VALOORES

*Digital Transformation*

## *in'* Digital Transformation

*DELIVERING*

## *DIGITAL ID*

*in'*

***FinTech***

***RegTech***

***GovTech***

***The Biggest part of Digital Transformation is,***
***Changing the Way we Think and Deliver, … to be Used!***

***in'VALOORES,***
***Be the Change you Want to Be,***
***and Make a Difference …***

***EXCELLENCE***
***in'EXECUTION***

***There is No Gain, without Pain,***
***… Based on a Solid Information Integrity***

***We Deliver Advanced Analytics-Based Governance, Risk, and Compliance Solutions to Financial Institutions, Central Banks, Banks, Insurance... It's been over 30 years of Success now.***

## VALOORES - A Brief Summary in few Lines

VALOORES empowers decision making, helping people and businesses around the globe reach their targets. Founded in 1989 in France, the Company is a pioneer in Master Data Governance, Retail & Merchandising, Supply Chain Optimization, KYC, Regulatory Compliance, Financial Crime - AML & Fraud, Predictive Analytics and Data Science to improve their on-going operations, executions and decisions.

# VALOORES DIGITAL ID in FinTech, RegTech, & GovTech

## VALOORES DIGITAL ID

VALOORES believes that Digital IDs are important to broaden public policy, especially for Financial Inclusion and can help bring more Micro, Small, and Medium Enterprises into the formal Financial Sector.

There are several aspects that are essential.

- The ID should be robust and secure
  - In many jurisdictions, not all IDs have all the attributes, and even those that possess them might not have universal coverage in the jurisdiction
  - With the absence of any form of legal ID impacts all access to basic financial services; a lack of unique ID obscures a reliable view of customer activity and can impact access to the full range of Financial Services, especially Credit and Insurance.
- The lack of a unique digital ID increases the costs of providing Financial Services to certain segments of society, thereby impacting financial inclusion.
- For financial inclusion, universal coverage of legal ID in a given jurisdiction is paramount.

VALOORES Data Governance - Mitigating Digital ID Risks

- The issue of sensitive data privacy (securing the data while at rest and in transit) and the potential for leakage, theft or misuse of personal data and the risks that arise from non-regulated players outside the traditional financial system.
- The appropriate classification and categorization of data, and adherence to Data Governance rules and procedures are the main ways to maintaining a robust digital ID framework.
- Another important challenge is the rapidly evolving nature of the technologies, and it is important

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

that central authorities and public bodies consistently incorporate new technologies and business models while protecting the financial sector and its customers.

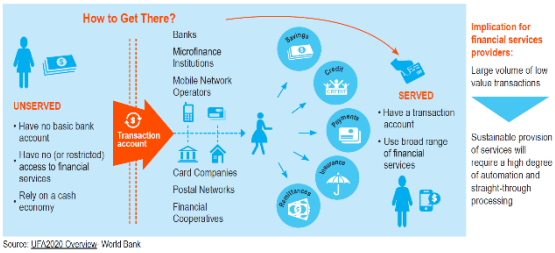
VALOORES believes that the Digital ID has immense potential and it is important that country's financial service supervisory framework recognizes this. Financial sector regulations, specifically those related to AML/CFT, have longstanding requirements related to identity validation, authentication and retention of records, to ensure the safety and integrity of the financial system, based in large part on the **Financial Action Task Force (FATF)** recommendations.

VALOORES is working closely with Governments and Financial Institutions to have an effective Digital ID system that meets the needs of the financial sector.

- Ensuring an integrated identity framework
- Capturing challenges related to digital ID, and risks to its appropriate implementation
- Establishing a reliable oversight model to include stakeholders beyond the traditionally regulated financial institutions who can introduce risks to digital identity systems
- Building authentication and service delivery systems that protect user privacy
- Establishing clear procedures to define responsibility in the event that errors emerge or that the security of a person's identity is compromised
- Leveraging the ID infrastructure for building out digital layers; ensure that services are safe, reliable and efficient
- Digital ID knowledge sharing

## VALOORES facilitating Customer Identification for Digital Financial Services

VALOORES facilitates access to digital financial services through its customer identity systems, products and services that are accessible, affordable, verifiable, and accommodates multiple needs and risk levels for a *Risk-Based Approach* to *Customer Due Diligence*.

