Building Block Definition
Identity and Verification

Developed by a team comprising Valerie Khan (Digital Equity Association), Jaume Dubois (Identity System Expert at ID2030), Debora Comparin and Stephanie De Labriolle (OSIA), Ramesh Narayanan (MOSIP), Raul Kaidro (RaulWalter), Dr Ramkumar (Board of Indian Standards), Dr Edgar Whitley (Associate Professor (Reader) at London School of Economics), Deepti Vikas Dutt (Amazon Internet Services Private Limited), and Jonathan Marskell (World Bank ID4D).
In cooperation with GIZ, ITU, DIAL, and the Government of Estonia

Table of Contents

1 Version History

Version	Authors	Comment
1.0.0	Valerie Khan (Digital Equity Association), Jaume Dubois (Identity System Expert at ID2030), Debora Comparin and Stephanie De Labriolle (OSIA), Ramesh Narayanan (MOSIP), Raul Kaidro (RaulWalter), Dr Ramkumar (Board of Indian Standards), Dr Edgar Whitley (Associate Professor (Reader) at London School of Economics), Deepti Vikas Dutt (Amazon Internet Services Private Limited), and Jonathan Marskell (World Bank ID4D).	Initial revision
1.1.0	The team is very grateful for the additional review support from other Building Blocks within GovStack, as well as from Anita Mittal	Applied feedback from technical review.

2 Description

The purpose of this document is to be the high-level specification of the Identity & Verification building block (IDV BB), describing its internal architecture, its external interfaces and how it is expected to interact with external building blocks.

The IDV BB creates, manages and uses a digital foundational identity (functional identity is not in scope of this document). As a part of the overall identity system, it can be interfaced with other building blocks in order to realize the complete set of requirements necessary for the identification and verification of the other GovStack building blocks.

The IDV BB is composed of a set of interoperable sub-components/modules dedicated to the management of the foundational national identity and its representation offering different services for ensuring a trusted foundational identity to enable its related use cases.

The guidance from this building block will take note of recognized approaches across the globe which in detail and deployment can vary greatly. These approaches will consider central, federated and distributed (decentralized) models, and will remain flexible to allow for inclusion and updating of existing solutions where possible. This version of the document is focused on central models, leaving federated and distributed models to be explored in a subsequent phase.

This building block may have its own internal workflows and UI together with its own repositories for delivering its functions.

3 Terminology

Authentication

- The process or action of verifying the identity of a user or process. For the purpose of this project, authentication has been replaced with the term 'verification' to allow for a clearer definition and for demarcation with other building blocks.

Biographic data (or Demographic data)

- Set of text attributes representing the identity given at birth
- Common attributes: Name, firstname, birthdate, birthplace, parents biographic data

Biometric data

- Set of physical attributes which can be used to identify a person
- Most common ones are fingerprints, face and iris
- More can be used like voice, behavioral, veins, etc.
- Those data can be used for different reasons:
    - Establishing uniqueness of a person
    - Verifying a person identity
    - Identifying an unknown person
    - Claiming an identity
    - Verifying presence or liveness;
    - Deduplication

Civil Registry

- A civil registry or CRVS (Civil Registry and Vital System) is a system recording life events (birth, death, mariage, divorces, adoptions, name changes, …) It is used to keep track of life events of individuals and to produce statistics for policy making.

Claim

(Following is a general description of claims. For the purpose of this document only the first claim description is relevant since claims for foundational identity only refer to the question 'who are you' and not 'what are you')

- Can be pertaining to identity - I am X
- Can be pertaining to entitlement or eligibility - X is allowed to vote
- Can be pertaining to membership - X is an employee of Y corp
- Can be pertaining to ownership - X owns Z car
- Can be pertaining to role - X is a doctor
- Can be pertaining to any other identity association - X is an organ donor, X studied subject Y at Institution Z
- Can protect persons privacy by disclosing state of attributes without disclosing the attribute itself (ie "is older than 18" don't need to share the age)
- Can be pertaining to 3rd party claim i.e I claim that something is answerable at a 3rd party verification place

Credential

Taken from WB ID4D, Practitioners Guide, Glossary, https://id4d.worldbank.org/guide/glossary; adapted from ID4D Technology Landscape and Public-Private Cooperation reports.

