific device (i.e. – the "something you have" of authentication), and their combination with user verification ensures that every authentication is multi-factor authentication.

FIDO protocols are designed to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device and is only used for user verification to approve the use of a private key.

For implementing authentication beyond a password, companies have traditionally been faced with an entire stack of proprietary clients and protocols.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

To enable interoperability between client authentication methods, FIDO standardizes the client and protocol layers. This allows many client authentication methods such as biometrics, PINs and second–factors to be used with a variety of online services in an interoperable manner.

The main FIDO specifications are Universal Second Factor (U2F) [5], Universal Authentication Framework (UAF) [6] and the FIDO2 project which includes both the Client to Authenticator Protocol (CTAP) [7] and W3C's Web Authentication (WebAuthn) [5].

The FIDO2 Project is a set of interlocking initiatives that together create a FIDO Authentication standard for the web and greatly expands the FIDO ecosystem.

FIDO2 is comprised of the W3C's Web Authentication specification (WebAuthn) and FIDO's corresponding Client-to-Authenticator Protocol (CTAP), which collectively will enable users to leverage common devices to easily authenticate to online services — in both mobile and desktop environments.

3.2.5.1 Universal Authentication Framework (UAF)

The goal of the Universal Authentication Framework is to provide a broad and comprehensive framework for cryptographically secure multifactor authentication. It includes first-factor (e.g. PIN and biometrics), second-factor, as well as a generalized architecture and protocol that can be extended to any platform or integrated with any system.

The UAF specification standardizes four pieces:

1. The authenticator, which is a device that creates and securely stores the authentication secrets

2. The server, which registers users and subsequently validates authentication requests

3. The client, which acts as a multiplexer and policy enforcer between multiple servers and multiple authenticators.

4. The protocol, which defines the message formats, cryptographic objects, etc. that are carried between the authenticator and the server through the client.

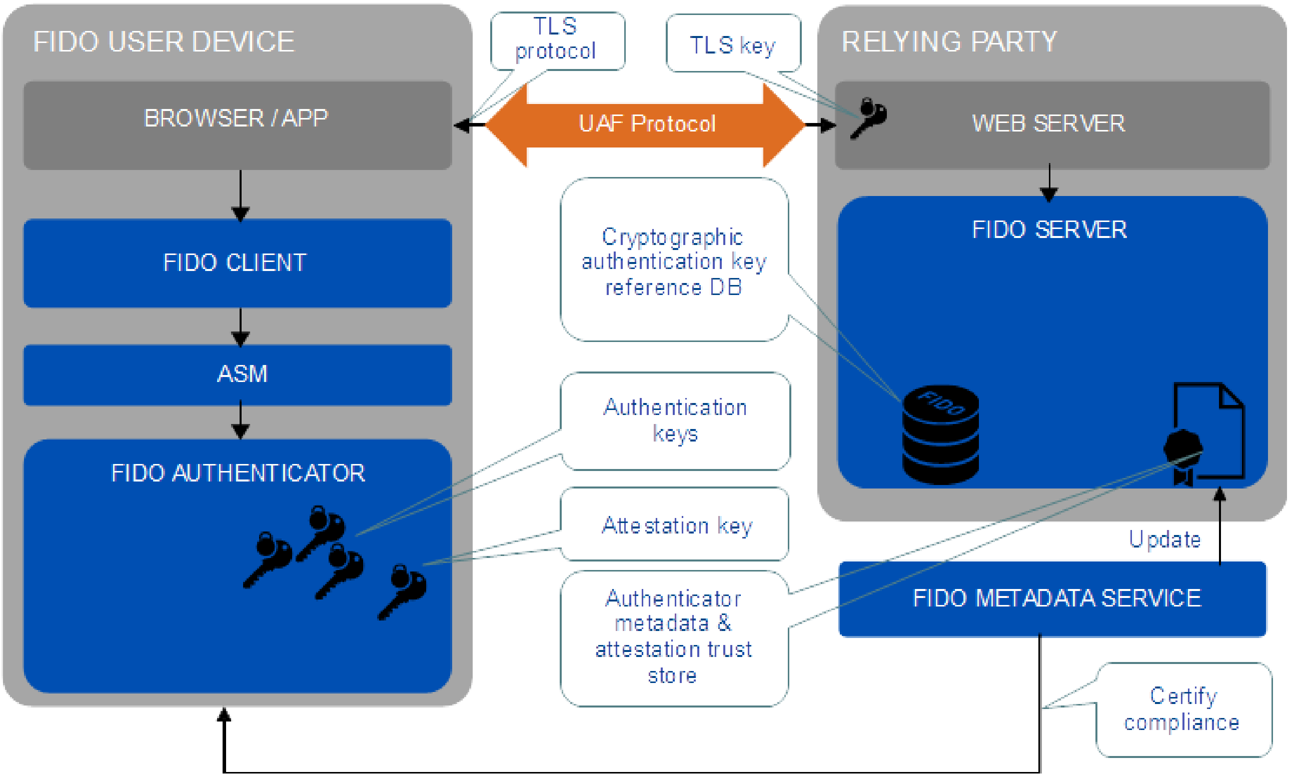

Figure 3: Universal Authentication Framework Architecture

This architecture is re-used by the other FIDO specifications.

3.2.5.2 Universal Second Factor (U2F)

The FIDO U2F specification is focused on the narrow goal of providing second-factor authentication in browsers. It defines a JavaScript API for browsers to perform second factor authentication using JavaScript register() and sign() functions; as well as defining NFC, Bluetooth Low Energy (BLE), and USB communications protocols for registering and authenticating with security keys. These specifications allow better user experience and more secure second factor authentication.

Note that the FIDO U2F JavaScript API has been superseded by WebAuthn and the transport specifications for NFC, BLE, and USB have been merged into the latest FIDO CTAP specifications.

3.2.5.3 Client to Authenticator Protocol (CTAP)

The CTAP specification describes a set of protocols for communication between external authenticator devices and a client/platform, as well as bindings of this application protocol to a variety of transport protocols using different device communication protocols (USB, NFC, Bluetooth). Each transport binding defines the details of how a client (such as a browser or operating system) can make requests to an authenticator to register or authenticate against various services.

CTAP is intended to be used in scenarios where a user interacts with a relying party (a website or native app) on some platform (e.g., a PC) which prompts the user to interact with an external authenticator (e.g., a smartphone).

In order to provide evidence of user interaction, an external authenticator implementing this protocol is expected to have a mechanism to obtain a user gesture. Examples of user gestures include: as a consent button, password, a PIN, a biometric or a combination of these.

The CTAP specification was created as part of the FIDO2 project, in conjunction with the WebAuthn specification. It contains two distinct protocols: 1) the original U2F transport protocols that enable authenticator devices to perform second factor authentication, retroactively named “CTAP1”; 2) an extended and reformatted set of U2F transport protocols that enable multifactor authentication, named “CTAP2”.

3.2.5.4 Web Authentication (WebAuthn)

As part of the FIDO2 project, the FIDO Alliance collaborated with the World Wide Web Consortium (W3C) to standardize the browser’s JavaScript APIs for cryptographically strong multifactor authentication – known as Web Authentication. The WebAuthn specification is a Proposed Recommendation of the W3C and includes both browser specific portions of authentication (APIs and browser processing rules) as well as generic message formats (assertions and attestations) that may be reused for non-browser implementations such as servers, operating systems, and authenticators communicating using the CTAP protocol. The WebAuthn specification also defines a series of extensible points, such as the ability to add new attestation formats and the ability to add new extensions to the protocol and define their processing rules.

3.2.5.5 FIDO Registration Flow

The figure below shows the simplified message flows for registration.

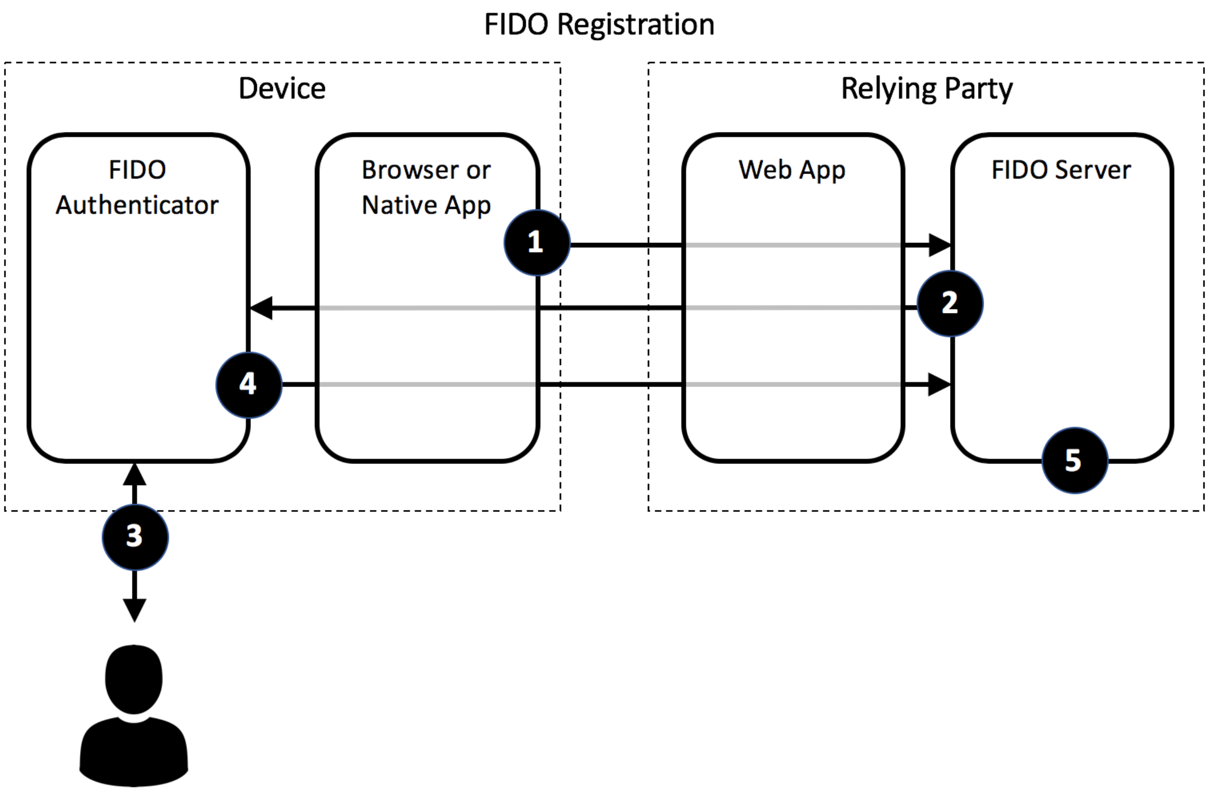

Figure 4: FIDO Registration of new keys

1. Initiate registration with Relying Party

2. FIDO Server sends registration challenge and requested registration options

3. Authenticator performs user verification on device to signal the user's consent to registering with the service

4. Authenticator generates a new key pair for the service and associates the private key with the service's origin. The public key is and device model number are signed over by a device model specific (shared across no less than 100,000 devices) attestation private key. The authenticator sends a registration response: device model number + device attestation signature + user's public key

5. Validate response and attestation. The device model number (AAGUID) can be used to look up metadata about the device, such as the attestation public key, the type of user verification being performed (e.g. – biometric, PIN), and the security characteristics of the device (e.g. – how private keys are protected; how biometric templates are protected; third-party security and biometric certifications).

6. The service stores user's public key for future authentication requests.

3.2.5.6 FIDO Authentication Flow

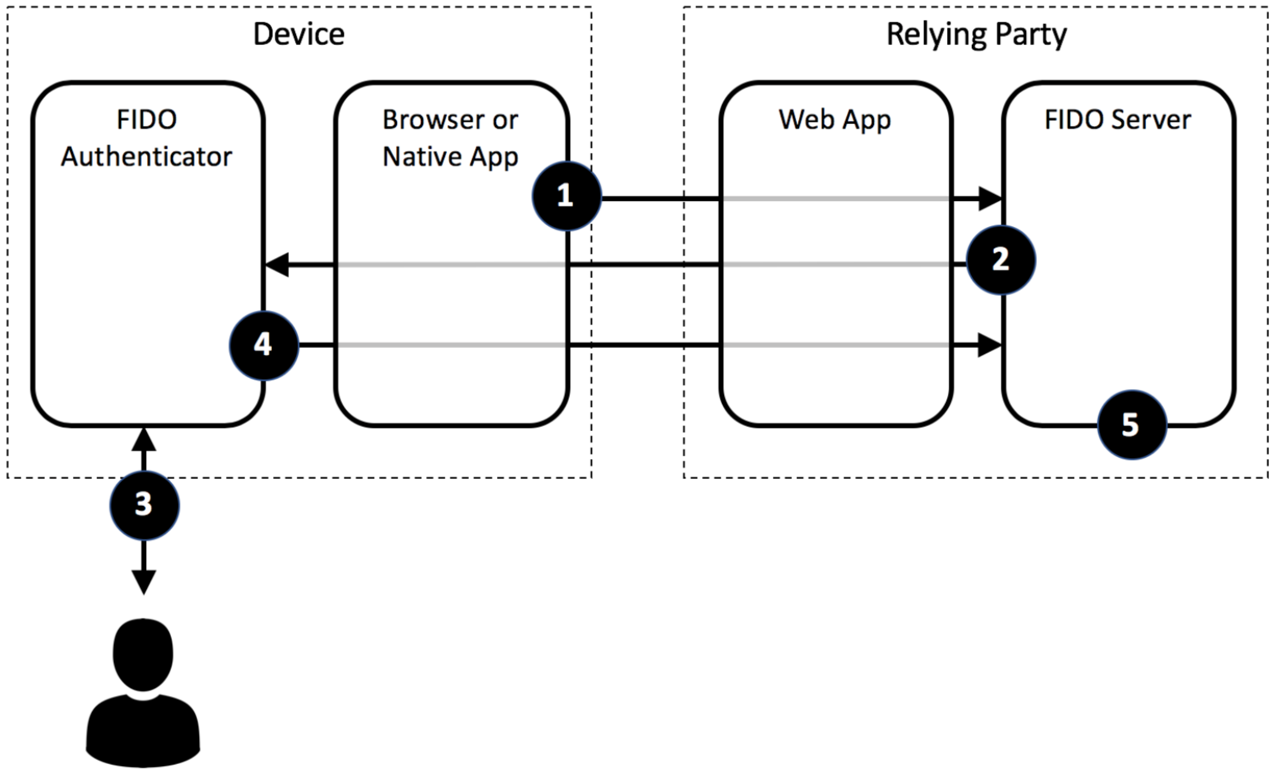

Figure 5: FIDO Authentication

1. Initiate authentication with Relying Party

2. FIDO Server sends authentication challenge and preferences for the authenticators or credentials to be used

3. Authenticator performs user verification on device to signal the user's consent to authenticate with the service

4. The authenticator uses the service's origin to look up the private key for authentication and uses the private key to sign the challenge from the server. The server sends an authentication response: challenge + signature.

5. The server retrieves the public key for the user and validates the signature on the challenge.

3.2.6 Mobile Connect Specifications

Mobile Connect is the mobile operator-facilitated secure universal identity solution developed by the GSMA in collaboration with Mobile Operators. The GSMA represents the interests of mobile operators worldwide spanning more than 220 countries and unites nearly 800 of the world's mobile operators, as well as more than 230 companies in the broader mobile ecosystem. To-date there are more than 470 million active Mobile Connect users via over 70 operators covering more than 40 countries and reaching more than 3 billion people.

Mobile Connect is a portfolio of mobile-enabled services that can be integrated into a Service Provider's application to support access to services provided by the Service Provider. Mobile Connect provides strong customer authentication, authorisation, and permissioned access to a User's identity and contextual network attributes. Figure 6 outlines the range of services provided by Mobile Connect.