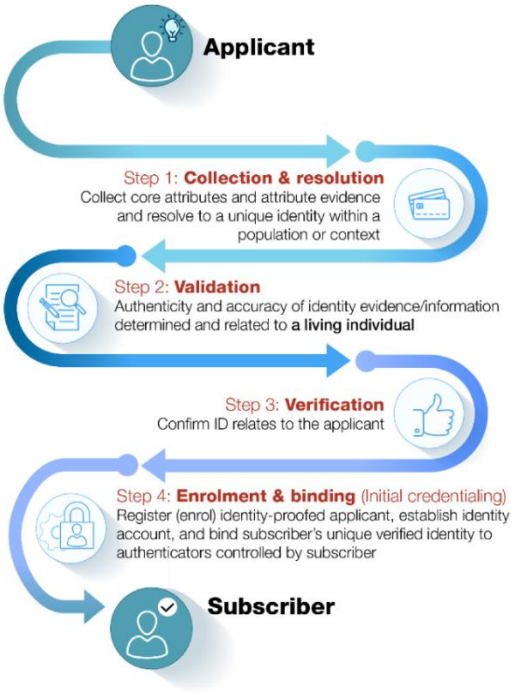



## VALOORES secures its Compliance with the FATF Guidance through all its Digital ID Implementations

VALOORES marches at the same drum with the FATF Guidance, that's intended to assist governments, regulated entities, and other relevant stakeholders, in determining how Digital ID systems work, and can be used to conduct certain elements of Customer Due Diligence (**CDD**) under the global **AML/CFT** standards of the FATF Recommendations.


VALOORES secures its Compliance with the FATF Guidance through a flexible Risk-Based Approach (**RBA**) whilst embracing Digital ID systems (with different **AML/CFT** assurance levels) for **CDD** that supports Financial Inclusion (Identity proofing / enrolment and authentication for tiered CDD).

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.




**Digital ID Potential.**

The Digital ID improves trustworthiness, security, privacy, and convenience of identifying natural persons in the global economy of the digital age; it can:

- Facilitate customer identification and verification at on-boarding
- Support ongoing due diligence and scrutiny of transactions
- Facilitate other customer due diligence (CDD) measures
- Detecting / reporting suspicious transactions and anti-fraud efforts

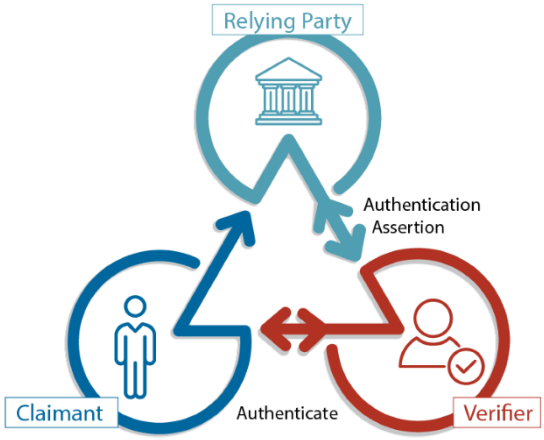
The Digital ID has the potential to reduce costs, increase efficiencies (resource reallocation to other AML/CFT functions), and contribute to Financial Inclusion, to further reinforce AML/CFT safeguards.

**Digital ID Risks.**

Identify, assess and mitigate the money laundering or terrorist financing risks is paramount when it comes to the use of Digital ID.

Cybersecurity flaws (privacy, fraud or other related financial crimes risks) can result in massive identity theft, compromising individuals' Personally Identifiable Information (PII).

Risks related to governance, data security and privacy also have an impact on AML/CFT measures.




