GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

White Paper

Verified Digital Identity – Key Applications Driving Growth & Adoption

www.goodeintelligence.com

First Edition December 2019

Published by:
Goode Intelligence
United Kingdom

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

VERIFIED DIGITAL IDENTITY – KEY APPLICATIONS DRIVING GROWTH AND ADOPTION

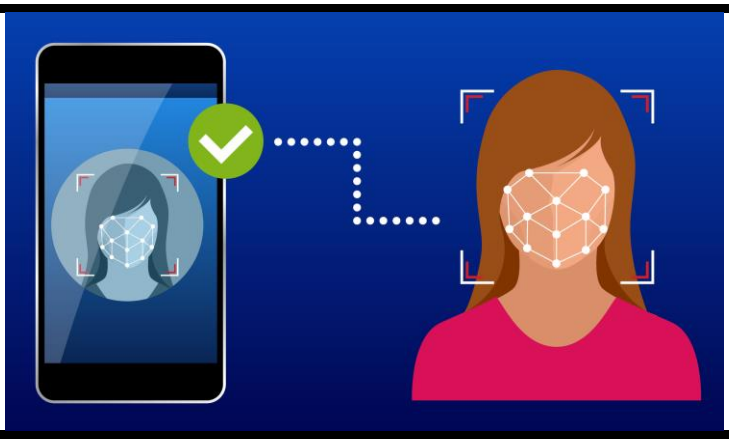
Introduction

This white paper from Goode Intelligence is derived from content from the 2019 market analyst report **The Digital Identity Report – The Global Opportunities for Verified Citizen & Consumer Digital ID; Market & Technology Analysis, Adoption Strategies and Forecasts 2020-2025 Identity Verification**.

The question of how we effectively and securely identify people and enable them to perform both offline and online tasks in a safe and secure manner is one of the fundamental ones of our time.

Verified Digital Identity

A digital identity that is issued by an identity issuer or provider who has a high level of assurance of the authenticity of the individual requesting the identity credential. The issued credential can be used in high-assurance applications/use cases.



Goode Intelligence has identified a number of key applications that are enabled by verified digital identity that include:

1. **Identity Verification**
    a. Supporting remote customer onboarding
2. **Access to eGovernment services**
    a. Providing a single digital identity to access cross-department digital government services including eVoting
3. **Assured Authentication**
    a. When the digital identity is highly assured and issued after strong identity and document verification then it can be used for assured authentication
4. **Digital Travel**
    a. Mobile driving licences (mDL)
    b. Kerb-to-Gate airport
5. **Age Verification**
    a. Offline – used in bars and clubs instead of a paper document
    b. Online – used to ensure access to adult (age restricted) digital content and services is upheld
6. **Digital Signature**
    a. Supporting smart contracts

Before we investigate these applications in more detail it is important to consider what digital identity is and to detail the three main digital identity models that are currently prevalent.

What is Digital Identity?

Everyone has a different definition of digital identity. This is a complex and fragmented market with multiple definitions of what digital identity is. It is not authentication, but a digital identity credential can be used for authentication.

> **"Without context, it is difficult to land on a single definition that satisfies all"**
> NIST Digital Identity Guidelines

Digital Identity has many definitions and here are a few that help frame this white paper:

"Digital Identity is the digital version of a person's physical identity – a digital representation of the individual" – BBVA

"Representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context" – ITU 2010

"Collection of individual attributes that describe an entity and determine the transactions in which that entity can participate." WEF. The WEF categorises attributes into three groups:

- Inherent (age/biometrics)
- Inherited (behaviour)
- Assigned attributes (ID number)

"A digital identity is information used by computer systems to represent a unique person, organisation, application or device. So, for a citizen or consumer, a "digital identity" is a trusted way of proving one or more attributes about themselves online or offline and the linkage of those attributes to that same person as a uniquely identifiable individual." UK Government.[1]

"Digital identity is the online persona of a subject, and a single definition is widely debated internationally. The term persona is apropos as a subject can represent themselves online in many ways. An individual may have a digital identity for email, and another for personal finances. A personal laptop can be someone's streaming music server yet also be a worker-bot in a distributed network of computers performing complex genome calculations. Without context, it is difficult to land on a single definition that satisfies all." NIST[2]