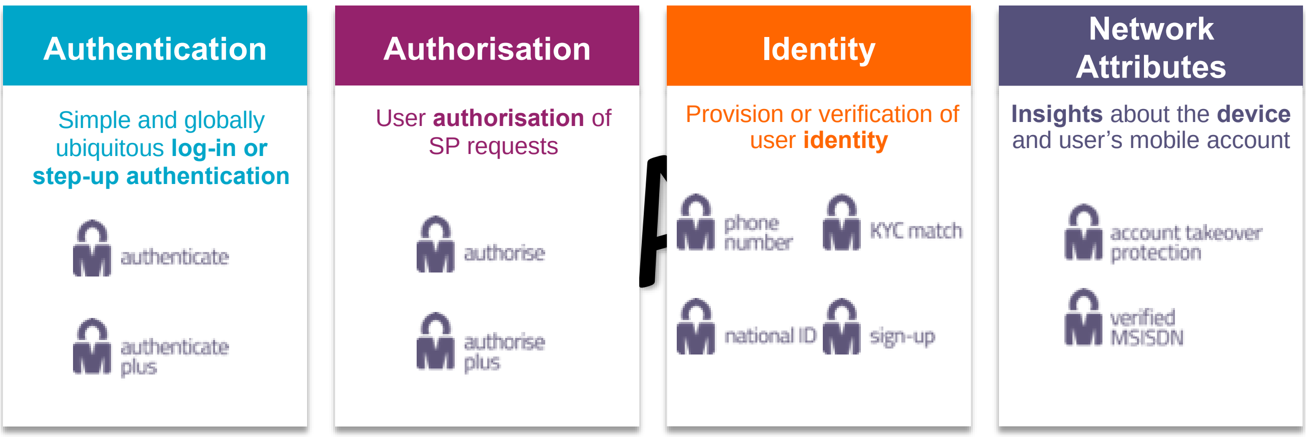

Figure 6: Mobile Connect Portfolio of Services

Mobile Connect uses a distributed architecture in which each Mobile Operator deploys Mobile Connect services for its particular user base, but with all deployments abiding by a strict set of technical standards to ensure that from a Service Provider's perspective, the experience of consuming Mobile Connect services from any of the Mobile Operators is consistent.

Mobile Connect is based upon the OpenID Connect (OIDC) protocol which provides an identity layer on top of the OAuth 2.0 protocol. It allows Users to be identified by their MSISDN (or a related Pseudonymous Customer Reference) and to be authenticated securely via their mobile device with the SIM providing security. Mobile Connect defines two profiles of OIDC to support Device-Initiated and Server-Initiated requests for authentication, authorisation or permissioned access to User attributes.

The serving Mobile Operator supports and selects an appropriate Authenticator to present the authentication and authorisation requests to the User on their mobile device to which the User responds. The Authenticator may also be used to seek User consent for the serving Operator to share or validate User attributes with the Service Provider. The Authenticator is selected based on Operator policy, device capability and the Level of Assurance required.

Mobile Connect authentication factors and insights include:

- Possession-based (Something I Have); the possession of the mobile device by the user. This is the first factor used in Mobile Connect Authentication.
- Knowledge/secrecy-based (Something I Know); for example, PIN/Personal Code.
- Active Inherence (Something I Am); for example, biometrics: fingerprints, iris scan, facial biometrics.
- Passive Inherence (Something the Network Knows); Mobile network-based inherence elements, such as usual cell sites (can also be used as "something the user does") available to the mobile operator. This separation between device and network is vital to fighting fraud and establishing ownership of the device.
- Contextual (Something I Do); for example, supplement the device-based authentication with network-based insights to create a more robust multi-factor authentication mechanism (such as pairing status between IMSI, IMEI and MSISDN).

Mobile Connect levels of assurance are a guide to the degree of confidence in an authentication process. As a critical element within the Mobile Connect ecosystem, the Mobile Connect levels of assurance are used in the Mobile Connect API (OpenID Connect), in the cryptographically-signed Identity Token sent as an authentication proof to the Service Provider, in the authenticator-selection policy and also in the Mobile Connect product-enablement policy.

3.2.6.1 Mobile Connect for eIDAS

Mobile Connect levels of assurance have been mapped against the minimum technical specification requirements of the Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means and authentication.

In the following table there is a mapping between Mobile Connect and eIDAS level of assurance.

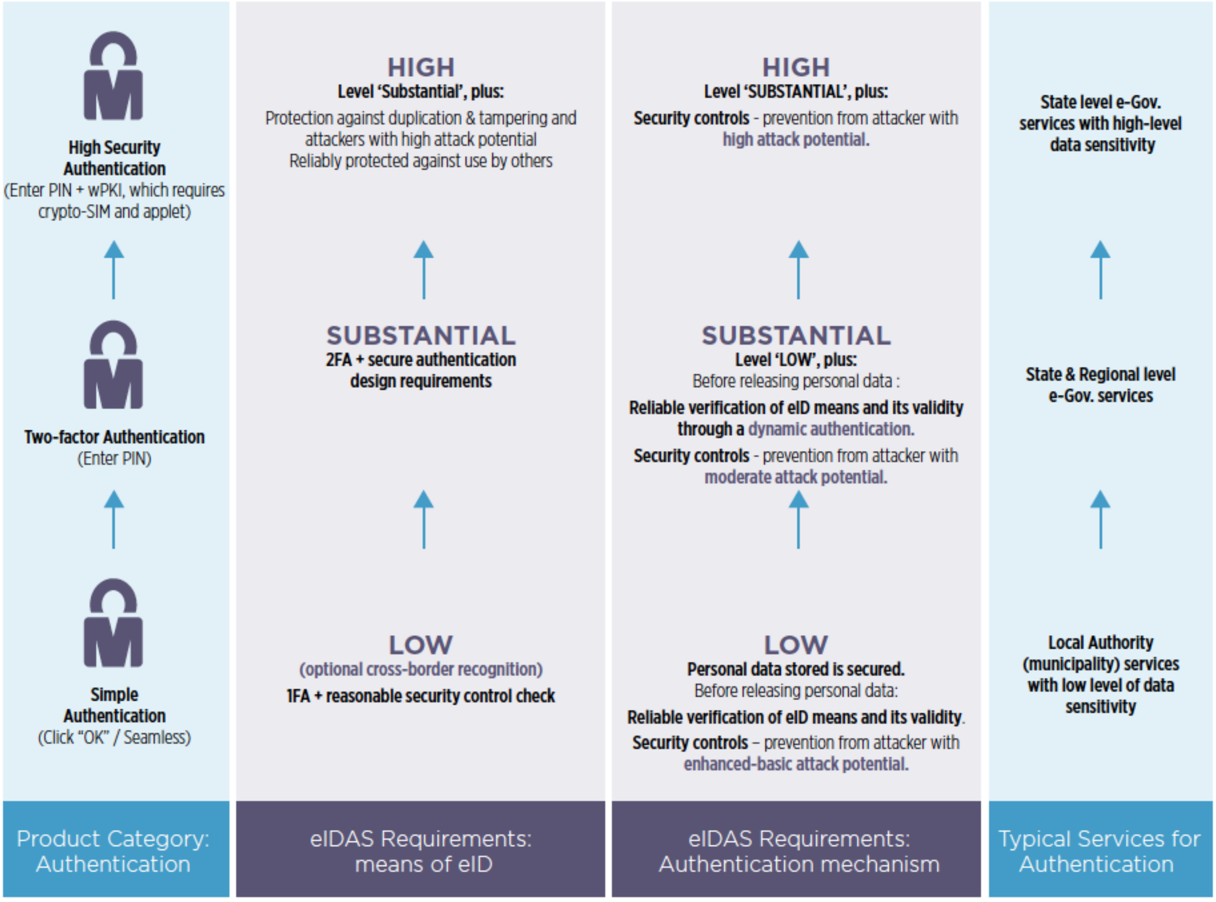

Figure 7: eIDAS level of assurance mapping with Mobile Connect

Mobile Connect also meets the eIDAS technical specification and interoperability requirements for integration with national ID as designed by EU Member States eIDAS Nodes in collaboration with the European Commission CEF project: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile. An example reference architecture of eIDAS for the integration with Mobile Connect is shown in the following diagram.

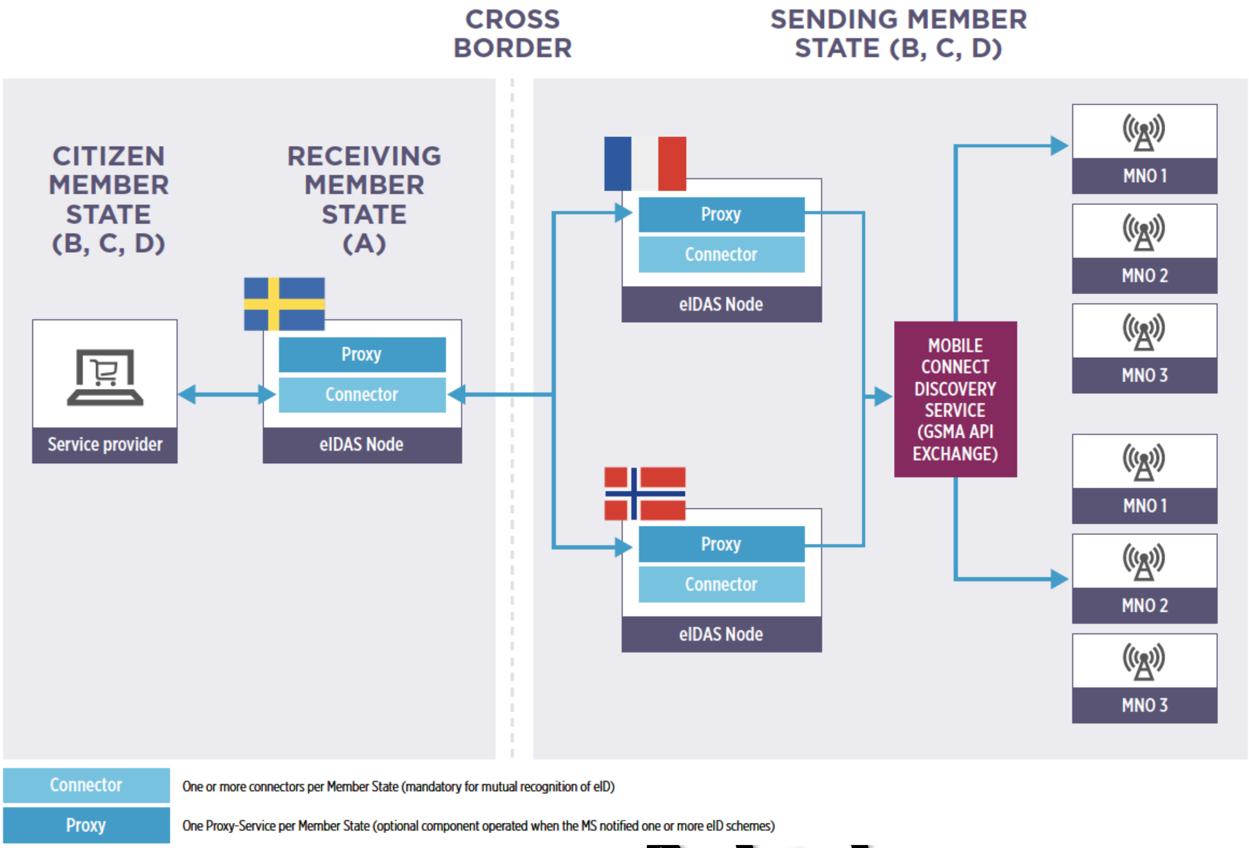

Figure 8: Mobile Connect and eIDAS reference architecture

A flowchart of Mobile Connect used within an eIDAS deployment is shown below.

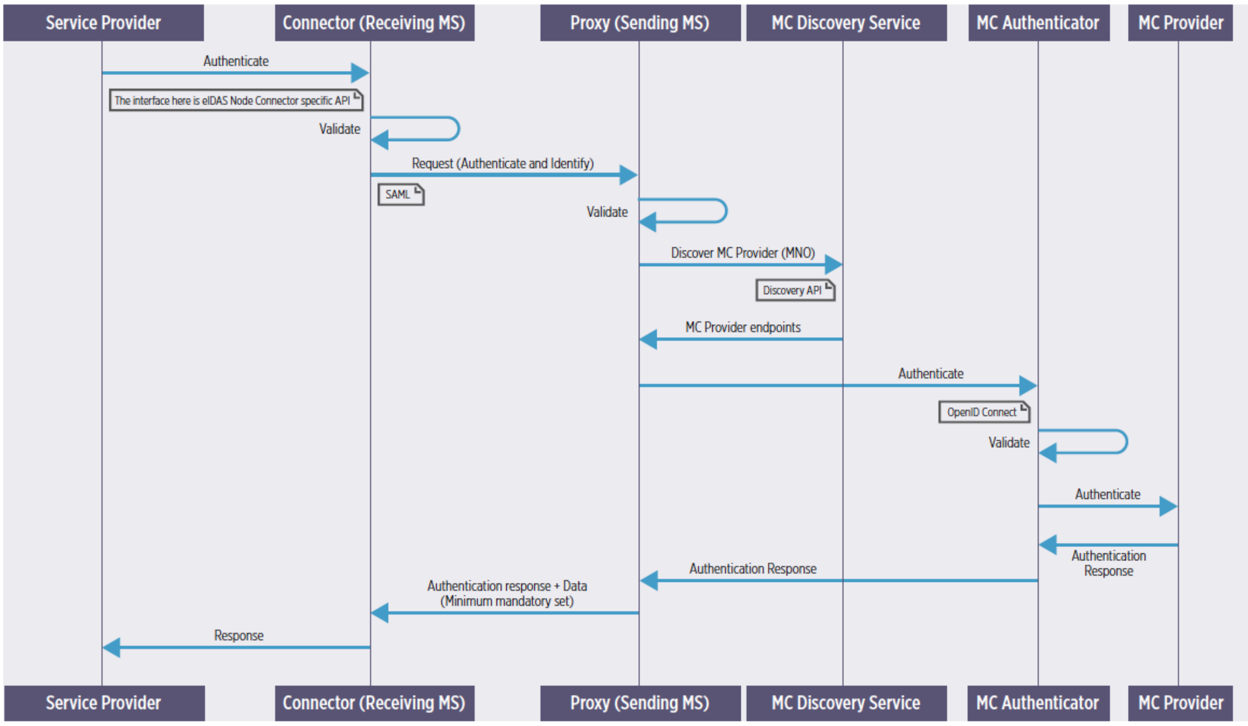

Figure 9: Mobile Connect and eIDAS technical flow

3.2.6.2 Mobile Connect for PSD2

In relation to PSD2, the Mobile Connect framework uses out-of-band Authentication, such that the Authentication channel is separated from the service request channel and utilises the SIM-enabled mobile device along with support from the mobile network in addition to providing dynamic linking to be fully PSD2 compliant. Mobile Connect can support SCA in both decoupled and OAuth modes.

The following figures illustrate the use cases, architecture and flows related to PSD2.

Scenario	Mobile Connect as Second Factor Solution (upgrade from SMS OTP)	Mobile Connect as Two-Factor Solution
Login to account	authenticate, authenticate plus, verified MSISDN	authenticate plus
Payment authorisation	authorise, authorise plus	authorise plus
Scenario	**Mobile Connect providing risk factors into fraud decision engine**	
Transaction risk monitoring, incl. for TRA*	account takeover protection, verified MSISDN, KYC match **Other products on roadmap (Proximity, Roaming...)**	