- A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider.

Credential management

- Is a document lifecycle management regardless of its form. An identity credential can appear in both physical (ID card, passport, driver's license) and electronic form (eID);

- Includes issuance, maintenance, suspension, termination of suspension, revocation and expiration;

- There should be no difference between physical and electronic documents with the exception of audit trail kept during usage of the electronic document (eID).

Digital Identity

(Adjusted from ITU, Digital Identity Roadmap Guide, 2018, http://handle.itu.int/11.1002/pub/81215cb9-en)

- Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.

- The digital identity allows an entity (citizen, business, administration) to be distinguished from any other.

- A set of digitally captured and stored attributes and/or credentials that satisfactorily within context identify someone or something.

- Is a 'representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context'. Building on this definition, we might state that a digital identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context.

Digital Identifier

- Digital identity fundamentally requires digital identifiers—strings or tokens that are unique within a given scope (globally or locally within a specific domain, community, directory, application, etc.). Identifiers are the key used by the parties to an identification relationship to agree on the entity being represented. Identifiers may be classified as omnidirectional and unidirectional.[19] Omnidirectional identifiers are intended to be public and easily discoverable, while unidirectional identifiers are intended to be private and used only in the context of a specific identity relationship.

- Identifiers may also be classified as resolvable or non-resolvable. Resolvable identifiers, such as a domain name or e-mail address, may be dereferenced into the entity they represent, or some current state data providing relevant attributes of that entity. Non-resolvable identifiers, such as a person's real-world name, or a subject or topic name, can be compared for equivalence but are not otherwise machine-understandable.

- There are many different schemes and formats for digital identifiers. The most widely used is Uniform Resource Identifier (URI) and its internationalized version Internationalized Resource Identifier (IRI)—the standard for identifiers on the World Wide Web. OpenID and Light-weight Identity (LID) are two web authentication protocols that use standard HTTP URIs (often called URLs), for example. A Uniform Resource Name (URN) is a persistent, location-independent identifier assigned within the defined namespace.

- *Source: https://en.wikipedia.org/wiki/Digital_identity*

Electronic Identity (eID)
An electronic identity:

- is a means for the user to prove electronically that they are who they say they are and thus gain access to services;
- is presented in electronic environment;
  - can appear in a form of certificate, username or email address or phone number;
- preferably is associated with an electronic identity hardware token;
- ideally has a hard link back to digital identity.

Electronic Identity Token
A secure electronic identity token

- is a hardware device to be used during electronic transactions in order to provide for electronic identity verification process;
- provides for additional level of assurance;
- stores a set of private keys with corresponding public keys;
- carries at least functions of electronic authentication and digital signature creation.

Electronic Transaction

- Is between two or more parties
  - The parties can be anonymous (privacy is protected if only attributes / details associated with claims are shared). This may involve a coordination hub that removes metadata that would allow the identity provider to have knowledge of which service was being accessed.
  - The transaction could be indifferent to the identity of the parties involved, since it is atomic or trust and repudiation is not a concern
  - Trust is needed on the identity of the parties for legal recourse, reversal, or non-repudiation
  - Parties are entities - Persons, Businesses or Things
  - If the party is a Thing, it is then deemed acting on behalf of a Person or a Business
- A transaction is a multi-step interaction and each step could involve flow of data or instructions
- At a step level there is a need for trust on the parties and the data
- At a transaction level there is a need for trust on the parties, the data and factors such as eligibility and permissions
- Privacy and security principles of need to know, selective disclosure, access control, information security against snooping are needed

Foundational Identity System (fID System) (also referred to as legal identification system)
(Adjusted from WB ID4D, Practitioners Guide, Glossary, https://id4d.worldbank.org/guide/glossary)
An identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. Common types of foundational identification (ID) solutions include civil registries, universal resident or national ID systems, and population registers.