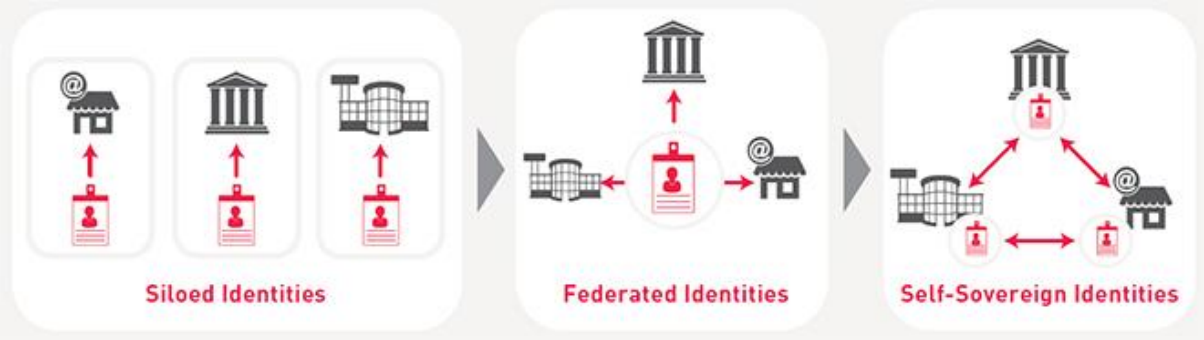
[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf
[2] https://pages.nist.gov/800-63-3/sp800-63-3.html

Digital Identity Models

Digital Identity schemes can be classified under one of three models:

1. **Centralised Identity:** Identity data is centrally held by an organisation that an entity has a relationship with, e.g. employee/employer and consumer/service provider.
2. **Federated Identity:** Identity data is held by a trusted identity provider, who attests claims made to services requiring identity.
3. **Self-Sovereign Identity:** Identity data *attested* by multiple identity providers is held by the person (entity) who decides when to share an attestation with a service provider.

Figure 1: Digital Identity Models



Source: Gemalto, a Thales company

Your digital identity is a lot more than your login credentials. Login credentials supports the connection between a person and the digital world. Your digital identity consists of thousands of data points that make up a profile of who you are and your preferences

Digital Identity Market Overview

Verified digital identity is issued and managed by two main entities:

- Government, both state and federal
- Commercial companies and organisations.

For these identity schemes, there are scenarios when a government-issued identity credential will be used, verified by a commercial organisation and less frequently, when a commercially issued identity credential will be used by a government entity.

Government issued digital identity operates on a permission model tied to the issuing entity, for instance permission to travel internationally or to drive a certain type of motor vehicle and includes:

- Travel identity including passports
- Drivers licences
- National ID (linked to a national citizen register)

Commercial identity predominantly analyses identity schemes that allow people to use digital identity credentials with more than one service provider – a ***relying party***[3]. These include Bank ID in the Nordics and Verified.Me in Canada where banks, telecommunication providers and governments collaborate to offer regional digital identity schemes.

- Commercial identities can be segmented into digital identity schemes managed by a range of industries, sometimes collaborating as a consortium, including: Financial Institutions
- Telecommunications providers
- Healthcare providers
- Technology/Social network providers including Apple, Facebook, Google and Microsoft

All of these entities, government and commercial alike, can also be classified as digital identity data owners. Verifiable identity data, often called attributes, is a critical component of a digital identity scheme and is used for identity verification or proofing.

The Smart Mobile Device (SMD) is the main endpoint for digital identity through enrolment, ID credential issuance and storage, authentication and digital signing services.

Digital Identity Mobile Wallets have become an important battleground in owning citizen and consumer data and the rush to 'own' citizens/consumers is creating a Digital Identity Wallet war – fought out between the technology giants and incumbent identity owners.

[3] Relying Party is a service, site or entity that depends on a 3rd party provider to identify and authenticate a user who is requesting access to a digital resource.

Key Applications Powered by Verified Digital Identity

CASE STUDY: PRECISE BIOMETRICS

Organisation: A company or a gym that needs an access system for entry.

Business Objective: To enable a secure and convenient way to access physical and/or digital services, with the identity enrolment carried out digitally by the end user. The user retains ownership of their digital identity throughout.