*TRA: Transaction Risk Analysis exemption

Figure 10: Mobile Connect PSD2 Use Cases

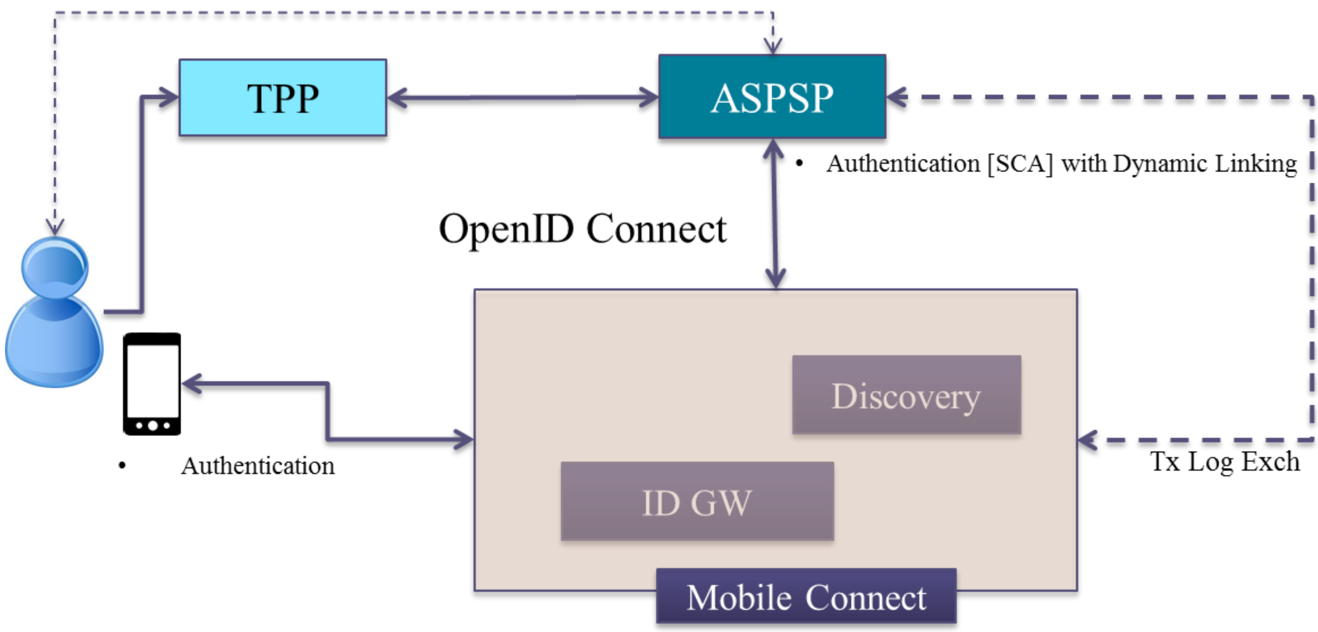

Figure 11: High Level Reference Architecture for PSD2

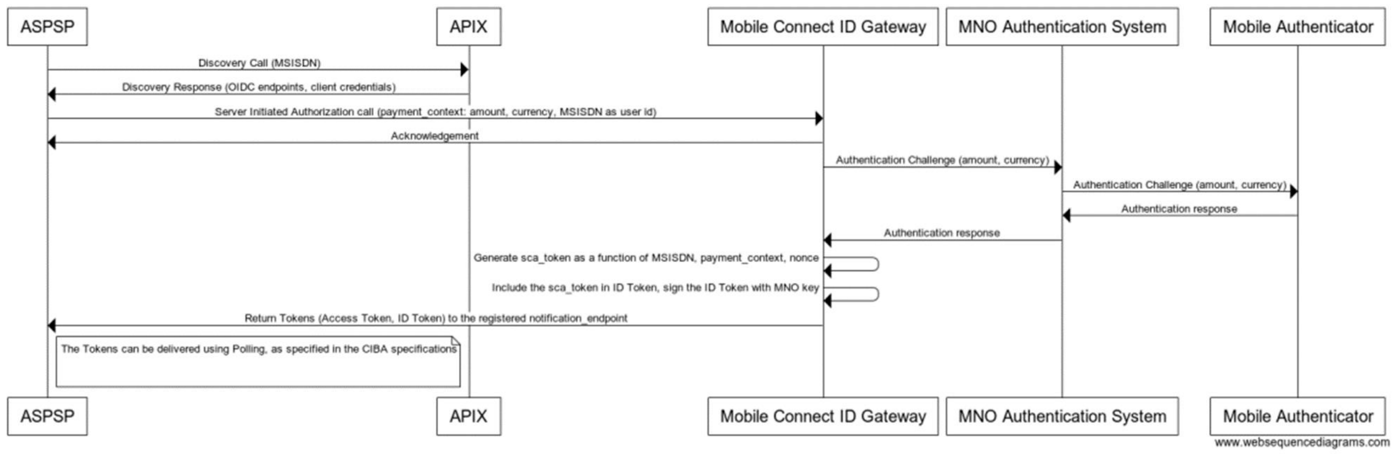

Figure 12: Mobile Connect Strong Customer Authentication - Server Initiated

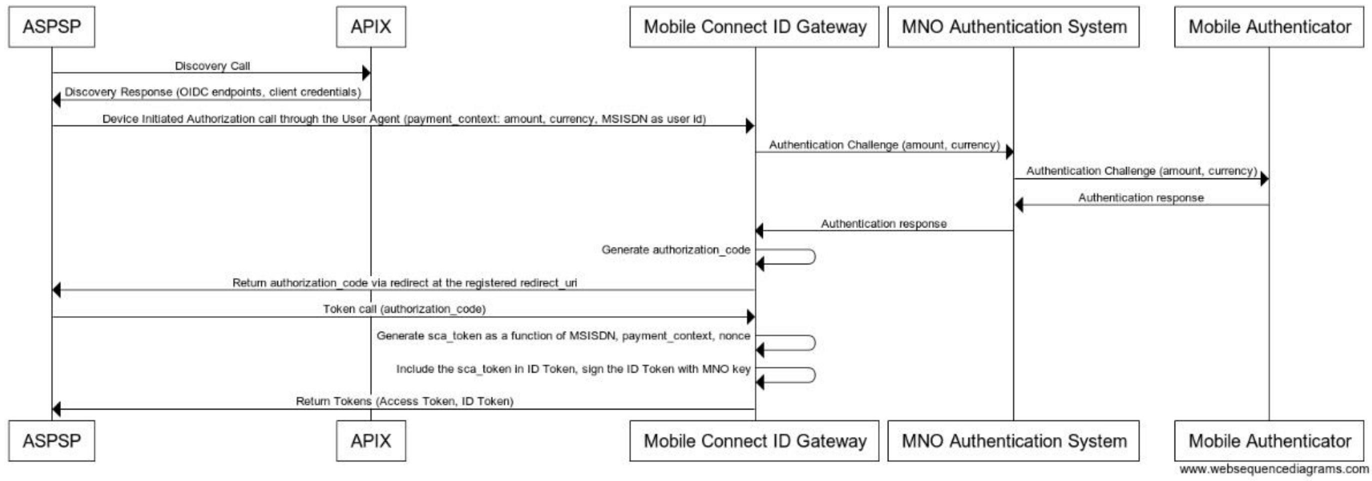

Figure 13: Mobile Connect Strong Customer Authentication - Device Initiated

3.2.7 IFAA Specifications

IFAA (Internet Finance Authentication Alliance) was established in June 2015, where around 200 international company and institute members collaborate to innovate authentication scenarios, develop biometrics-based standards, and deliver financial-grade interoperable authentication solutions.

IFAA has been applying continuous focus to address authentication challenges by improving the efficiency while reducing the cost of device adaptation. The main IFAA specification is IFAA Local Passwordless Technical Specification (T/IFAA 0001-2016), which requires strict protection of user data in the trusted execution environment. To date, this specification has been supported by more than 1.2 billion mobile devices and 360 device models. In July 2018, an updated version IFAA Local Passwordless Technical Specification (T/IFAA 0002-2018) was published to describe the optional security-enhanced solution which uses SE (Secure Element) to protect sensitive applications, keys and data.

IFAA specifications have powered massive adoption of fingerprint authentication in scenarios of e-commerce, Internet Finance, Banking, Traveling, Mobile Office as well as IOT. Increased coverage of banks has been seen in the past months.

IFAA identifies two technical models for biometric authentication: local model and remote model. At present IFAA specifications focus on the local model, but the remote model is also on IFAA's schedule.

3.2.7.1 IFAA Biometric Authentication – Local Model

In the local model, the biometrics system resides in the user equipment. The biometric data are collected, stored and compared locally by the biometrics system when called by the user application but the authentication decision is not made locally. A credential will be provided based on the output of the local biometrics system and sent by the user application to the server side. The authentication decision will be made by the authentication server based on the credential provided from the user equipment.

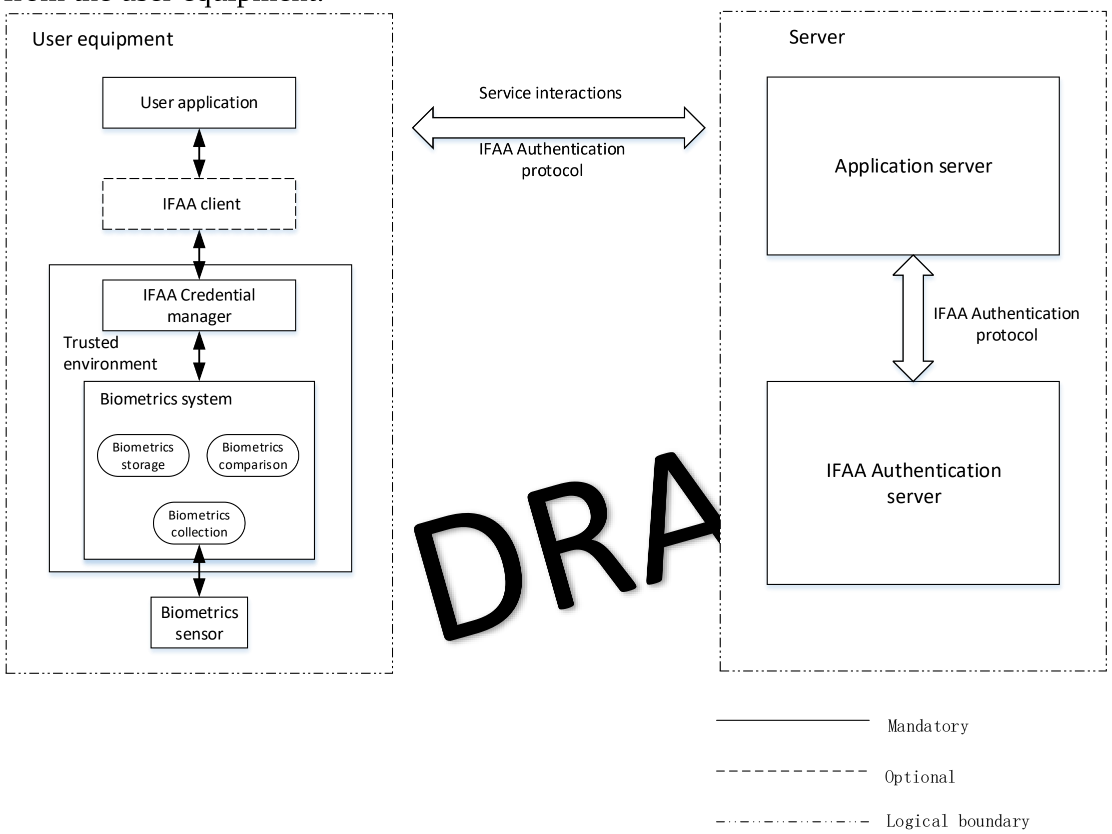

Figure 14 is the technical framework of this model.

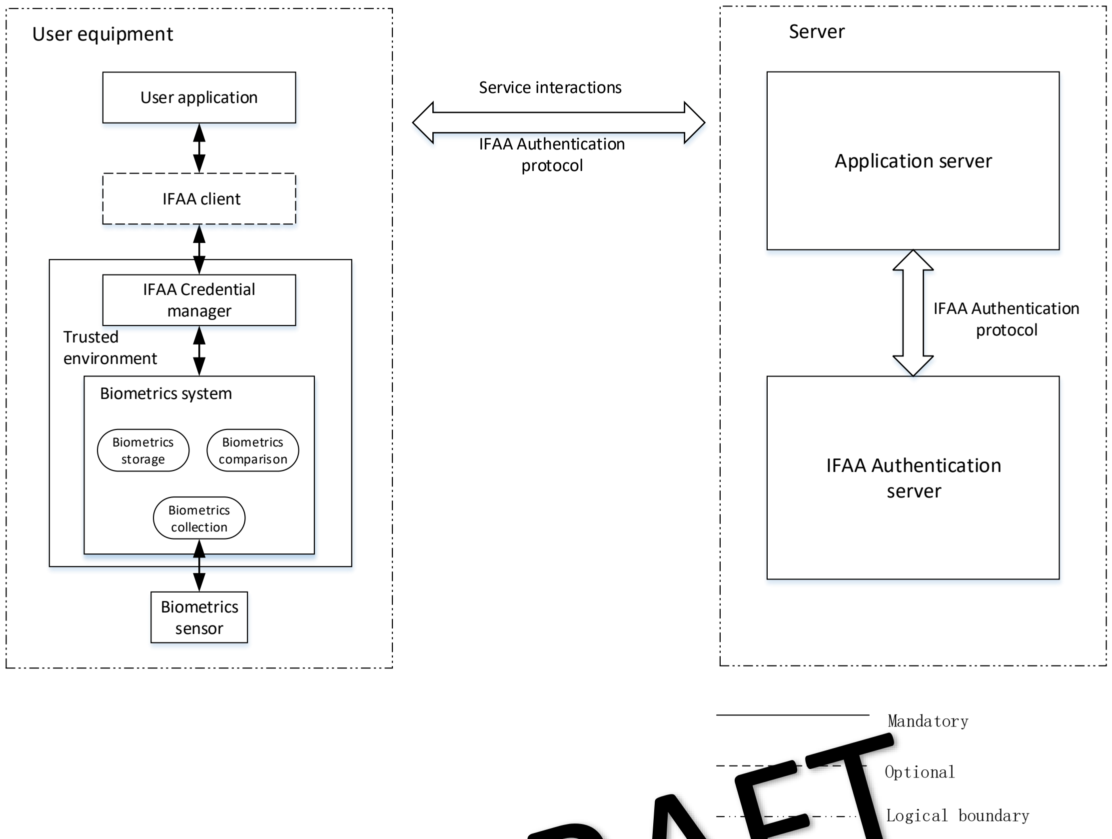

Figure 14: IFAA biometric authentication – local model

IFAA specifications define three main protocols for the local model: registration, authentication, and deregistration.

Figure 15 is the message flow of the registration protocol:

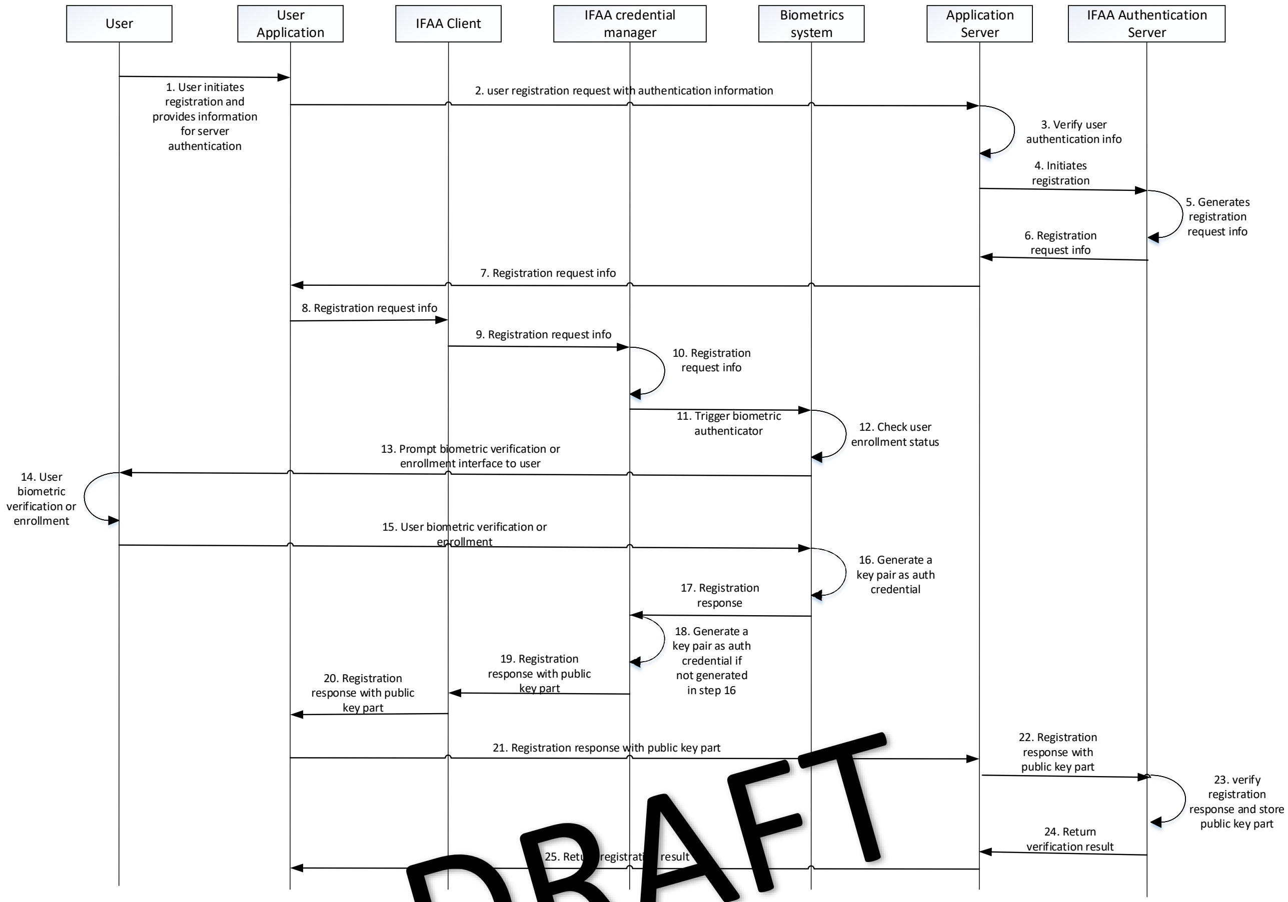

Figure 15: IFAA biometric authentication – local model – Registration

Figure 16 is the message flow of the authentication protocol:

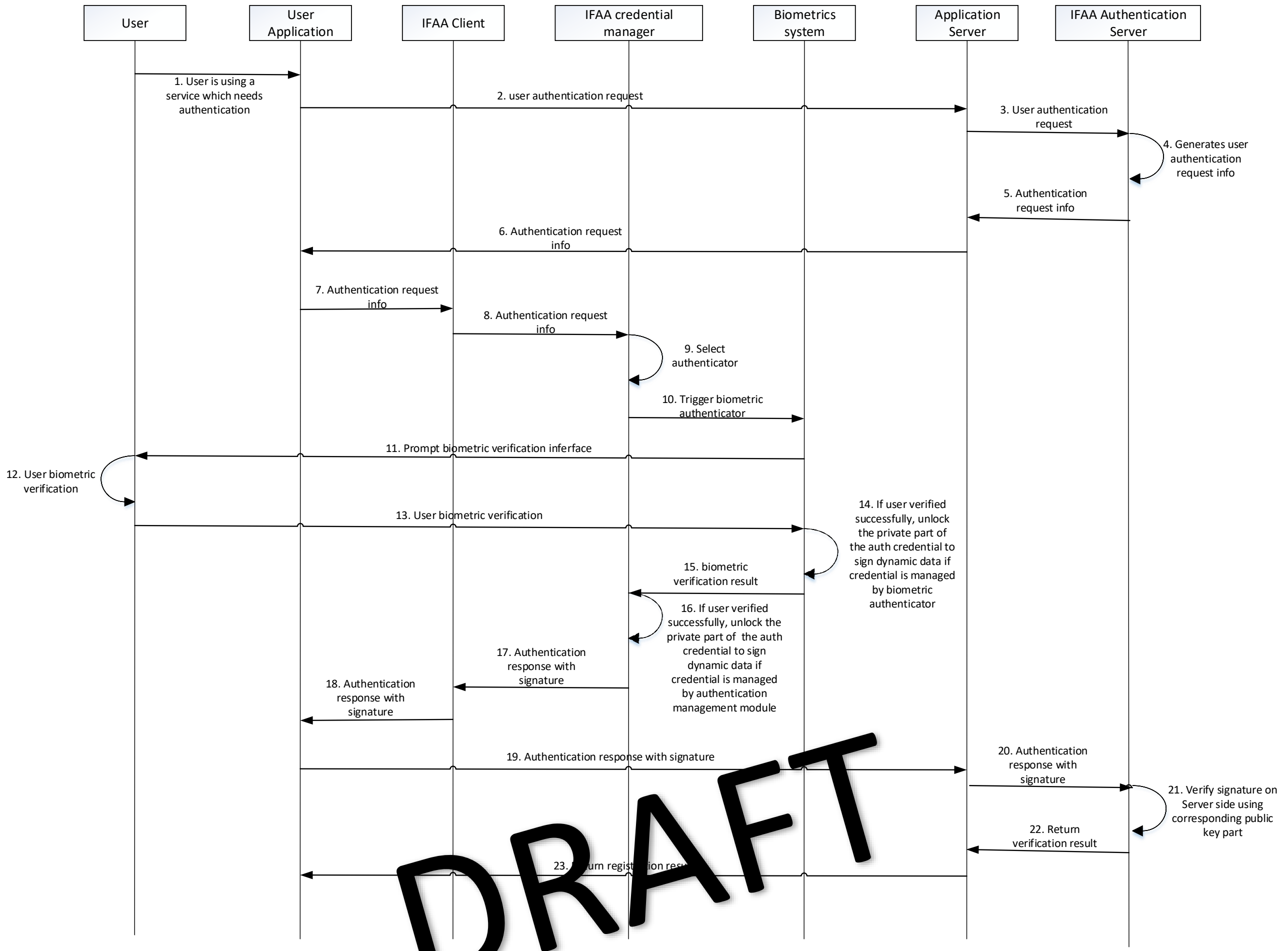

Figure 16: IFAA biometric authentication – local model – Authentication

Figure 17 is the message flow of the deregistration protocol:

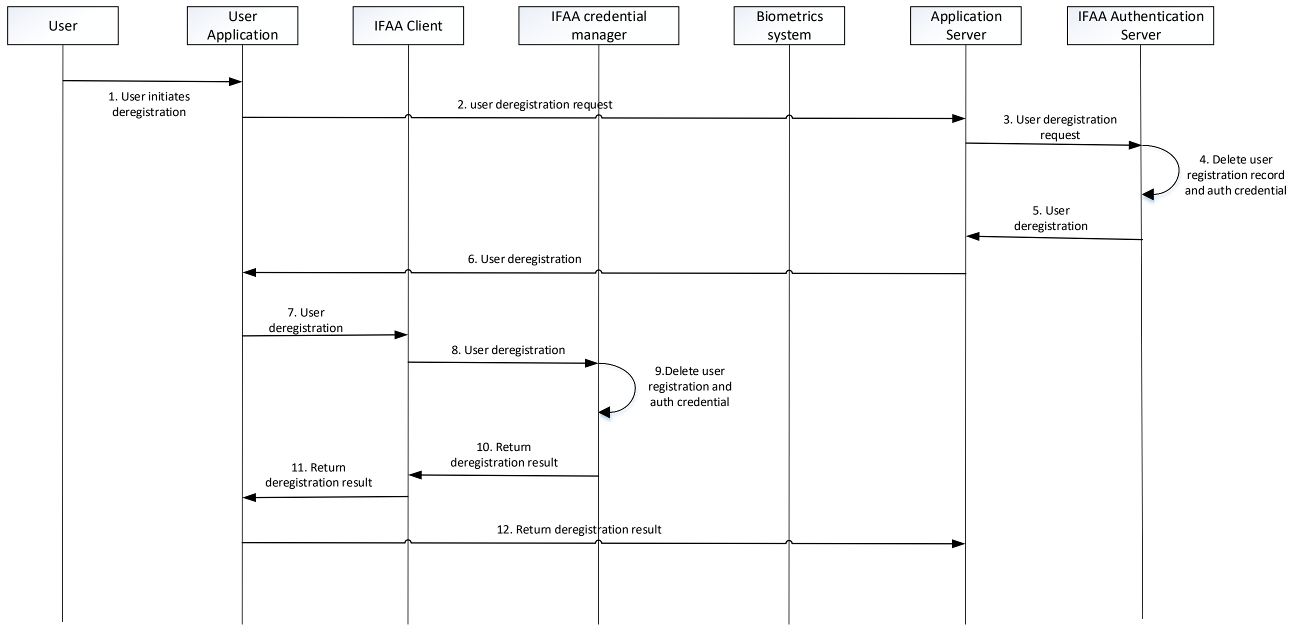

Figure 17: IFAA biometric authentication – local model – Deregistration

3.2.7.2 IFAA Biometric Authentication - Remote Model

In the remote model, the biometrics system is divided into two parts: the biometrics collection module resides in the user equipment, but the biometrics storage module and comparison module reside in the authentication server. The biometric data are collected locally but not stored or compared locally, instead they are sent to the server side by the user application and verified by the biometrics system in the authentication server. Figure 18 is the technical framework of this model.

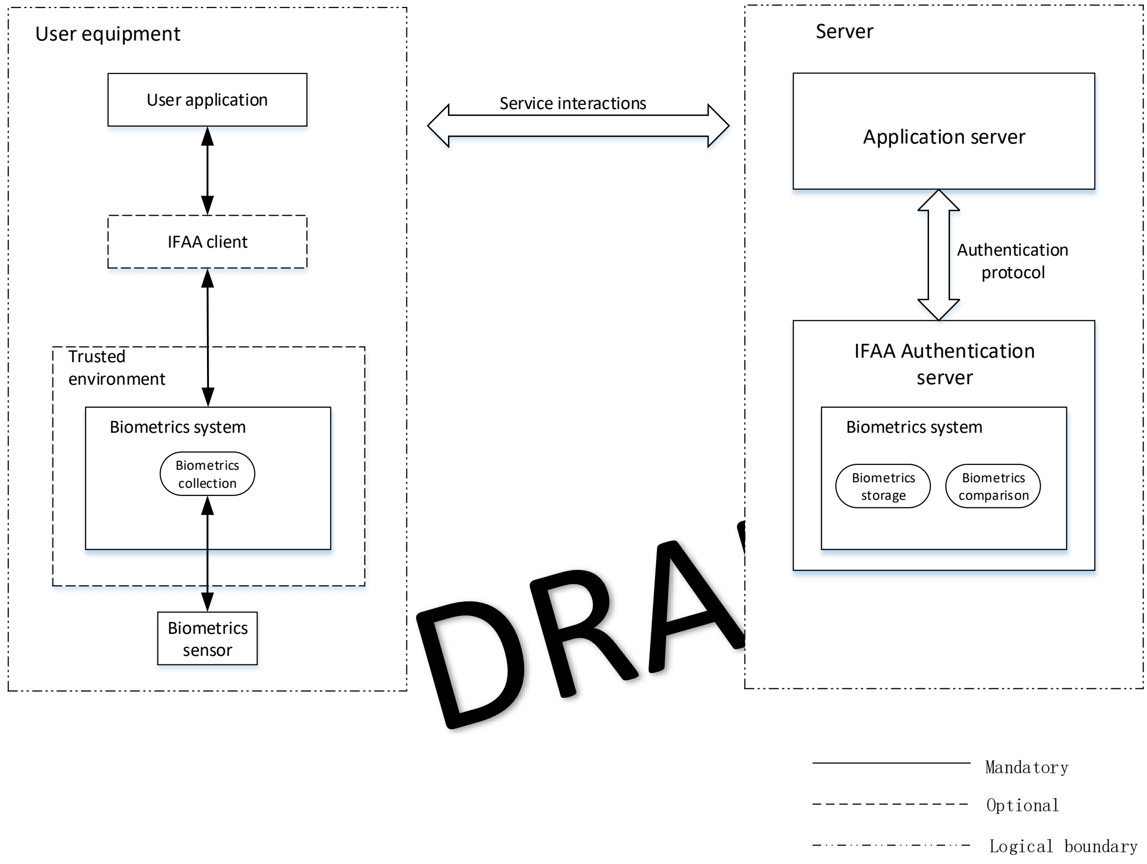

Figure 18: IFAA biometric authentication – remote model

3.2.8 Aadhaar Authentication Specifications

Aadhaar refers to a 12-digit random identification number issued by the Unique Identification Authority of India (UIDAI). Originally established under an executive order in January 2009, UIDAI came to become a statutory body under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"), under the Ministry of Electronics and Information Technology (MeitY), Government of India. It is the largest national biometric database in the world and the Authority has issued more than 1180 million Aadhaar numbers so far.

Aadhaar is an identity system with open APIs (Application programming Interfaces) to online authenticate the identity claim and the UIDAI has been tasked with three key functional processes: enrolment, identification and authentication. Through an extensive network of enrolment agencies, UIDAI collects the demographic (name, date of birth, gender, address) and biometric (fingerprints, iris scan and photograph) information of individuals for the purposes of enrolling them into the Aadhaar system. A number of applications like eSign, digital locker, Mobile banking Apps etc based on biometrics technology are using Aadhaar based authentication services.

The three key functional processes: enrolment, identification and verification (Figure 19) are carried out by UIDAI through the biometric system that represents the technical and functional blocks that capture, process, store, compare and decide on processing of biometric data:

- **Enrolment process**: creating and storing an enrolment data record for an individual who is the subject of a biometric capture process in accordance with the enrolment policy. The subject usually presents his/her biometric characteristics to a sensor along with his/her identity reference. The captured biometric sample is processed to extract the features which are enrolled as a reference in the enrolment database with identity reference.
- **Identification process**: searching the enrolment database against the captured and extracted biometric features to return a candidate list. The candidate list consists of individuals whose references match with the feature in comparison subsystems and have a similarity score value higher than a predefined threshold value.
- **Verification process**: testing a claim that an individual who is the subject of a biometric capture process is the source of a specified biometric reference. The subject presents his/ her identity reference for a claim of identity and biometric characteristic(s) to the capturing device, which acquires biometric sample(s) to be used for comparison with the biometric reference linked to the identity reference for identification. The verification process has a possibility of impacting a subject's information privacy, since this process requires both biometric reference and identity reference. The identification process requires exhaustive search of enrolment database. So, this also has a possibility of impacting on subject's physical privacy. Verification is generally considered to be less privacy intrusive than identification. In Aadhaar system verification is done via online authentication having only a "yes/no" answer.

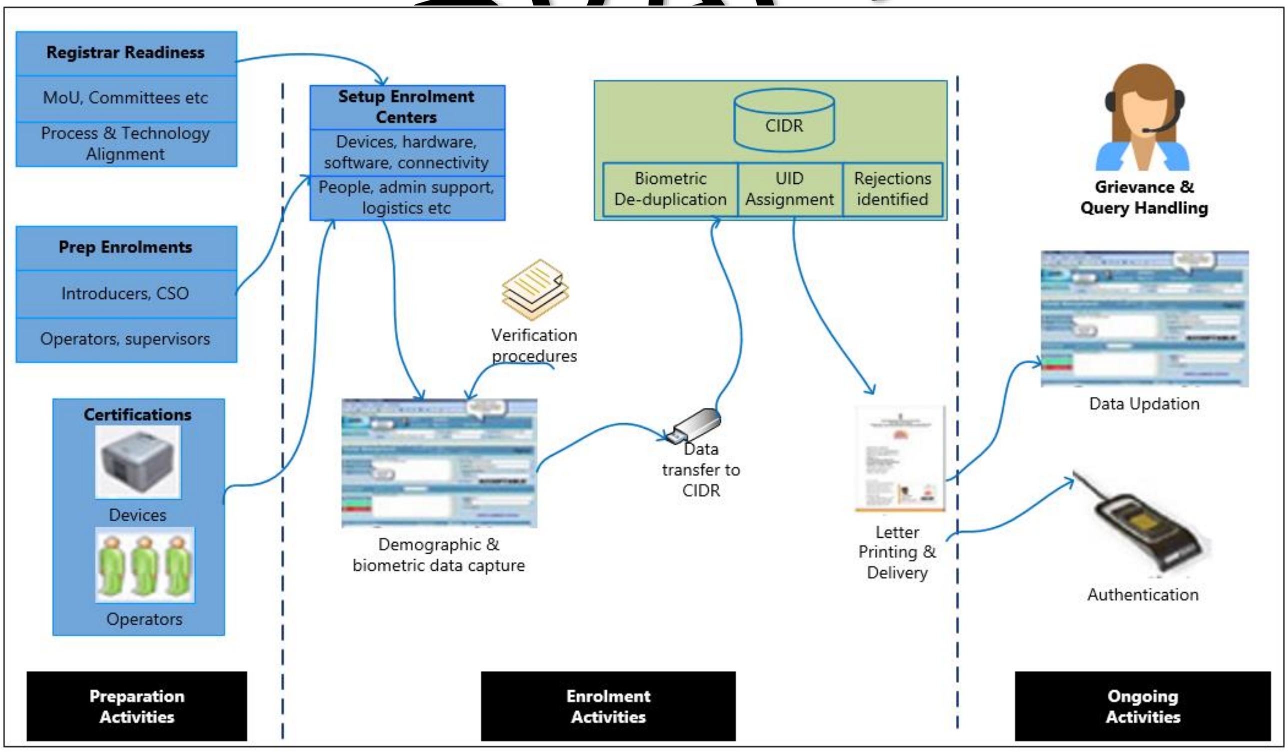

Figure 19: Aadhaar end-to-end process flow

3.2.9 The ID2020 Alliance

The ID2020 Alliance is a public-private partnership committed to improving lives through digital identity. The Alliance brings together multinational institutions, non-profits, philanthropy, business, and governments to set technical standards for a safe, secure, and interoperable digital identity that is owned and controlled by the user. It funds high-impact pilot projects that bring digital identity to vulnerable populations, and uses the data generated to find scalable solutions and inform public policy.

The overall objective of the ID2020 Alliance is to empower individuals, enable economic opportunity and advance global development by increasing access to digital identity.

By 2030, the Alliance aims to have facilitated the scaling of a safe, verifiable, persistent digital identity system, consistent with UN Sustainable Development Goal 16.9: “By 2030, provide legal identity for all, including birth registration”. From 2017 to 2020, the Alliance’s work will focus on two areas: developing and testing the best technological solutions for digital identity; and, working with governments and existing, established agencies to implement these solutions.

ID2020, working with these implementing agencies and governments, will finance digital identity pilot projects. These pilots will assess the cost, human resource requirements, opportunities and pitfalls associated with various pathways for enrolment and participation.

At their 2018 Summit, the ID2020 Alliance announced two pilot projects.

One of the two ID2020-supported pilot projects will be led by Alliance partner iRespond and will be conducted in close partnership with the International Rescue Committee (IRC). The pilot will offer blockchain-based digital identification, linked to individual users through iris recognition, for refugees accessing the IRC's services in the Mae La Camp in Thailand. Initially, these digital identities will enable the recipients to access improved, consistent healthcare within the camp through an accurate and secure electronic medical record. In the future, the same system may electronically document both educational attainment and professional skills to aid with employment opportunities.