Typical capacities include::

- Provide recognition before the law and proof of legal identity.
- The name and nature of legal identification systems varies under national law, but typically includes civil registration systems, national identification systems, population registries, and other foundational identification systems.
- Maintains a registry of natural persons and provides issuance and lifecycle management of foundational identities.
- Those persons are people needing to interact with a country: citizens, diaspora, foreign residents, foreign workers, refugees, etc.
- Has an identity issuance and management process that takes care of accuracy of information in order to act as a reliable root of trust.
- Offers identity assurance in the form of identity verification in the digital realm.
- Digital identity and electronic identity serve as foundational level attributes.

Functional Identity
(Adapted from PRINCIPLES ON IDENTIFICATION, February 2021. Retrieved from: https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf)

- Is linked to systems which have a specific function with specific business rules: ie education, healthcare, justice, .. are functional domains which could establish and use functional Identities.
- Functional identification systems provide official proof of identity and authorization for particular purposes or sectors. This typically includes identification systems that provide voter identification, ration cards, social security numbers, health cards, tax numbers, and more; in some cases these credentials may also be recognized as proof of identity for other purposes or sectors.
- Historically functional identities are created in the absence of / as complements to foundational identities. In the presence of proper foundational eID, there is no further need for a separate functional eID.
- Is often associated with a credential that provides entitlements - a functional health identity card both provides identity services of a kind and entitles the holder to access health care services.

Functional Identity System
A functional identity system

- Maintains a registry of credentials.
- Associates the identity of a person with the entitlement that the functional credential offers.
- Optionally offers uniqueness based on the credential type.
- Optionally offers identity assurance based on the credential type.
- Optionally digital based on the credential type.

Identity Credential

- An identity document in a physical or digital form that an identity credential holder may present to authenticate his identity in a physical or electronic interaction;
- *Data, or the physical object upon which the data may reside, that an identity credential holder may present to authenticate his identity in an electronic or online transaction.*

Identity Registry

- An identity registry contains individuals identity information, it can be related to group or sub-groups (ie for a functional system, a region, a company)

Identity verification

- Offers mechanisms for verifying a person's identity locally or by hitting a service offering the verification capabilities
- Local verification involves trusting the source of the information by (for example) using digital signatures rather than having to go back to the root source of truth (and hence creating a privacy invasive audit record of the check)
- Identity verification services might be available in synchronous and asynchronous modes and might have real time or non real time responses
- Online identity verification uses a single or multi-factor mechanism. Identity verification involves an identifier and the factors. The identifier may be the UIN or an alias that is associated with the UIN in reference to the eID term described above..
- A foundational identity system can offer verification services in a centralized or multi-provider (federated/ distributed) model.
- In a federated model identity verification has to come from different sources based on the credential used. This means that there is a need for discovery, registration, resolution and routing of verification requests to the appropriate verification service. This needs a web of trust model to be defined. Such a model will also be repeatable for cross border usage where it will be dealing with a federation of foundational identity systems.

IDV BB

- Stands for Identity and Verification Building Block
- Building block specified in current documentation
- In charge to create, manage life cycle, audit mechanisms, and verify identities

Population registry

- A population registry is a database/system which includes records of the entire population of a country covering citizens but also foreigners staying in the country and also the national diaspora.

UIN

- Stands for Unique Identity Number, this number uniquely identifies a person in the Foundational ID system. UIN are an optional approach and not necessary.

4 Key Digital Functionalities

Identity systems can follow different approaches between centralized, federated or distributed identities.

- With the **Centralized Identity approach**, the identity is managed in a unique central place and offered as a service to the systems around. Foundational Identity follows a Centralized approach.

- With the **Federated Identity approach**, the identities are multiple and managed in different systems which are all trusted to ensure identity verification services. Federated systems may be functional systems which could include different characteristics of persons. This approach helps to leverage existing identity assets.
    - In a federated identity approach the IDV BB could:
    - act as an Identity Provider and expose authentication services via federation (see Open ID Connect Standards).
    - offer services for identity proofing to external Identity Providers via the Identity Verification services standardized interfaces.
- With the **Distributed identity approach** (also named decentralized or self-sovereign identity), the identity is owned and managed by the end person in a form of credentials (physical or digital) for which the owner is in full or as-needed control of its usage. This model if compared to centralized to federated presents lots of benefits in terms of privacy protection.