## VALOORES Digital Identity

VALOORES digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions. It provides remote assurance and manages the lifecycle of individual digital identities.


A person's digital is composed of a variety of attributes, used as authentication factors.

- Biographic data (e.g., name, age, gender, address)
- Biometric data (e.g., fingerprints, iris scans, hand prints)
- Credentials issued by the service provider (e.g., unique ID number, eDocument, eID, mobile ID)
- Other attributes that are more broadly related to what the person

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

does or something someone else knows about the individual.

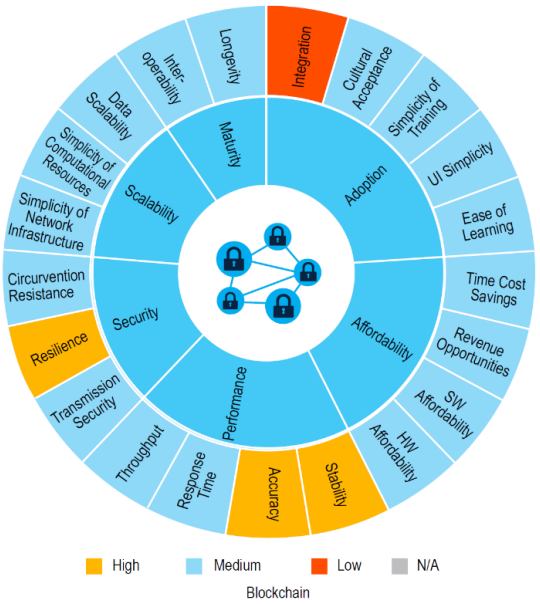
## VALOORES BLOCKCHAIN and the Digital Identity

VALOORES believes that federated authentication provides the solution to trust unknown identities across organizations or even borders; this is illustrated by BLOCKCHAIN.

BLOCKCHAIN is being trialed for various financial sector applications including funds transfers, payment settlement and regulatory oversight, and due to its decentralized and transparent nature also increasingly in identity management as well; i.e. supporting the development of self-sovereign identity (SSID) with underlying legal ID which is first validated by the issuing authority before being managed by an individual / entity on their own.

The immutable nature of the ledger ensures that dispute resolution is embedded and enforced by computer protocol. The transparency, resilience and replication at each node offered by the shared ledger is a useful tool for tracking and maintaining the integrity of the information.

VALOORES BLOCKCHAIN empowers individuals to have complete control over their identity including where, when and what parts of their identity they wish to share. VALOORES though is constantly matching its development progress against the dimensions of Maturity, Ease of Adoption, Affordability, Performance, Security and Scalability.




## Application of Digital Identity in VALOORES Financial Services

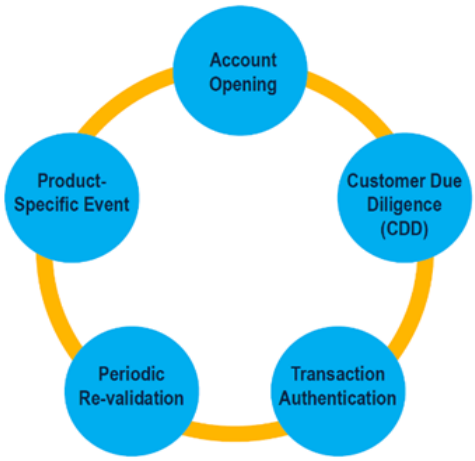
VALOORES believes that Identity is integral to providing and obtaining Financial Services, and is needed at various transaction points when using financial services. The role Digital ID plays varies at each of these transaction points, and for different services.

During account opening, a customer is required to provide information so that the Financial Services Providers can carry out CDD procedures. Information needs to be validated and matched against other information gathered from other sources, such as credit bureaus, to validate the provided information and assess the suitability of the product to the individual. Once complete, a transaction identifier maybe issued (for example a debit card and PIN), to be used for authentication in future transactions or access to other services.