The second pilot project will be led by Everest working in partnership with The Indonesian National Team for the Acceleration of Poverty Reduction (TNP2K) in the office of the Vice President of the Government of Indonesia. The pilot will facilitate the transfer of liquid propane gas (LPG) subsidies by delivering them to a biometrically validated digital wallet over a transparent and low cost blockchain. The goal of the pilot is to modernize delivery, reduce financial leakage, and enable banking services through financial inclusion. Addressing the current problems of delivery inefficiencies and lack of transparency will provide economically disadvantaged individuals greater access to energy subsidies.

3.2.10 Verifiable Credential and Decentralized Identifier Draft Standards

New approaches and technologies are emerging to use distributed ledgers (also known as ‘blockchains’) to establish identity networks that are not dependent on centralized data authorities. These identity networks are described in many different ways by different groups. Two core standards projects are central to these new developments: W3C Verifiable Credentials [6] and W3C Decentralized Identifiers [7]. This group of technologies and standards are still being developed and do not yet have wide adoption.

3.2.10.1 Verifiable Credentials

From the W3C Verifiable Credentials Data Model specification:

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies such as digital signatures makes verifiable credentials more tamper-evident and therefore more trustworthy than their physical counterparts. Holders can generate presentations and share them with verifiers to prove they possess verifiable credentials with certain characteristics. Both credentials and presentations can be rapidly transmitted, making them more convenient than their physical counterparts when establishing trust at a distance.

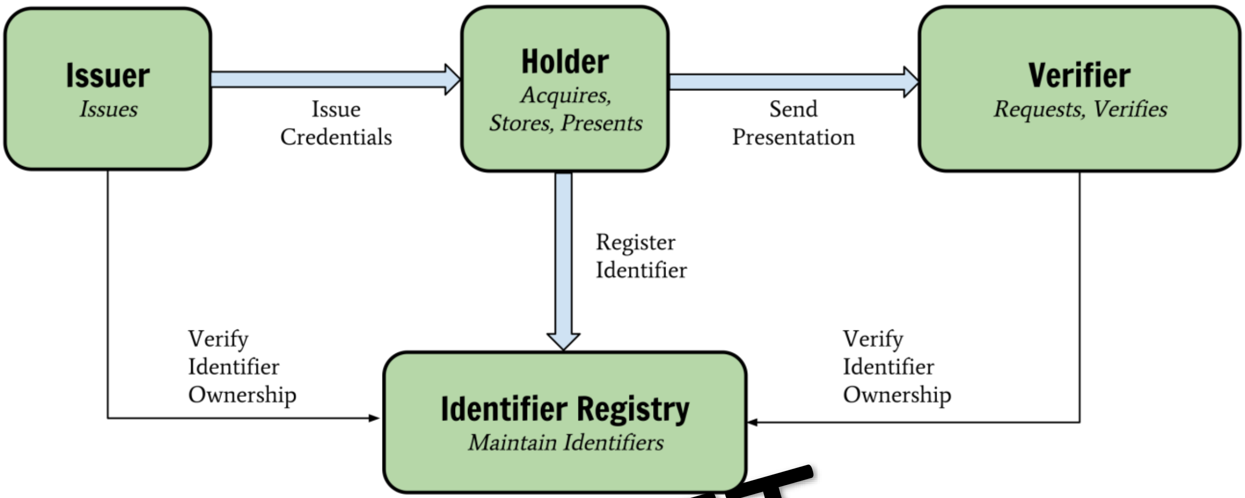

Figure 20: Roles and Relationships of Verifiable Credentials

The roles are described in the specification as:

Holder

A role an entity may perform by possessing one or more verifiable credentials and generating presentations from them. Examples of holders include students, employees, and customers.

Issuer

A role an entity may perform by creating a verifiable credential, associating it with a particular subject, and transmitting it to a holder. Examples of issuers include corporations, non-profits, trade associations, governments, and individuals.

Verifier

A role an entity may perform by requesting and receiving a verifiable presentation that proves the holder possesses the required verifiable credentials with certain characteristics. Examples of verifiers include employers, security personnel, and websites.

Identifier Registry

A role a system may perform by mediating the creation and verification of issuer identifiers, keys and other relevant data required to use verifiable credentials. Some configurations may require correlatable identifiers for subjects. Examples of such data repositories include trusted databases, decentralized databases, government ID databases, and distributed ledgers.

Verifiable credentials are a central feature in section 4.1.3 Example 3: Zug eID – Ethereum Blockchain-based Digital ID.

3.2.10.2 Decentralized Identifiers

The Decentralized Identifier specifications are being created to establish a globally-addressable identifier namespace for distributed ledger and blockchain systems. Decentralized Identifiers are the addressing scheme used for Verifiable Credentials.

From the W3C Decentralized Identifier draft specification:

> The emergence of distributed ledger technology (DLT), sometimes referred to as blockchain technology, provides the opportunity for fully decentralized identity management. In a decentralized identity system, entities are free to use any shared root of trust. Globally distributed ledgers (or a decentralized P2P network that provides similar capabilities) provide a means for managing a root of trust with neither centralized authority nor a single point of failure. In combination, DLTs and decentralized identity systems enable any entity to create and manage their own identifiers on any number of distributed, independent roots of trust.
>
> The entities are identified by decentralized identifiers (DIDs). They may authenticate via proofs (e.g., digital signatures, privacy-preserving biometric protocols, etc.). DIDs point to DID Documents. A DID Document contains a set of service endpoints for interacting with the entity. Following the dictums of Privacy by Design, each entity may have as many DIDs as necessary, to respect the entity's desired separation of identities, personas, and contexts.
>
> To use a DID with a particular distributed ledger or network requires defining a DID method in a separate DID method specification. A DID method specifies the set of rules for how a DID is registered, resolved, updated, and revoked on that specific ledger or network.
>
> This design eliminates dependence on centralized registries for identifiers as well as centralized certificate authorities for key management—the standard pattern in hierarchical PKI (public key infrastructure). Because DIDs reside on a distributed ledger, each entity may serve as its own root authority—an architecture referred to as DPKI (decentralized PKI).

Decentralized Identifiers are implemented in the uPort Ethereum Blockchain-based Digital ID system.

4 Implementation examples of Strong Authentication Systems

This section contains examples of strong authentication systems that cover DFS use cases. The examples also illustrate mechanisms related to the authentication assurance phases of ITU-T Recommendation X.1254.

Authentication Assurance Phase	**DFS Use Cases**	**Use case examples**
Enrolment	Account opening (Section 4.1): ▪ eKYC	▪ Aadhaar eKYC (Section 4.1.1) ▪ K-FIDO Enrolment (Section 4.1.2) ▪ Zug eID (Section 4.1.3) ▪ FIDO Enrolment (Section 4.1.4) ▪ Healthcare provider user enrolment (Section 4.1.5)

Authentication	Access a Digital Financial Service (Section 4.2): ▪ Storing Funds ▪ Buying ▪ Paying Bills ▪ Sending/receiving funds ▪ Borrowing ▪ Saving ▪ Insuring Assets and Risks	▪ Alipay fingerprint payment (Section 4.2.1) ▪ Aadhaar authentication (Section 4.2.2) ▪ Aadhaar Unified Payments Interface (Section 4.2.3) ▪ K-FIDO Authentication (Section 4.2.4) ▪ Healthcare provider Next-Generation Authentication (Section 4.2.5) ▪ SK Telecom - Mobile Connect Authentication (Section 4.2.6)

Table 3: Digital Financial Services Use Case Examples

4.1 Use case: Enrolment and Account opening

The examples presented for the Enrolment use case describe how previously-established identity information can be used to create new service accounts and to satisfy KYC requirements. The key aspect in the examples is that the person has been enrolled previously with an authority: their identity information collected, verified and stored. This stored identity information is then available for later presentation to service providers, controlled by the person's authentication to release that identity information.

Use of digital sources of identity information for not-in-person KYC and account opening is both convenient for the person but also presents risks for impersonation. Therefore, use of using strong authentication mechanisms is recommended.

4.1.1 Example 1: Aadhaar eKYC

eKYC service allows resident to authorize Unique Identification Authority of India (UIDAI) to share electronic version of Aadhaar information (demographic information and photo ONLY) with the explicit authentication of the resident. In eKYC service, UIDAI encrypts the eKYC response data containing resident's latest demographic and photograph information using KUA public key and subsequently forwards the encrypted response to KUA. On receiving the encrypted response, the KUA decrypts the data using their own private key and returns an XML with 7 pieces of data - Name, Address, DOB, Gender, Phone#, Email Address & photograph, this eliminates collecting photocopy of Aadhaar letter from resident.

Benefits of Aadhaar-based eKYC process:

eKYC has facilitated the telecom operators immensely on account of paperless acquisition of subscribers, and thus substantially enhanced the Ease of Doing Business. Some of the benefits are described below:

- Activation – there is no requirement for filling up of CAF and submission of photograph along with POI and POA documents.
- Secure process - customer's data is fetched from central UIDAI server in encrypted format and not stored on any of the POS terminals except for the company's server.

- No document copy or photograph is required – this gives additional confidence to the customers as they don't need to submit any documents which can be later misused by the retailers for pecuniary gains.
- Extremely quick activation – as against the traditional process for activation of SIM card which could take between 12-24 hours, the SIM card is activated in very short time once the form gets submitted from the POS terminal to the company's back office. This scores very high on customer satisfaction.
- Apart from the above benefits, this process also helps TSPs do away with archaic processes of CAF collection, data entry, document scanning, tele-verification and physical storage and retrieval of CAFs and documents from the warehouse. As an outcome of this, TSPs are able to store the KYC information of their customers in an electronic format which can be retrieved very quickly being an electronic record.
- The process also benefits the government authorities be it the TERM Cells for audits and the law enforcement agencies (LEAs) as this is a highly compliant process and will significantly help in traceability of the customer should there be need for any law enforcement requirement.

4.1.2 Example 2: K-FIDO Enrolment example

This section describes how "K-FIDO" combines FIDO UAF specification and PKI to enable authentication and ID verification at the same time for successful commercial Fintech deployments in Korea. K-FIDO is a specification to be published by KISA (Korea Internet Security Agency), enabling biometric accredited certification services that provide accredited certificates without password using FIDO in Korea.

Korean National ID is used in offline identification and contains a unique Resident Registration Number. To facilitate private and secure online identification and authentication, an i-PIN backed by a PKI certificate issued by a small number of service providers can be generated and associated with the Resident Registration Number. Figure 21 illustrates this relationship.

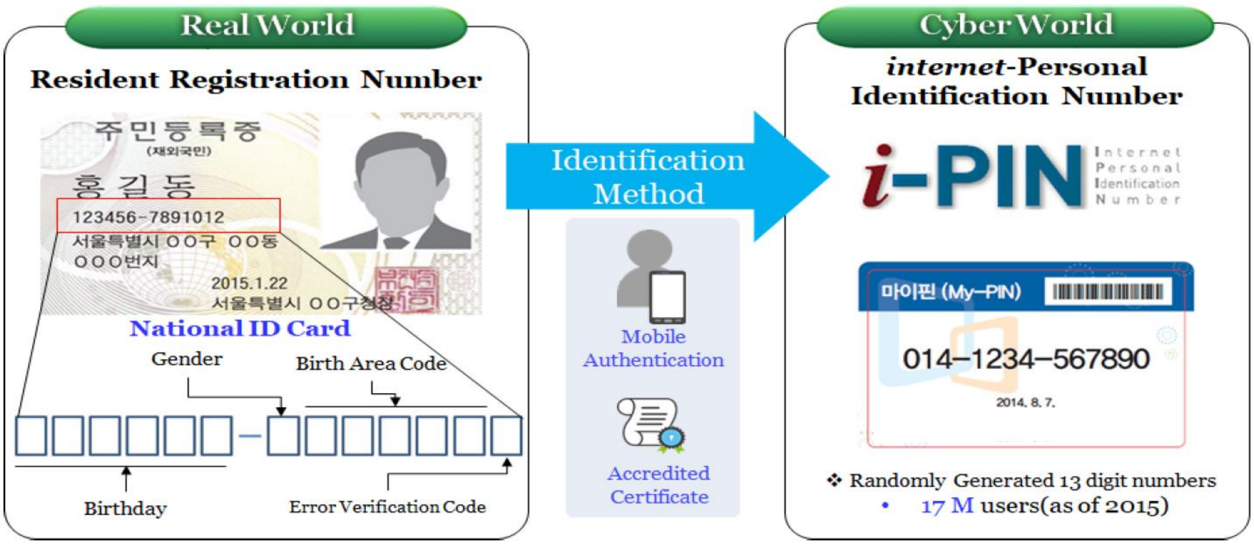

Figure 21: National ID and i-PIN in Korea

The citizen can use many identification methods such as accredited certificates, mobile, bank accounts, and credit cards for internet services that request an online (i.e. non face-to-face) identification method.

Online service providers can choose Identification methods such as Accredited Certificates, Mobile Authentication, i-PIN, K-FIDO, or FIDO depending on the required authentication levels of assurance.

The citizen must register in order to connect their PKI certificate and i-PIN to their FIDO-enabled mobile device. Once registered, the citizen identity data can be provided to other service providers after a strong FIDO authentication.

Figure 22 illustrates the registration process.

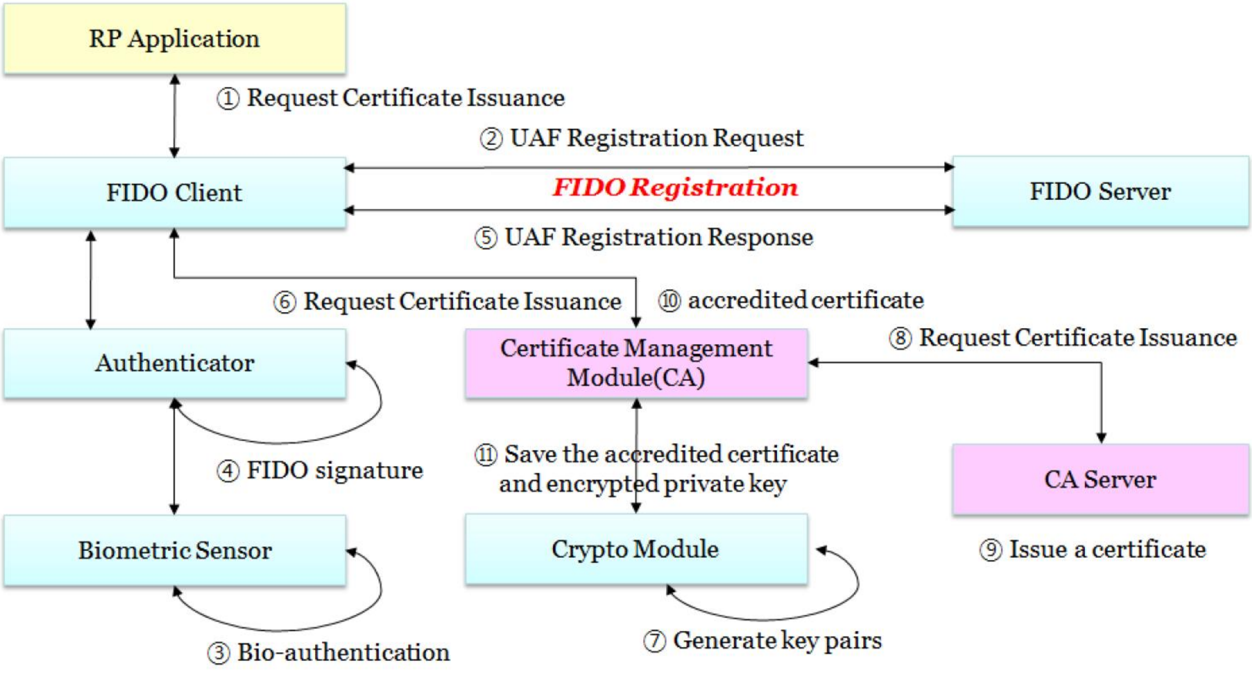

Figure 22: Registration process of K-FIDO service

① RP App starts bio-registration and requests a user certificate issuance.

② The FIDO server triggers a UAF registration request to the FIDO client.

③ The user performs a bio-authentication with FIDO authenticators using their respective user verification method, e.g. fingerprint, iris, etc.

④ The selected FIDO authenticator generates the FIDO authentication private key. The selected FIDO authenticator generates a FIDO signature using the attestation private key.

⑤ The FIDO server verifies the signature using the attestation public and verifies the authentication public key. If verified, the FIDO server trusts the authenticator it is talking to and the authentication public key that was sent from the authenticator in the authentication response. The FIDO server checks FIDO registration message and if passed, the FIDO server stores the authentication public key.

⑥ The FIDO client requests the user certificate issuance to the certificate management module.