In each of these approaches trust in the identity and verification needs to be established. The centralized and federated approaches have organizations that provide trust through their ID proofing process but trust in the organizations themselves needs to be evaluated. Federated is an early form of decentralization and establishes a web of trust. If the same is extended to include relying parties and other service providers who participate in identity proofing, a distributed model is being created.

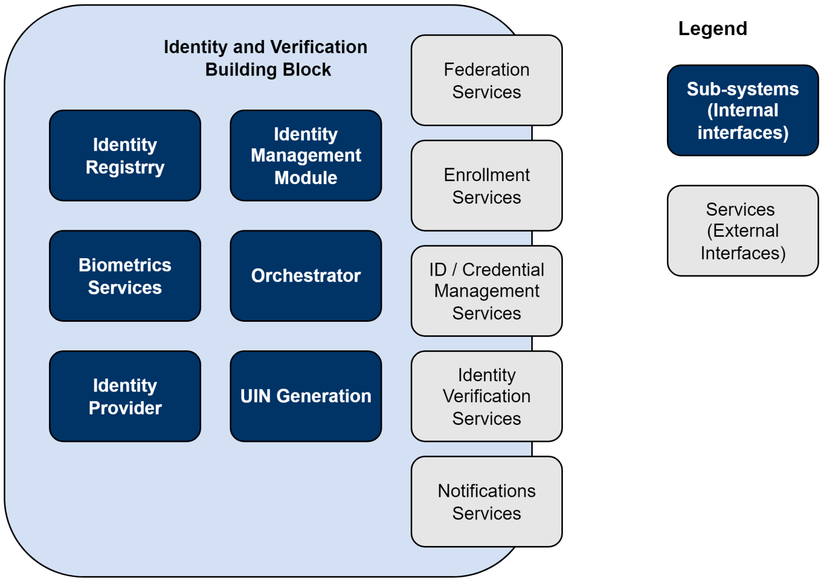
The concept of federated and distributed identity approaches are not covered in this first version and will be explained in more detail in the second interaction of this report.

Overall, this report advocates that regardless which approach is chosen, the data should always belong to the individual, but the level of control offered to them might vary based on features offered as well as the underlying needs. For example a population registry cannot "forget" a person and might not allow for that.

There is no one-fits-all solution and often a combination of those approaches enables most benefits.

4.1 Identity and Verification Building Block

The diagram below shows the high level view of the *IDV BB*.


Identity and Verification Building Block
Identity Registrry
Identity Management Module
Biometrics Services
Orchestrator
Identity Provider
UIN Generation
Federation Services
Enrollment Services
ID / Credential Management Services
Identity Verification Services
Notifications Services
Legend
Sub-systems (Internal interfaces)
Services (External Interfaces)

IDV BB offers 5 different external APIs:

Abstract

IDV BB offers a set of external services to the other building blocks

- **Federation services** are there to federate and harmonize multiple identities, which is creating a link in between various digital identities that an individual may have.

- **Enrollment Services** allow to on-board new identities for individuals, which means collecting its personal identity data, evidence of them, biometrics.

- **ID/Credential Management Services** permit to issue and manage the life cycle of Identity credentials, those services will allow to issue identity documents, to manage their renewal, declare them as stolen.

- **Identity Verification Services** allow a service provider to verify an identity or some of its attributes, for example checking a person declared identity or verifying its age.

- **Notification services** will allow a third party to subscribe to events occurring on identity and to receive notifications, useful to inform external functional building block when a person was born or has passed off so that the external system can take required actions.

Details of services

- **Enrollment services**
  - API to on-board new identities, this API is to be used by registration systems that may vary in their form and technologies, this API is there to receive the raw data in a predefined format.