Information gathered during account opening, as ing address, other contact details, and employment status, can change over the customer lifecycle. Hence, periodic re-validation is required to ensure that key data underpinning CDD continues to be valid (frequency varies

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

according to local regulatory requirements), depending on of the customer's risk profile.




VALOORES groups its applications and utility of Digital ID into the following.

- Account opening
- Ongoing authentication and customer consent
- Back-office processes

VALOORES Digital ID applications in each of these areas.

- Account Opening
- Customer Due Diligence
- Authentication

VALOORES Digital ID potential.

- Transform payment services for Financial Services Providers, Government-to-Person (G2P), and humanitarian assistance
- Improve identification of firms and employees
- Digital Signatures
- Regulatory Compliance Reporting

## VALOORES Digital ID - Account Opening

One of the important applications of Digital ID in the financial sector is account opening at a financial institution through a mobile money provider. Another application is the digitization of government payments, to reduce the number of unbanked people.

## VALOORES Digital ID - Customer Authentication

After Account Opening and Customer Due Diligence, Financial Services Providers need the ability to authenticate customer identities for a variety of services and transactions.

VALOORES offers the following.

- Secure digital authentication mechanisms, based on attributes and credentials established during account setup, to ensure that only legitimate customers to access services and to prevent identity theft and Fraud.
- Automated methods of authentication that do not require the costs and manpower of face-to-face interaction.

VALOORES believes that the market is heading towards de-coupling authentication credentials from a specific financial product, and making it available as a service on its own.

- Example: The growing use of token-based authentication to access one's accounts at an institution; allow users to enter username and password to obtain a token which allows them to fetch a specific resource.

### *VALOORES Biometric Based Authentication*

VALOORES believes in exploring biometrics for authentication, as a response to AML and CFT concerns.

- Biometrics are physical and behavioral attributes of a person and are increasingly used as a means of proving one's identity.
- Biometric recognition uses an individual's unique physiological and behavioral attributes to identify and authenticate his or her identity. The type of attribute collected and matched is called modality.
- VALOORES supports all types of

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

modalities: Hard, Soft and Hidden.

- The Hard or traditional modality includes iris scans, fingerprints or signatures
- The Soft is related to faces, skin color, hair color or measurements and to bodies, like height or weight. It also includes behavioral characteristics and mannerisms such as gait, keystroke patterns, and mouse usage.
- The Hidden modalities, also referred to as intrinsic, are based on medical data or X-rays.

VALOORES believes that Biometrics are an opportunity for customers: the use of modalities such as fingerprint scanning and facial recognition will not only offer a great deal of convenience in general, but also a new form of security and identity verification, which may suit some customers better than traditional tools.

### *Personal Identification Number (PIN)*

- Some customer segments cannot use PINs reliably, due to illiteracy, innumeracy or lack of familiarity with the technology and other issues. The security of the PIN lies in being able to commit it to memory.
  - Infrequency of use though leads people to write their PINs down, often on the back of the card or mobile phone they are using, leading to PIN compromise.
- PINs can and often are easily be shared with others, which can present a security risk.
- Regulatory authorities in several countries have concerns that a PIN is not secure enough, for at least some financial transactions.

### *Smartcards*

- Smartcards (embedded integrated circuit or chip) can be used to store attributes and credentials such as PINs or biometric data, and with the appropriate application, can enable interaction with recorded data (i.e. Smartcards can be used to verify that a fingerprint sample collected by a connected device is the same as a template stored in the Smartcard).
- Smartcards can either be “contact” cards that are read when in direct physical contact with a reader, or “contactless” card that uses Near Field Communication (NFC) or radio frequency identification (RFID) technology.
- Complications and risks
  - Data privacy, dilution of data ownership, liability between state identity authorities, payment service providers and banks, and general risk and fraud management.

### *Mobile SIM Authentication*

- With the ubiquity of mobile phones, there is increasing interest in using the unique identification numbers associated with mobile subscriber

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

identity modules or SIM cards. The algorithms contained in the SIM card allow for encrypted communication between the user and the network. For authentication, the authenticating body generates a random sequence of numbers that is sent to the user's mobile; this is the user's public key. The public key together with the user's private key and authentication algorithm contained in the SIM, verifies the user.