⑦ The crypto module generates a private and public key pair for the user certificate.

⑧ The certificate management module requests the user certificate issuance from the certification authority.

⑨ The certificate management module stores the user certificate and the private key in the secure element such as USIM, Trustzone, etc. However, the private key should be encrypted by an encryption key in keystore or keychain. The registration process is completed.

Notes on user's identity:

- Before step six happens where the FIDO client requests the user certificate issuance, the user is assumed to have finished user identification using such a mechanism like mobile authentication, accredited certificate, bank account authentication, etc. Thus, the user identity is known at the sixth step.
- The user uses FIDO authentication after the user has finished identification, while it is not tightly coupled. The general scenarios are as follows;

  1) A user performs user's identification defined by a service provider.

  2) A user uses FIDO or K-FIDO service (the scope of K-FIDO).
- Authenticators decide where the user certificates are stored. KISA recommends secure elements such as keyStore, keyChain, USIM, or Trustzone, etc.

4.1.3 Example 3: Zug eID – Ethereum Blockchain-based Digital ID

Since November 2017 the Swiss City of Zug has been offering blockchain-based digital IDs to all of its 30,000 citizens. [8]

The Zug eID consists of three parts. First is the digital vault, which is part of the mobile app. This contains the actual digital ID, which is encrypted; it can be unlocked by the owner biometrically or using a PIN code. Second is the Ethereum blockchain where the app creates a unique cryptographic address for its holder. Third is the certification portal used by the officials who check that the applicant is a resident of Zug.

After the applicant's name, address, date of birth, nationality, and passport number or ID card number have been verified, this data is digitally signed by the City of Zug, and the signature is stored as a certificate in the citizen's digital vault. Since the City's public key is publicly available from the Ethereum blockchain, anyone who receives an eID from its holder can readily verify its authenticity.

After a successful residency check, the City of Zug — itself a digital identity on the blockchain, albeit with special privileges — signs the identity contract of the user, for anyone to see and verify on the Internet. The owner of this special identity is the Zug city clerk.

From that moment on, the owner of the eID can use the mobile app to provide identity information. The authenticity of this data can be validated by checking its digital signature on the blockchain.

In the second quarter of 2018 Zug planned to organise a consultation on a specific topic for existing eID holders. Its primary goal was to collect ideas for e-voting based on the new eID.

4.1.4 Example 4: FIDO Enrolment example

In contrast to the previous examples, the FIDO specifications have made an explicit and conscientious decision to separate "identity proofing" from "enrolment". This allows for a more modular architecture where any identity proofing technique can be combined with FIDO enrolment, including Alipay, Aadhaar eKYC, existing PKI credentials (such as K-FIDO above), various NIST / FIPS LOAs, etc.

A preferential architecture with FIDO is that strong identity proofing is performed once, and then identity is bound to cryptographically and physically secure credentials.

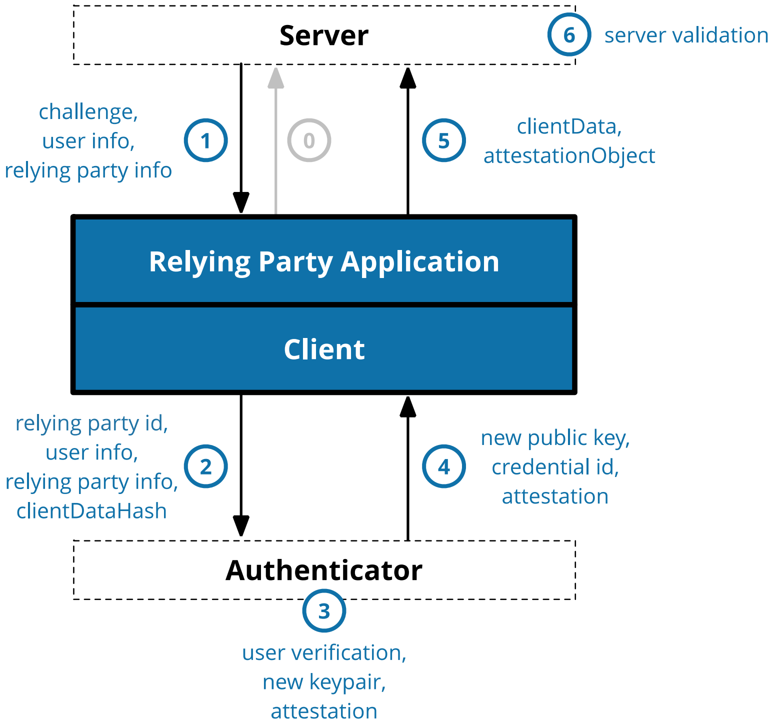

Figure 23: Registration process of FIDO

The enrolment steps are:

0. **Application Requests Registration** - The application makes the initial registration request after completing identity proofing / KYC and within the same session or trusted environment.
1. **Server Sends Challenge, User Info, and Relying Party Info** - The server sends a challenge, user information, and relying party information to the Relying Party Application. The Relying Party Application can be a mobile, web, native, or other application and its implementation is outside of the scope of the FIDO specifications. The protocol for communicating with the server is not specified and is also outside of the scope of FIDO. Typically, server communications would be REST over TLS, but they could also be SOAP, RFC 2549 or nearly any other protocol provided that the communication channel is secure. The parameters received from the server will be passed to the client to create credentials, typically with little or no modification.
2. **Client Calls authenticatorMakeCredential on Authenticator via CTAP** - Internally, the client will validate the parameters and fill in any defaults, which become the clientData. One of the most important parameters is the origin, which is recorded as part of the clientData so that the origin can be verified by the server later. The parameters to the credentialCreate call are passed to the authenticator, along with a SHA-256 hash of the clientData (only a hash is sent because the link to the authenticator may be a low-bandwidth NFC or Bluetooth link and the authenticator is just going to sign over the hash to ensure that it isn't tampered with).
3. **Authenticator Creates New Key Pair and Attestation** - Before doing anything, the authenticator will typically ask for some form of user verification. This could be entering a PIN, using a fingerprint, doing an iris scan, etc. to prove that the user is present and consenting to the registration. After the user verification, the authenticator will create a new

asymmetric key pair and safely store the private key for future reference. The public key will become part of the attestation, which the authenticator will sign over with a private key that was burned into the authenticator during its manufacturing process and that has a certificate chain that can be validated back to a root of trust.

4. **Authenticator Returns Data to Client** - The new public key, a globally unique credential id, and other attestation data are returned to the client where they become the attestationObject.

5. **Client Creates Final Data, Application sends response to Server** – The authenticatorMakeCredential call returns a PublicKeyCredential, which has a rawId that is the globally unique credential id along with a response that is the authenticator's attestation response containing the clientData and the attestationObject. The PublicKeyCredential is sent back to the server using any desired formatting and protocol.

6. **Server Validates and Finalizes Registration** - Finally, the server is required to perform a series of checks to ensure that the registration was complete and not tampered with. These include:

   - Verifying that the challenge is the same as the challenge that was sent
   - Ensuring that the origin was the origin expected
   - Validating that the signature over the clientDataHash and the attestation using the certificate chain for that specific model of the authenticator

A complete list of validation steps can be found in the WebAuthn specification [5]. Assuming that the checks pan out, the server will store the new public key associated with the user's account for future use -- that is, whenever the user desires to use the public key for authentication.

4.1.5 Example 5: Healthcare provider user enrolment

A healthcare provider's online enrolment processes attempt to help onboard a new member using customer attribute information and determine if the attributes presented during enrolment are usable. The strategic goal is to improve the user experience and better identify a member at enrolment time in combination with other internal authentication processes.

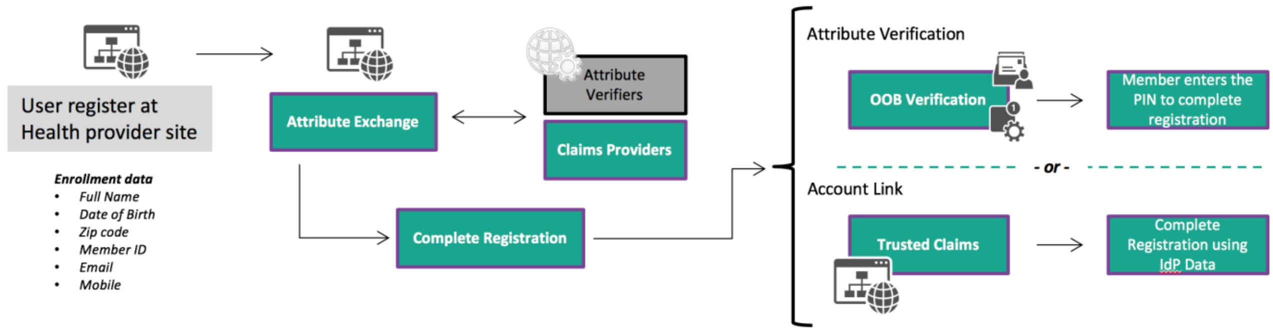

Figure 24: Healthcare provider user enrolment

Option 1: Federated Account Linking

During online enrolment, member is allowed to select an option to perform identity verification via a trusted Identity Provider (e.g. a bank).

Member is redirected to bank (IdP or Attribute Provider)) via federation standards. Member authenticates to the IdP. Healthcare provider obtains user information from IdP to compare to initially collected user data.

Member is allowed to complete enrolment with the healthcare provider.

Option 2: Attribute Verification

Instead of the IdP providing attributes to the healthcare provider for consumption and evaluation after authenticating the user, the healthcare provider sends attributes collected in enrolment to the IdP (with user consent).

IdP evaluates, and provides a response indicating the quality or accuracy of the attributes collected during enrolment. The healthcare provider completes member enrolment using OOB verification techniques.

4.2 Use case: Authentication to access a digital financial service

The examples for the Entity authentication use case describe how next generation authentication mechanisms are used to authenticate an individual for authorization to consume services.

4.2.1 Example 1: IFAA use case – Alipay fingerprint/face payment

Alipay is the most popular mobile payment application in China. It supports fingerprint or face authentication when a user wants to transfer money through mobile devices. The Alipay payment authentication process adopts the local model of IFAA and is based on the IFAA authentication protocol as illustrated in Figure 16. Figure 25 is the snapshot from Alipay.

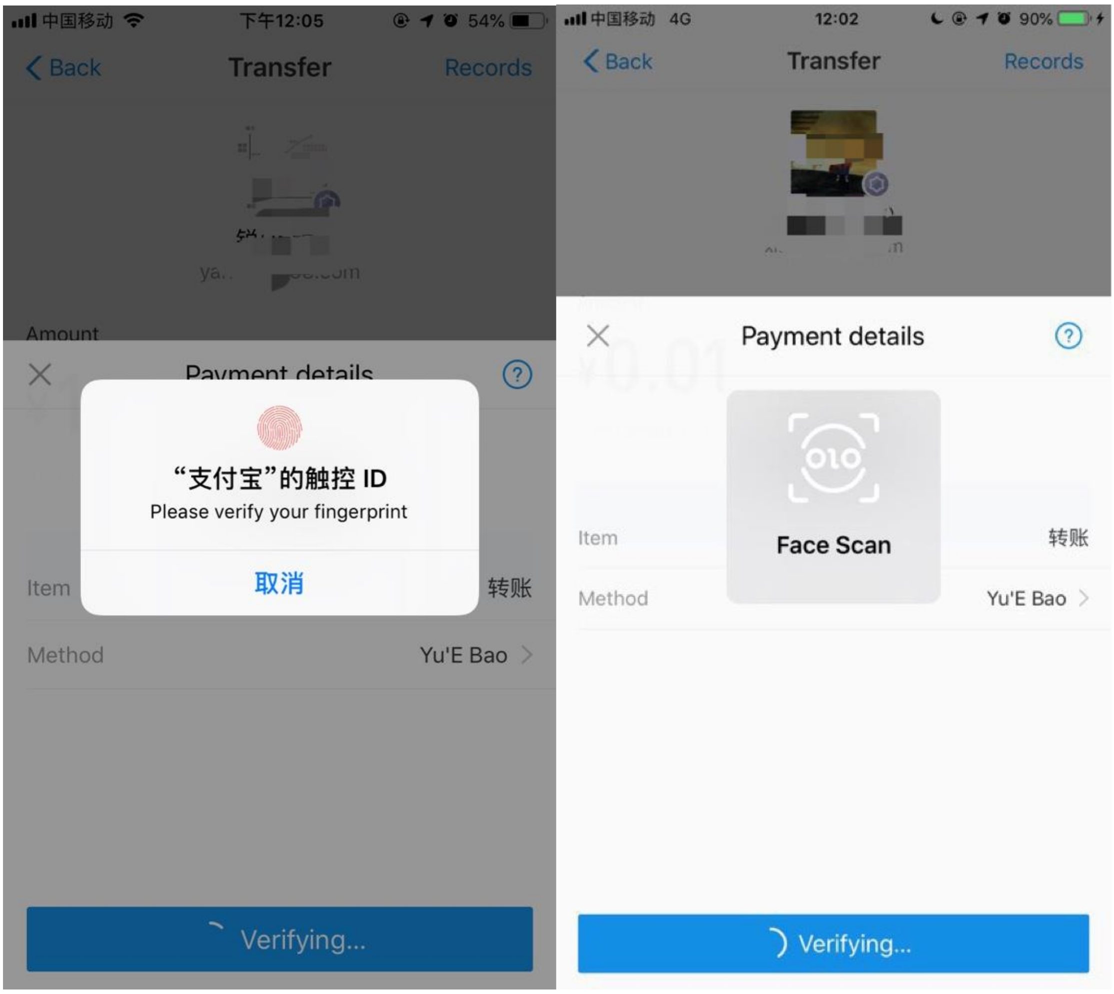

Figure 25: IFAA use case – Alipay fingerprint/face payment

Figure 26 is the technical framework of Alipay payment authentication system.

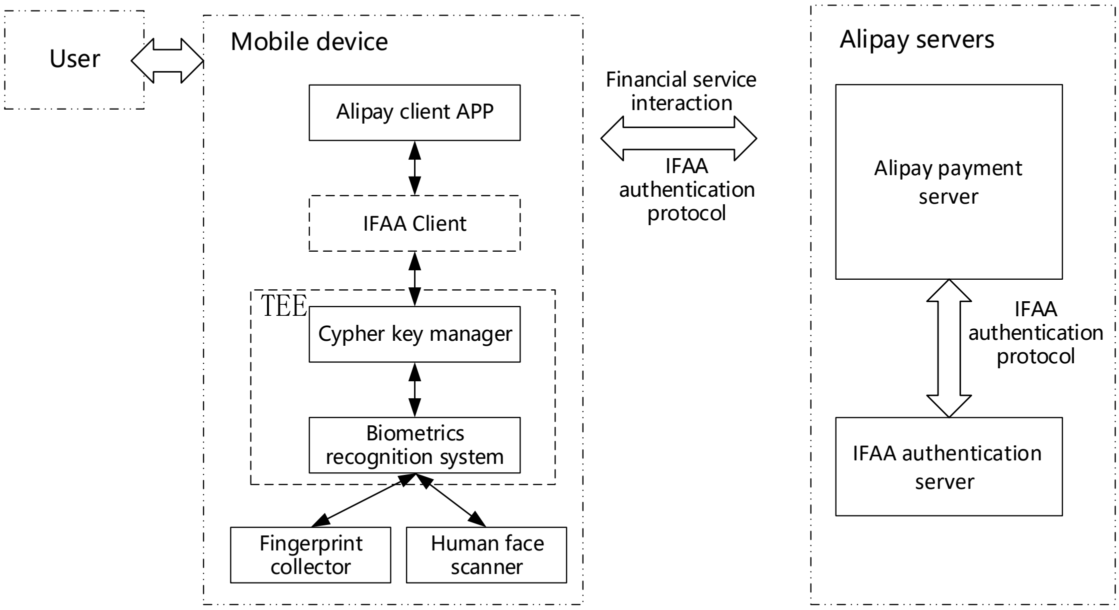

Figure 26: IFAA use case – Alipay fingerprint/face payment – Technical framework

The Alipay user first initiates the registration request through the Alipay client app and runs the registration process as in Figure 15. After a successful registration, the user can initiate a payment request through the Alipay client app.

To begin a payment process, the Alipay client app first interacts with the Alipay payment server to confirm whether mobile payment can be carried out. If yes, the Alipay client app calls the key manager (or optionally, the IFAA client) to authenticate the user as in the following:

1) Require the user to perform fingerprint/face authentication based on the local fingerprint/face template.
2) After fingerprint/face verification, the key manager invokes the local stored user authentication private key to sign the transaction information, and sends it to the Alipay payment server through the Alipay client app.
3) Alipay payment server sends the authentication information to the IFAA authentication server for verification and retrieves the verification results.
4) Alipay payment server authorizes the payment after successful verification.