  - The enrollment service will need to evaluate the identity related claims based on the registration data (e.g. differentiating between self-asserted or vouched for data in comparison to data coming from an authoritative source (such as a CRVS system). Depending on the context, some of this data (and meta-data) might need to be archived for audit purposes or to allow for repeated anti-fraud checks (e.g. data from an authoritative source was used but subsequently was reported lost / stolen). As this meta-data forms the basis of the resulting identity service, only identity-specific data needs to be stored in the live system, with meta-data being held separately (and under additional security controls).

  - Enrollment services may be designed to be permissive, i.e. allowing for enrollment based on partial / poor quality data dependent on the context.

  - Those data need to be traceable and auditable so they should come in with all evidence and capture contextual meta-data, but should not permit tracking of such without evidence of permission (declarative process)

- **Credential Management Services**
  - API to get access and update the credential associated to the identity, also manage issuance and life-cycle of credentials whatever physical or digital.

- **Identity and Verification Services**
  - API to offer identification services to the 3rd party players . Those services can be identity verification, attributes sharing or answers to claims (ie I claim I'm older than 18 years old) Usage can be multiple in public services, but also private, even cross-countries. They can be based on identity attributes : text, biometrics, also known documents and even on what people know (PIN code, Passport) or what they own (smartphone with SIM card)

- **Notifications services**
  - API allows to trigger external processes according to events happening on the identity data managed by the identity system (ie name change, death, new child born, document lost or stolen, ..) In order to preserve privacy and respect the principle of single source of truth, the notification should only mention an identity change event to a set of subscribers for them to be aware they may need to refresh a right or create a new record in their system (ie: a birth may generate change in households register of social security and or person reaching 60 may be allowed to retirement pension)

- **Federations services**
  - API allowing federation of identities from external identity providers. Indeed, individuals may already have an existing form of digital identity they need to keep using and would like to associate with their national identity. In that case the Federation services will be able to attach those forms of identity based on their identifier to their national identity managed by IDV BB, also to allow delegation to them of individual's authentication.

It includes internal sub-building blocks/ modules, notably:

- **Identity Registry** is a system storing and managing the identities. It contains and manages all the data that might need to be collected (according to local laws and regulations) including demographic (ie name), biographics (ie age), portrait, known identifiers, known documents and can offer consultation or management services on them. As the system must be auditable it must keep track of identity changes and keep evidence leading to those changes. Privacy and Data protection rules force us to carefully manage storage and access to data, by respecting specific data protection design rules (minimization, isolation, anonymization, ..) Generally speaking, countries apply privacy and data protection laws similar to European GDPR which impose to minimize data stored including in time and always performs informed consent of the individuals of their end usages. The registry should allow for portability of data from one solution to another. For this the registry should support open data formats as well as standards based data formats. This applies to biometric and biographic data. The module should also offer APIs for such data portability.

- **Identifier Management module**, managing identifiers assigned to identities. In case a Unique Identity Number (UIN) is used and is acting as 'primary key' of identity, it is recommended that such number does not contain any personally identifiable information and hence can be used and shared publicly. The UIN should also be non-revocable. There may also be a set of tokens or aliases identifiers to use the identity and, where required, to link to data in functional systems.

- **Biometric Services** which offer capacities to compare biometrics in between identities. Key use cases being 1:N search which consist in confirming unicity of a person by comparing its biometrics to all ones stored in the system, 1:1 search to confirm an identity by comparing biometrics data one to one. Those services may be asynchronous when an adjudication system is in place, an adjudication system being a human based decision workflow allowing operators to take decision on uniqueness or identities match based on candidates identified automatically by the biometric search system. *Centralized databases of biometrics can introduce significant privacy risks, see, for example, https://www.theguardian.com/global-development/2021/sep/07/the-taliban-are-showing-us-the-dangers-of-personal-data-falling-into-the-wrong-hands. Biometric services also provide standard interfaces for managing biometric data for operations on biometric data such as conversion, compression, templatization, matching, segmentation and more.*