The Challenge

Often when a person is first hired as a new employee or arrives at a premises as a new member (for example at a gym), the process to enable access can be a lengthy one involving taking photographs of the individual, issuing them with a pass or tag and setting up access rights so they can enter the pre-determined areas. As well as taking time, this is inconvenient and not cost efficient. Then, once people have been granted access in this way, there is the problem of dealing with lost or forgotten passes/tags with new or temporary ones having to be issued – another admin cost and further inconvenience. Finally, even though the initial process of access and identity checking has been carried out correctly, it is difficult to ensure that only the correct person continues to enter by relying on this method of using passes/tags since they can be stolen or borrowed, enabling access to the wrong person, compromising security.

The Solution

Precise Biometrics has developed a modern method utilising face biometrics to access office and membership facilities. Using its solution Precise YOUNiQ, the digital identity of the end user is integrated into the physical access domain, eliminating the need for access cards and tags.

The new employee/member is sent a link to a web app in order to digitally onboard to the access system. They provide a selfie, similar to the current process when arriving as a new employee or registering at a gym where someone will take a photo of you, only this is now done at a time convenient to the individual. Depending on local requirements, identity is also added if required for further security. Next the selfie is transformed into a biometric template and securely stored in a server connected to the camera at the facility's entrance. Finally when the person arrives at the facility, the camera will live video stream them approaching. As the system recognises the individual, the door opens automatically with no need to stand and wait for facial recognition to take place. There are no physical cards or other tokens to remember, lose or be stolen.

The Results

Gym

Joining the gym provides members with a great customer experience for access, including services such as trialling its facilities before signing up for full membership as the need to visit the gym first is now eliminated.

Existing members continue to experience this excellent service as they can enter the gym whenever they want to without the need to remember to bring an extra physical object such as a tag or an access card.
For the gym this is seen as a cost efficient, convenient way to handle access, and an innovative opportunity to promote their services as new potential members can try out their facilities before becoming a full member.

Company

Many of us will have experienced first-hand the difficulties of being onboarded as a new employee to a company. With Precise YOUNiQ, a person can be conveniently and securely onboarded remotely to enable access rights for their new office.

For companies receiving high numbers of visitors, this solution also enables a welcoming experience by enrolling them remotely in a similar way to new employee onboarding prior to their visit. No temporary access cards or tags are needed.

In both cases, Precise YOUNiQ is a solution that ensures that customers are able to specify particular features aligned with their requirements, which are then delivered and deployed in an agile development way by Precise Biometrics.

THE DIGITAL IDENTITY REPORT – THE GLOBAL OPPORTUNITIES FOR VERIFIED CITIZEN & CONSUMER DIGITAL ID; MARKET & TECHNOLOGY ANALYSIS, ADOPTION STRATEGIES AND FORECASTS 2020-2025

The first edition of **The Digital Identity Report – The Global Opportunities for Verified Citizen & Consumer Digital ID; Market & Technology Analysis, Adoption Strategies and Forecasts 2020-2025** is a comprehensive 228 page report that includes a review of current global adoption, market analysis including key drivers and barriers for adoption, interviews with leading stakeholders, technology analysis with review of key technologies and profiles of companies supplying solutions across key verticals plus forecasts (regional and global) for digital identity users, key technologies, and revenue within the six-year period 2020 to 2025.

The report examines the market for both government and commercial scheme issued digital identities around the world in three digital identity models: Centralised, Federated and Self-Sovereign. The report includes:

1. Review of current global adoption
2. Market analysis, including key drivers and barriers for adoption
3. Adoption Strategies and examples segmented by region and industry
4. Technology analysis
5. Analysis of important technology vendors and services providers operating in this sector
6. Forecasts for digital identity users and revenue within the six-year period 2020 to 2025

ABOUT GOODE INTELLIGENCE

Goode Intelligence is a leading identity, authentication and biometrics research, consulting and events organisation founded in 2007, headquartered in London.

For more information about Goode Intelligence or our research please visit www.goodeintelligence.com. Follow us on Twitter.

Further information about **The Digital Identity Report – The Global Opportunities for Verified Citizen & Consumer Digital ID; Market & Technology Analysis, Adoption Strategies and Forecasts 2020-2025** report can be found at https://www.goodeintelligence.com/report/the-digital-identity-report-the-global-opportunities-for-verified-citizen-consumer-digital-id-market-technology-analysis-and-forecasts-2020-2025/

Interested in Digital Identity?

Join us at one of our identity events.

Our next event, Identity Summit London 2020, hosted by Rise London, takes place on 30 January 2020 in London to bring together the identity industry to discuss and debate the latest trends and technology developments that are shaping this industry.