4.2.2 Example 2: Aadhaar authentication

Aadhaar authentication is the process wherein the Aadhaar Number, along with other attributes, including biometrics, are submitted online to the Central Identities Data Repository (CIDR) for its verification on the basis of information or data or documents available with it. During the authentication transaction, the resident's record is first selected using the Aadhaar Number and then the demographic/biometric inputs are matched with the stored data which was provided by the resident during enrolment/update process. Alternatively, authentication can also be carried out on the basis of the OTP. All biometric/OTP authentication schemes are valid for e-KYC service too.

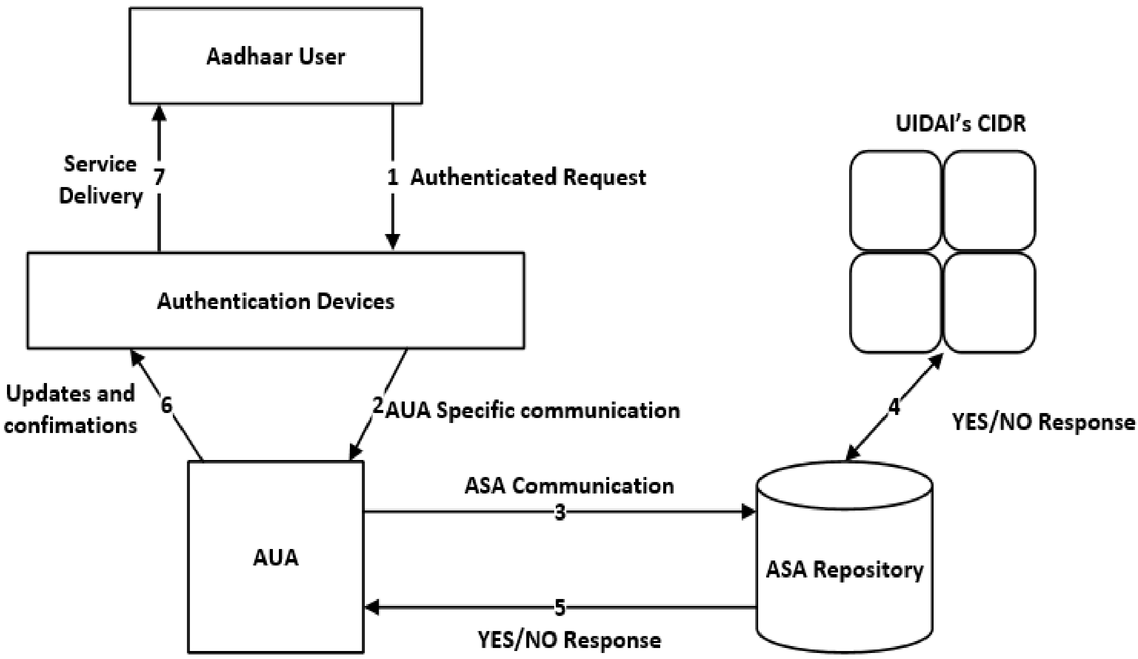

Figure 27: Technical process of Authentication & e-KYC services

The following are the major steps in the Aadhaar authentication process as shown in Figure 27 above:

- Aadhaar holder sends the authentication request through the devices
- Aadhaar authentication enabled application software which is installed on the device, encrypts and sends the data to AUA server
- AUA server, after validation, adds necessary headers (AUA specific wrapper XML with license key, signature, etc.), and passes the request through ASA server to UIDAI CIDR.
- Aadhaar authentication server returns a "yes/no" based on the match of the input parameters.
- Based on the response from the Aadhaar authentication server, AUA/Sub-AUA conducts the transaction and Aadhaar holder receives the service.

Additional Security features for Authentication/KYC service:

- To further enhance the security of Aadhaar authentication eco-system, under Regulations 14(n) and 19(o) of Aadhaar (Authentication) Regulations, 2016, it is mandatory to use Hardware Security Module (HSM) for digital signing of Authorised XML and decryption of e-KYC data.
- For digital signing of Authorised XML, Authentication request is digitally signed by the requesting entity (AUA/ KUA) and/or by the ASA using HSM, as per the mutual agreement between them. However, to decrypt the e-KYC response data received from UIDAI, the KUA shall necessarily use its own HSM.
- The HSM to be used for signing Auth XML as well as for e-KYC decryption is FIPS 140-2 compliant.
- All AUA/ KUA/ASA ensure the implementation of HSM in Aadhaar authentication services.

- To eliminate the use of stored biometrics, UIDAI has mandated the use of registered devices by AUA/KUAs and ASAs. The registered devices provide the following key additional features compared to public devices:
    - Device identification – every device is required to have a unique identifier allowing traceability, analytics, and fraud management.
    - Eliminating use of stored biometrics – biometric data is signed within the device using the provider key to ensure it is indeed captured live. Then the Registered Device (RD) Service of the device provider must form the encrypted PID block before returning to the host application.

4.2.3 Example 3: Aadhaar Unified Payments Interface

It is an instant payments system developed by the National Payments Corporation of India (NPCI) and allows consumers to make bank account-to-account transfers instantly with a single identifier 'Virtual Payment Address (VPA)' i.e. without any additional bank account information like Account Number, IFSC code etc. For using UPI, users need to create a Virtual Payment Address (VPA) of their choice and link it to any bank account. The VPA acts as their financial address for sending or receiving money. UPI can be used for Peer-Peer, Peer-Merchant & Business-Business payment transactions. UPI system provides an ecosystem driven scalable architecture and a set of APIs taking full advantage of mass adoption of smartphone.

Features of UPI:

- Simplicity - Paying and receiving payments is as easy as swiping a phone book entry and making a call on mobile phone. Everyone who has an account is able to send and receive money from their mobile phone with just an identifier without having any other bank/account details. All we need to do is to "pay to" or "collect from" a "payment address" (such as Aadhaar number, Mobile number, RuPay Card, virtual payment address, etc.) with a single click.
- Adoption – the solution is scalable to a billion users and large-scale adoption as it allows adoption across smartphone and feature phone users and provides full interoperability across all payment players, phones, and use cases. People using smartphone should be able to send money to others who are not yet using any mobile application and vice versa. Similarly, it is fully interoperability between multiple identifiers such as Aadhaar number, mobile number, and new virtual payment addresses.
- Security - It provides end to end strong security and data protection. Considering self-service mobile applications, data capture must be strongly encrypted at capture. Similarly, solution allows a mechanism to pay and collect using true virtual addresses without having to reveal any bank/account details. While providing convenient, solution offer 1-click 2-factor authentication, protection from phishing, risk scoring, etc.

4.2.4 Example 4: K-FIDO authentication

Various user authentication methods used for user authentication for web portals, e-transactions, financial institutions and e-government services are typically supported. Figure 28 illustrates K-FIDO authentication.

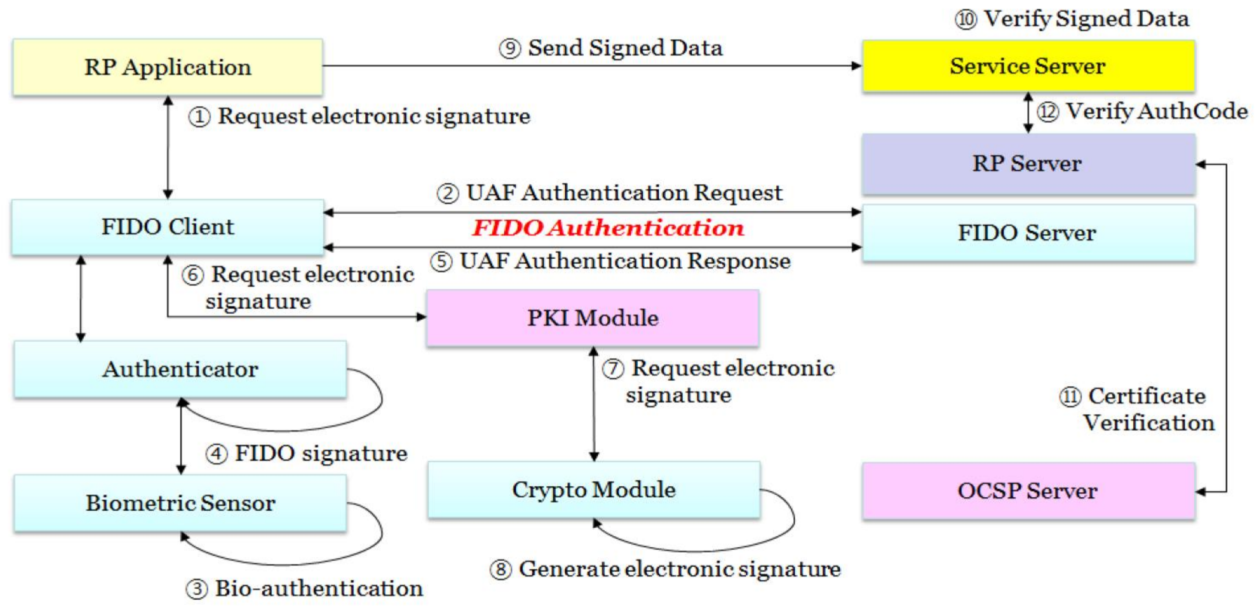

Figure 28: Authentication Process of K-FIDO Service

① RP App performs bio-authentication and requests electronic signature for a service provider.

② FIDO server triggers UAF authentication request to FIDO client.

③ A User performs a bio-authentication by the FIDO authenticator using the same method as at Registration time.

④ The FIDO authenticator generates FIDO signature (using the FIDO authentication private key).

⑤ The FIDO client sends UAF authentication response to FIDO server. The FIDO server checks FIDO authentication message and if passed, the RP server generates an Authcode.

⑥ The FIDO client requests electronic signature generation to PKI module.

⑦ The PKI module requests electronic signature generation to Crypto module.

⑧ In case of secure element such as Trustzone, or USIM, the electronic signature will be generated by the private key inside the secure element. However, in case of keystore or keychain, the encrypted private key should be decrypted by a decryption key stored in keystore or keychain and electronic signature will be generated by the private key with crypto module.

⑨ RP App sends the signed data to Service server.

⑩ Service server verifies the signed data.

⑪ Service server or RP Server checks user certificate’s verification from OCSP server.

⑫ Service server checks the Authcode from FIDO service provider. And Service server sends the result to the user.

4.2.5 Example 5: Healthcare provider customer authentication

A large healthcare provider is now in a multi-year process of rolling out its next-generation authentication (NGA) platform across mobile and web applications. With NGA, the healthcare provider is forging new industry best practices for improving healthcare access through a two-pronged approach to strong authentication. First, they have adopted passwordless FIDO Authentication with biometrics for their customers' online account credentials, reducing their reliance on highly vulnerable "shared secrets," like passwords and one-time-passcodes with strong, unphishable, public key cryptography.

While deploying standards-based strong authentication like FIDO helps resolve many of the authentication problems organizations have faced around security and user experience, healthcare providers still have to contend with risks associated with lost and stolen devices. Thus, the healthcare provider is rolling out the second core component of the NGA platform — continuous, behavior-based authentication — to ensure that the authenticated user is the same person throughout the lifetime of the session. To do this, the healthcare provider looks at several user attributes (such as the way they hold their phone) and assigns risk scores to determine how much access to give a user during a session. If high risk is detected during a session, the healthcare provider may challenge the user for additional information before allowing continued access from that device.

4.2.6 Example 6: SK Telecom – Mobile Connect

SK Telecom (SKT) is the largest mobile operator in South Korea serving 28 million of the country's 57 million subscribers. SK Telecom has been a pioneer in harnessing the potential of identity services. As early as 2005, it started offering T-Auth, its own mobile identity solution supporting a combination of mobile authentication and attribute matching.

SKT saw an opportunity in Korea's regulations, which require content providers to actively ensure that their customers are authorised to access particular content. Effectively, this means that content providers are responsible for checking that customers wishing to purchase content are over the legal age. SKT realised that its customer account information could help service providers meet this requirement. It designed T-Auth to address this use case with minimal impact on the user experience.

SKT has designed the user journey to minimize user friction during authentication. Figure 29 shows a typical authentication flow: the customer attempts to access a service provider application and is redirected to the T-Auth mobile app for authentication; the customer enters their PIN and biometric sample; on successful authentication T-Auth sends the authentication result and attribute data to the service provider.

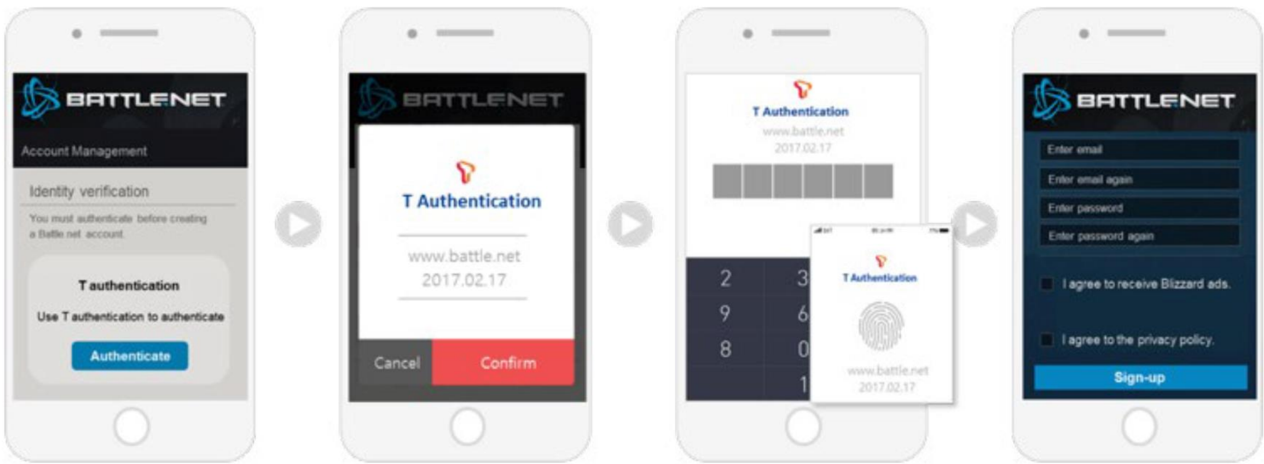

Figure 29: Simplified User Journey to Authenticate to a Gaming Account Using T-Auth

In early 2017, SKT became compliant with Mobile Connect, the global mobile operator authentication, authorisation and identity framework. As a result, T-Auth is now interoperable with other mobile authentication and identity solutions provided by operators outside of Korea.

4.2.7 Example 7: FIDO Authentication

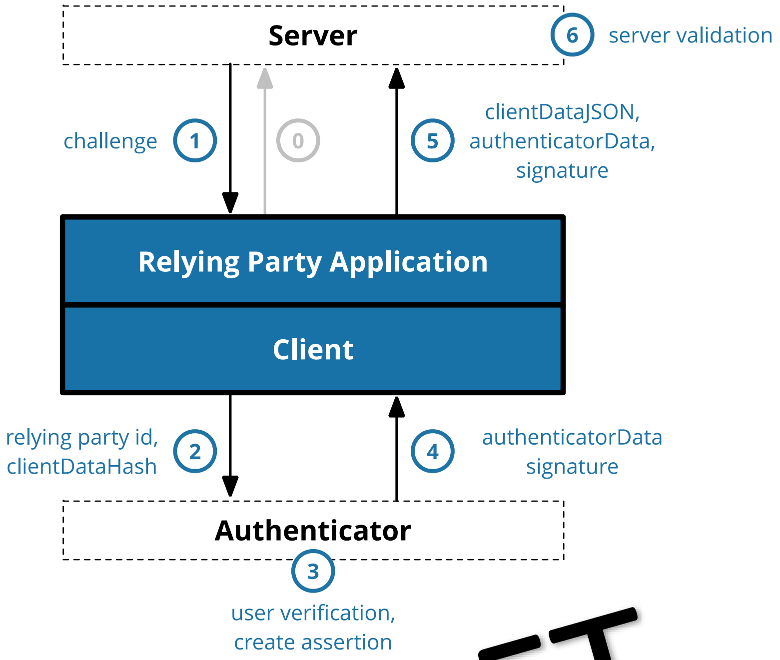

Figure 30: Authentication process of FIDO

0. **Application Requests Authentication** - The application makes the initial authentication request. The protocol and format of this request is outside of the scope of FIDO.
1. **Server Sends Challenge** - The server sends a challenge to the application. The protocol for communicating with the server is not specified and is outside of the scope of FIDO. Typically, server communications would be REST over TLS, but they could also be SOAP, RFC 2549 or nearly any other protocol provided that the protocol is secure. The parameters received from the server will be passed to the credentialGet call, typically with little or no modification.
2. **Client Calls authenticatorGetCredential on Authenticator via CTAP** - Internally, the client will validate the parameters and fill in any defaults, which become the clientData. One of the most important parameters is the Relying Party ID, which recorded as part of the clientData so that the Relying Party ID can be verified by the server later. The parameters to the credentialGet call are passed to the authenticator, along with a SHA-256 hash of the clientData (only a hash is sent because the link to the authenticator may be a low-bandwidth NFC or Bluetooth link and the authenticator is just going to sign over the hash to ensure that it isn't tampered with).
3. **Authenticator Creates an Assertion** - The authenticator finds a credential for this service that matches the Relying Party ID and prompts a user to consent to the authentication. Assuming both of those steps are successful, the authenticator will create a new assertion by signing over the clientDataHash and authenticatorData with the private key generated for this account during the registration call.