- It enables customers to create and manage a digital ID via a single log-on on their mobile phone.
- Cryptographic SIM cards offer subscribers secure mobile authentication through a local BankID solution to provide secure online user identification and user digital signature verification.

## VALOORES Digital ID - Payment Systems and Services

VALOORES Digital ID enables re-structuring payment services and processes.

### *Combining ID and Payment Applications*

ID and payment applications can be combined in one form factor such as a mobile phone and its associated SIM card or even a smartcard or other chip based token. If the basic Digital ID credentials are unique and enable individuals to reliably assert their identity without including other data attributes by default, this will spur developments to minimize the disclosure of data.

Linking a payment application to a Digital ID by co-hosting the two applications on the same smartcard can potentially be problematic.

- Payment or Money Transfer Provider isn't a bank; in order to function, the application needed to be linked to a bank account not under the control of the Payment Provider, presenting issues around consumer choice, data protection and simple practicality, beyond the challenge of having a particular commercial brand being tied to a national ID system.

### *Using VALOORES Digital ID Infrastructure for Authentication*

VALOORES Digital ID infrastructure can be used for authentication in place of a dedicated authentication arrangement for a payment instrument. It serves as an important tool for the central authentication for a variety of e-KYC transactions, instead of a dedicated authentication arrangement for a single payment instrument. This increases the level of assurance without adding a corresponding decrease in usability.

VALOORES fingerprint authentication mechanism allows an individual to pay, by simply providing a fingerprint at a participating merchant expelling the need to enter an account number or present a payment card.

### *VALOORES Digital ID Credential as an "Address"*

The Digital ID credential can be used in lieu of a bank account number to direct payments removing the need to reveal the recipient's account number to the payer agencies. This is accomplished by maintaining a mapping between the

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

credential and payment related identifiers.

### *VALOORES Digital ID for Government to Person (G2P) Payments*

The Digital ID brings a government to person (G2P) benefit that supports efficiency and aims to remove Fraud. It can be utilized to support automatic and hassle-free payouts as well as to remove payments made to fraudulent accounts.

It offers to government departments and agencies, for instance, the capacity of direct transfer of benefits and subsidies under a direct benefit transfer scheme, i.e., paying the benefit as a monetary value instead of as physical goods or services.

The same principle can be used for disaster relief and humanitarian relief payments made directly to transaction accounts.

Mapping the individual's Digital ID to the eligibility records in the social benefit transfer systems, enables government agencies to reliably ensure that only eligible individuals are receiving the transfers and no individual is able to avail the same services from different locations or different points of time using a different identity. This has substantial implications for the public financial management systems and is also critical for public sector employee salaries and pension payments.

## VALOORES Digital ID - Regulatory Compliance Reporting

Some of the Regulatory Compliance Reporting schemes, like Credit Reporting, collects data around consumers' behavior against financial obligations, reliably linking all records collected from different institutions to the relevant consumer, and building up a profile of the customer. When it comes to credit products, lenders use risk management and underwriting procedures that traditionally supplement their credit appraisal process with data pulled from this credit reporting system.

Credit reporting for disadvantaged individuals though, remains a challenge. An effective credit reporting relies on mechanisms for identifying individuals and firms as well as for linking them unequivocally with their financial obligations.

There's a need to uniquely identify the individual or legal entity and use that unique identifier to organize all the records in the database. The lack of a unique ID in a credit reporting system could lead to inaccuracies and create serious problems to the integrity of the database such as duplication or the inability to match an individual to a credit score due to differently spelled names or addresses. This fundamentally impacts the effectiveness of credit reporting systems.


VALOORES Digital ID enables the credit reporting system to correlate details between systems, and provide Fraud Prevention services based on the vast amounts of data collected from different sources; detect errors and signs of potential Fraud including identity theft through monitoring techniques based on data reporting patterns.