4. **Authenticator Returns Data to Client** - The authenticator returns the authenticatorData and assertion signature back to the client.
5. **Client Creates Final Data, Application sends response to Server** - The authenticatorGetCredential call returns a PublicKeyCredential with the authenticator's assertion response. It is up to the application to transmit this data back to the server using any protocol and format of its choice.
6. **Server Validates and Finalizes Authentication** - Upon receiving the result of the authentication request, the server performs validation of the response such as:
    1. Using the public key that was stored during the registration request to validate the signature by the authenticator.
    2. Ensuring that the challenge that was signed by the authenticator matches the challenge that was generated by the server.
    3. Checking that the Relying Party ID is the one expected for this service.

A full list of the steps for validating an assertion can be found in the WebAuthn specification [5]. Assuming the validation is successful, the server will note that the user is now authenticated (e.g. – set a flag for the session, set a cookie, etc.).

5 Design Considerations for Use of Biometrics in Authentication

Biometrics are typically used in one of two modes for authentication purposes: identification and verification. Identification is the process of comparing the individual's biometric data to all samples in the database, to determine which individual is present. Verification is the process of checking that the biometric data of the claimed identity is the same as the biometric data presented by the individual.

Note: the text below is from World Bank. 2018. Technology Landscape for Digital Identification [9]

In determining which modalities to incorporate in a biometric-recognition system, decision makers must consider the following criteria:

- Accuracy: false acceptance rate (FAR) and false rejection rate (FRR) under operational conditions
- Universality: presence of the trait in members of the relevant population—important because certain traits (like fingerprints) may be poor or damaged in certain demographics and can lead to a failure to enroll (FTE) the individual
- Stability: permanence of the trait over time or after disease or injury
- Collectability: ease with which good quality samples can be acquired
- Resistance to circumvention: vulnerability of the modality to fraud
- Acceptability: degree of public openness for use of the modality
- Usability: ease with which individuals can interact with the technology used to capture the biometric data
- Cost: costs of sample collection and matching; namely, hardware, and software costs

According to Yanushkevich [10], leading biometric technologies include:

- Facial recognition attempts to identify a subject based on facial characteristics (eye socket position, space between cheekbones, etc.).

- Fingerprint recognition systems rely on the biometric device's ability to distinguish the impressions of ridges and valleys made by an individual's finger.
- Hand geometry solutions take more than 90 dimensional measurements to record an accurate spatial representation of an individual's hand. The geometry of the hand is not known to be very distinctive and may not be invariant during the growth period of children. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops.
- Palmprint recognition is based on the palms of the human hands that contain pattern of ridges and valleys (like the fingerprints) and additional distinctive features such as principal lines and wrinkles. When using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles may be combined to build a highly accurate biometric system.
- Iris scanning/recognition uses a camera mounted between three and 10 feet away from the person to take a high definition photograph of the individual's eyes. It then analyses of two-three hundreds different points of data from the trabecular meshwork of the iris.
- Retina scanning/recognition involves an electronic scan of the retina, the innermost layer of the wall of the eyeball.
- Signature dynamics/recognition not only compares the signature itself, but also marks changes in speed, pressure and timing that occur during signing.
- Keystroke dynamic techniques measure dwell time (the length of time a person holds down each key) as well as flight time (the time it takes to move between keys). Taken over the course of several login sessions, these two metrics produce a measurement of rhythm to each user.

- Voice/speaker recognition techniques digitize a profile of a person's speech into a template voiceprint and stores it as a table of binary numbers. During authentication, the spoken passphrase is compared to the previously stored template.
- Gait recognition is defined as the identification of a person through the pattern produced by walking. Gait has particular advantages over other biometrics: it can be used at a distance, uses no additional skills on the part of the subject, and may be performed without the subject's awareness or active participation. Gait is not supposed to be very distinctive but is sufficiently discriminatory to allow verification in some low-security applications.
- Ear recognition attempts to identify a subject based on the shape of the ear and the structure of the cartilaginous tissue of the pinna. Ears are characterized by a stable structure that is preserved from birth well into old age. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

6 Guidance for Regulators

This report provides examples of strong authentication systems that have been implemented using a range of standards and technologies. Regulators and policymakers have a role to play in ensuring DFS providers use appropriate, strong authentication methods. The Chertoff Group report "Strong Authentication in Cyberspace" [11] includes guidance for policymakers, in particular, to encourage movement away from password-based authentication:

1. Require strong forms of authentication.

- Passwords are difficult for people to use and are inherently weak. Ensure that strong forms of authentication are considered when analyzing risk in DFS.

2. Recognize the security limitations of shared secrets.

- Recognize that previous generation authentication technologies that rely on shared secrets or passwords have inherent security weaknesses.

3. To gain widespread adoption, authentication must be easy to use.

- Poor user experience dissuades people from using systems. Newer strong authentication approaches and technologies avoid disruption of user flow while increasing authentication strength.

4. Understand that the old barriers to strong authentication no longer apply.

- Strong authentication products have evolved to remove barriers present in previous-generation technologies. The strong authentication system technologies described in this paper demonstrate that shifting reliance from a person's memory to secure hardware components is possible and can be cost effective.

5. Authentication solutions must support mobile.

- Mobile has become a significant web access mode and is accelerating. Newer strong authentication approaches are taking advantage of properties inherent in mobile devices and built-in high security technologies.

6. Privacy matters.

- Ensure that strong authentication technologies are not designed to use user surveillance techniques in the guise of stronger security. Strong authentication approaches can be designed with privacy in mind and avoid unnecessary transmission and aggregation of personal information.

7. Biometrics are making authentication easier – but must be applied appropriately.

- Biometric sensors are becoming ubiquitous in consumer-grade devices. This offers new possibilities for authentication systems. However, biometric approaches do not work for all people and, if designed badly, can actually decrease overall system security. For example, if biometrics are used as a combination of user identification and authentication method, compromise of the biometric sample could lead to total compromise of that person's accounts. If used, biometrics should be used as only one element in a strong authentication system, preferably as an on-device unlock mechanism.

8. Don't prescribe any single technology or solution – focus on standards and outcomes.

- Technology changes and evolves continually. Even systems and technologies that are ubiquitous today may fall out of favour at any time. By focusing on use of standards and outcomes, regulators can avoid steering DFS providers into technology dead-ends.

7 Standardization Objectives

International standards for strong authentication mechanisms continue to be improved. Areas that need additional focus include:

- Behavioural biometrics
- Relative strengths of authenticators

- Requirements for security capabilities of mobile devices relative to authenticator strength
- User experience requirements for strong authentication

ITU-T SG 17 is the lead study group on identity management and currently Q10/17 is updating Recommendation X.1254 "Entity Authentication Assurance" to reflect recent changes to NIST Special Publication 800-63-3 "Digital Identity Guidelines".

Additionally, FIDO UAF 1.1 and FIDO CTAP protocols have been standardized in SG 17 as recommendations X.1277 and X.1278.

The work presented in this report was written with the consideration of being submitted to Q10/17 of ITU-T SG 17 for further standardization as part of the X.1254, X.1277 and X.1278 work.

Annex A – Bibliography

[1] ITU-T, "ITU-T FG-DFS Main Recommendations," March 2017. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Main-Recommendations.pdf.

[2] ITU-T, "The Digital Financial Services Ecosystem," May 2016. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/FINAL%20ENDORSED%20ITU%20DFS%20Introduction%20Ecosystem%2028%20April%202016_formatted%20AM.pdf.

[3] ITU-T, "Reccomendation X.1254 Entity Authentication Framework," 07 September 2012. [Online]. Available: http://handle.itu.int/11.1002/1000/11608.

[4] National Institute of Standards and Technology, "Special Publication 800-63B," National Institute of Standards and Technology, Washington, DC, 2017.

[5] D. Balfanz, A. Czeskis, J. Hodges, J. Jones, M. B. Jones, A. Kumar, A. Liao, R. Lindemann, E. Lundberg, V. Bharadwaj, A. Birgisson and H. Le Van Gong, "Web Authentication: An API for accessing Public Key Credentials Level 1," 20 September 2018. [Online]. Available: https://w3c.github.io/webauthn/. [Accessed 21 September 2018].

[6] M. Sporny and D. Longley, "Verifiable Credentials Data Model 1.0," 18 September 2018. [Online]. Available: https://w3c.github.io/vc-data-model/. [Accessed 18 September 2018].

[7] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant and M. Sabadello, "Decentralized Identifiers (DIDs) v0.11," 23 August 2018. [Online]. Available: https://w3c-ccg.github.io/did-spec/. [Accessed 20 September 2018].

[8] A. Offerman, "Swiss City of Zug issues Ethereum blockchain-based eIDs," February 2018. [Online]. Available: https://joinup.ec.europa.eu/node/700433. [Accessed September 2018].

[9] World Bank, "Technology Landscape for Digital Identification," 2018. [Online]. Available: http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).. [Accessed 20 09 2018].

[10] S. N. Yanushkevich, "ENCM 509 Fundamental of Biometric System Design Chapter 1," [Online]. Available: http://www.ucalgary.ca/btlab/files/btlab/ch1.pdf. [Accessed 15 July 2018].

[11] The Chertoff Group, "Strong Authentication In Cyberspace," February 2017. [Online]. Available: https://www.chertoffgroup.com/files/docs/StrongAuthenticationinCyberspace_8KeyPrinciplesforPolicymakers.pdf. [Accessed September 2018].

[12] Open Banking Limited, "Customer Experience Guidelines," September 2018. [Online]. Available: https://www.openbanking.org.uk/providers/standards/. [Accessed 09 2018].

[13] ITU-T, "ITU-T FG-DFS Executive summary," March 2017. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Executive-summary.pdf.

[14] FIDO Alliance, "Frequently Asked Questions," [Online]. Available: https://fidoalliance.org/faqs. [Accessed 15 July 2018].

[15] FIDO Alliance, "Client To Authenticator Protocol v2.0," 27 September 2017. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-ps-20170927/fido-client-to-authenticator-protocol-v2.0-ps-20170927.html. [Accessed 15 July 2018].

[16] FIDO Alliance, "Universal Authentication Framework," 02 February 2017. [Online]. Available: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-protocol-v1.1-ps-20170202.html. [Accessed 15 July 2018].

[17] World Bank, "Technology Landscape for Digital Identification," World Bank, Washington, DC, 2018.

[18] FIDO Alliance, "Setting the Standard for Healthcare Security: Aetna Rolls out FIDO and Behavioral Authentication.," 19 July 2017. [Online]. Available: https://fidoalliance.org/aetna-deploys-fido-authentication. [Accessed 11 04 2018].

[19] OpenID Foundation, "OpenID Foundation Specifications," [Online]. Available: http://openid.net/developers/specs/. [Accessed 07 August 2018].

[20] OpenID Foundation, "OpenID Connect FAQ and Q&As," [Online]. Available: http://openid.net/connect/faq/. [Accessed 07 August 2018].

[21] FIDO Alliance, "FIDO Deployment Case Study K-FIDO," September 2017. [Online]. Available: https://fidoalliance.org/wp-content/uploads/FIDO-Deployment-Case-Study-K-FIDO_170905.pdf. [Accessed September 2018].

[22] "Press Release," 14 09 2018. [Online]. Available: https://www.prnewswire.com/news-releases/id2020-alliance-launches-inaugural-pilots-welcomes-new-partners-at-annual-summit-300713089.html?tc=eml_cleartime. [Accessed 27 11 2018].

[23] "ID2020 Alliance - Committed to improving lives through digital identity," 2017. [Online]. Available: https://id2020.org/s/ID2020AllianceDoc_UPDATED.pdf. [Accessed 27 11 2018].

[24] "Press Release," 14 09 2018. [Online]. Available: http://www.globenewswire.com/news-release/2018/09/14/1571269/0/en/Everest-ID2020-and-the-Government-of-Indonesia-TNP2K-Secretariat-Announce-Innovative-Identity-and-Blockchain-Pilot-Solution-to-Enhance-the-National-LPG-Subsidy-Program.html. [Accessed 27 11 2018].

[25] GSMA, "Mobile Connect - Operator cooperation in South Korea has created a successful identity solution," 2017. [Online]. Available: https://www.gsma.com/identity/wp-content/uploads/.../mc_skt_case_08_17_v.1b.pdf.. [Accessed 13 09 2018].

[26] FIDO Alliance, "FIDO & PSD2: Meeting the needs for Strong Customer Authentication," 2017. [Online]. Available: https://fidoalliance.org/wp-content/uploads/FIDO-PSD2-white-paper-FINAL.pdf. [Accessed 20 09 2018].

[27] European Banking Authority, "Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)," 2017. [Online]. Available: https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf. [Accessed 12 09 2018].

[28] FIDO Alliance, "Universal Second Factor Overview," 11 April 2017. [Online]. Available: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html. [Accessed 15 July 2018].

Annex B – Guidance for DFS Providers

DFS Providers engage with consumers and manage most aspects of their user experience. Careful attention to customer journeys and user experience can increase trust in the system and increase operational security. Open Banking has published Customer Experience Guidelines [12] that describe 'experience principles' which were developed to assist designers.

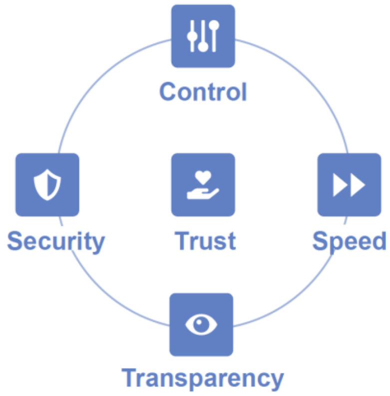

Figure 31: Open Banking experience principles for user engagement

Control: Consumers need to have a sense of control through having the right tools and clear information at the right time.

Speed: Speed must be appropriate to the specific customer and interaction. Fastest is not always best.

Transparency: Transparency of choice, action and information about consequences are crucial.

Security: Fraud and data privacy are top concerns for users of DFS. Messaging and information about security measures must be clear and direct.

Trust: The combination of the Control, Speed, Transparency and Security principles create a trusted environment for the customer.

Annex C – Guidance for Authentication System Providers

Authentication standards organizations publish guidance material for authentication system providers to assist with implementation. Guidance material relevant to the standards cited in this report include:

<u>NIST Trusted Identities Group:</u>

https://www.nist.gov/itl/tig/projects/special-publication-800-63

Implementation guidance

“NIST will work with the community to prepare implementation guidance for the Digital Identity Guidelines. The goal is to give implementers easily deployable guidance and help them meet the requirements.”

<u>Fido Alliance:</u>

https://fidoalliance.org/white-papers/

FIDO Alliance White Paper: Enterprise Adoption Best Practices – Managing FIDO Credential Lifecycle for Enterprises (April 2018):
“This white paper provides guidance to IT and Security professionals on how manage FIDO authentication credentials throughout their full lifecycle.”

FIDO Alliance White Paper: FIDO & PSD2 – Providing for a Satisfactory Customer Journey (September 2018):
“This white paper examines the different authentication models that could apply within the interactions of a Third-Party Provider and an Account Servicing Payment Service Provider. It proposes the FIDO standards as a solution to simplify the user experience, for any of these models, in a way that meets the Strong Customer Authentication requirements of PSD2.”

FIDO Alliance White Paper: Enterprise Adoption Best Practices – Integrating FIDO & Federation Protocols (December 2017):
“This white paper outlines how the FIDO standards compliment federation protocols. It also provides guidelines on how to integrate the two in order to add support for FIDO-based MFA and replace or supplement traditional authentication methods in federation environments.”

<u>OpenBanking:</u>

https://www.openbanking.org.uk/providers/standards/

Customer Experience Guidelines

“This document brings together regulatory requirements and extensive customer research to provide customer experience guidelines and examples of customer journeys for third party providers and account providers. They are designed to encourage adoption of Open Banking-enabled products and services.”

<u>GSMA Mobile Connect:</u>

https://developer.mobileconnect.io/step-by-step-guide

“Implementing Mobile Connect involves interacting with a number of different services and technologies. This section shows each of the steps you need to follow and offers guidance on how to complete the steps.”