## VALOORES Digital ID - Document Management and Digital Signature

VALOORES Digital ID helps businesses streamline onboarding of new customers and allow legally-binding contracts to be signed online.

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

Once the required ID validation and verification checks have been completed, Financial Services Providers need to preserve the records of the validation conducted, as required under the jurisdictional regulations. The use of VALOORES Digital Environment supplemented with VALOORES Digital ID allows for a more efficient method to record, store and retrieve validations, by both the Financial Services Providers, and external parties such as auditors and regulators.

Consumer protection regulations in the financial sector rightly require express consent from customers to provide them with a service or change the terms and conditions of a current service. Digital signatures have been a solution to these concerns, however it has been a slow and expensive process to extend the service to non-corporate customers. In addition, it involves risks regarding consumer protection and consent which need to be addressed adequately.

VALOORES Digital ID, however, offers simpler and more cost effective means to provision digital signatures, in an easy to use user interface. It opens up opportunities for supporting remote account opening.

Access to Digital Signature infrastructure and allowing customers to authenticate themselves digitally enables financial institutions to interact remotely with customers, exchange agreements as well as terms and conditions and other confidential documents digitally. This can bring about significant cost savings for both individuals and the FSP by reducing the cost of paper based processing, transmission and associated staff time.

## VALOORES Digital ID - Insurance

A unique digital ID is an important asset in the insurance industry as well.
VALOORES Digital ID offers the ability to establish remote ownership of an asset; for example, it can link a driver's license to a unique ID establishing a unique link that has implications for insurance.

For uses such as universal health care coverage which require large scale and integration, the importance of valid authentication and accurate records are being considered by governments globally. The ability of Digital ID systems to aggregate data and provide valid authentication and maintain accurate records is extremely important and is more relevant in countries which are scaling up for universal health coverage.

Health financing and insurance schemes also need complete and accurate records on service usage and data on system performance to correctly bill patients and care providers, and to inform budgeting and management decisions.

## VALOORES Digital ID - Levels of Assurance

When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that she is who she claims to be depends on

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.

the degree of security assurance provided and the context in which the information is captured, referred to as the level of assurance (LOA).

Assurance levels depend on the strength of the identification and authentication processes, and are critical to access control and reducing identity theft. The higher the LOA, the lower is the risk that service providers will rely on a compromised credential during a transaction. For “identity proofing,” the LOA is dependent on the method of identification, including the scope of personal information and attributes collected about an individual during enrollment, and the degree of certainty with which these attributes are ascertained. For example, if personal data are collected during enrollment but not de-duplicated or checked against existing databases for veracity, this would constitute a low LOA because there is no validation of the identity information.

These levels shown below, along with corresponding definitions from the European Union’s eIDAS (Electronic identification and trust services) framework, and range from weak authentication protocols with extremely high security risk levels, to strong authentication protocols with minimal risk levels.
The level of risk is based not only on the credentials and processes used for authentication, but also on the robustness of identity proofing during the registration phase.

## VALOORES - Future Outlook

VALOORES is proud of the VBS success achieved till now; a myriad of solutions implemented in multiple lines of business so far. VALOORES is determined to innovate and solve Governance, Risk, Compliance, Profitability Problems and emerging challenges downstream.

VALOORES continues to partner with Regulators (Central Banks, Financial Information Units…) and Industry Catalysts (Thomson Reuters, Financial Integrity Network…) around the globe, and on board more Compliance and Financial Crime Experts, professionals, engineers, business analysts, and data scientists, to push the boundaries of Compliance, through **FinTech**, **RegTech**, & **GovTech**.

*The Global Outlook has considerations for Governments and Financial Institutions on their journey toward a 21st century Governance Risk and Compliance framework*

*Here comes VALOORES Added Values, to Walk with you, and stay this minute in advance of the Governance, Risk, & Compliance Headwinds…*

VALOORES

Over 30 years of
successful deliveries **déjà!**

**valoores.com**

Copyright © VALOORES. All rights reserved. Confidential and Proprietary.