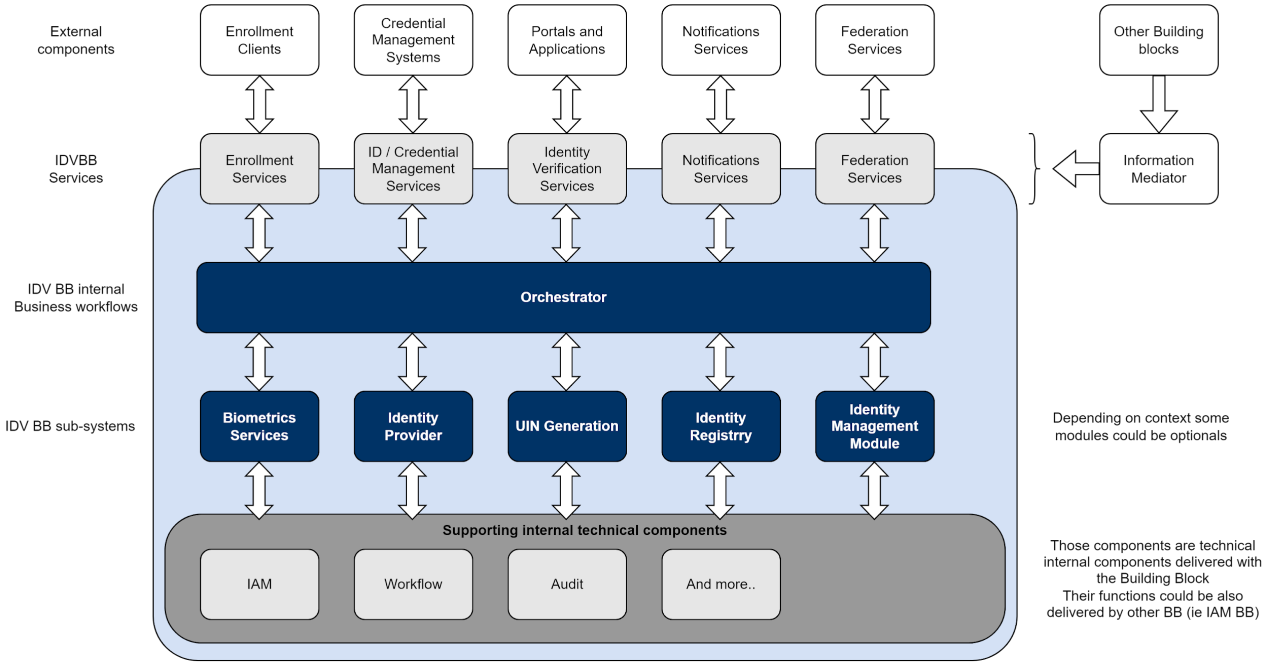
- **Orchestrator (optional but strongly recommended)** is often embedded in the Identity system in order to run the control steps and actions required to build an identity. It's recommended to use an internal workflow for that, which may lead to triggering an external workflow if, for example, required to launch additional actions after identity creation.

- **Identity Provider** can be part of IDV BB and provide reference identities for identity verification, it can be also optional when in a decentralized (or distributed) identity model.

- **UIN Generator**, allows to generate Unique Identity Numbers which are unique in the system. UIN Generator will follow predefined business rules for that generation and will make sure that a new generated number has never been already issued.

4.2 Identity System Components

The graphic below presents the overall view of the Identity System with its main components.


External components
Enrollment Clients
Credential Management Systems
Portals and Applications
Notifications Services
Federation Services
Other Building blocks
IDVBB Services
Enrollment Services
ID / Credential Management Services
Identity Verification Services
Notifications Services
Federation Services
Information Mediator
IDV BB internal Business workflows
Orchestrator
IDV BB sub-systems
Biometrics Services
Identity Provider
UIN Generation
Identity Registrry
Identity Management Module
Depending on context some modules could be optionals
Supporting internal technical components
IAM
Workflow
Audit
And more..
Those components are technical internal components delivered with the Building Block
Their functions could be also delivered by other BB (ie IAM BB)

4.2.1 Specificity of the Identity Registration System

Identity Registration system must be understood as different from a classical application registration system, as it establishes a person's foundational ID which is likely to act as a basis for their digital twin (digital twin is the equivalent of a physical real person in the digital realm) for all digital interactions and therefore will be of high importance for him/her as well as being highly attractive for hackers, demanding the highest level of security.

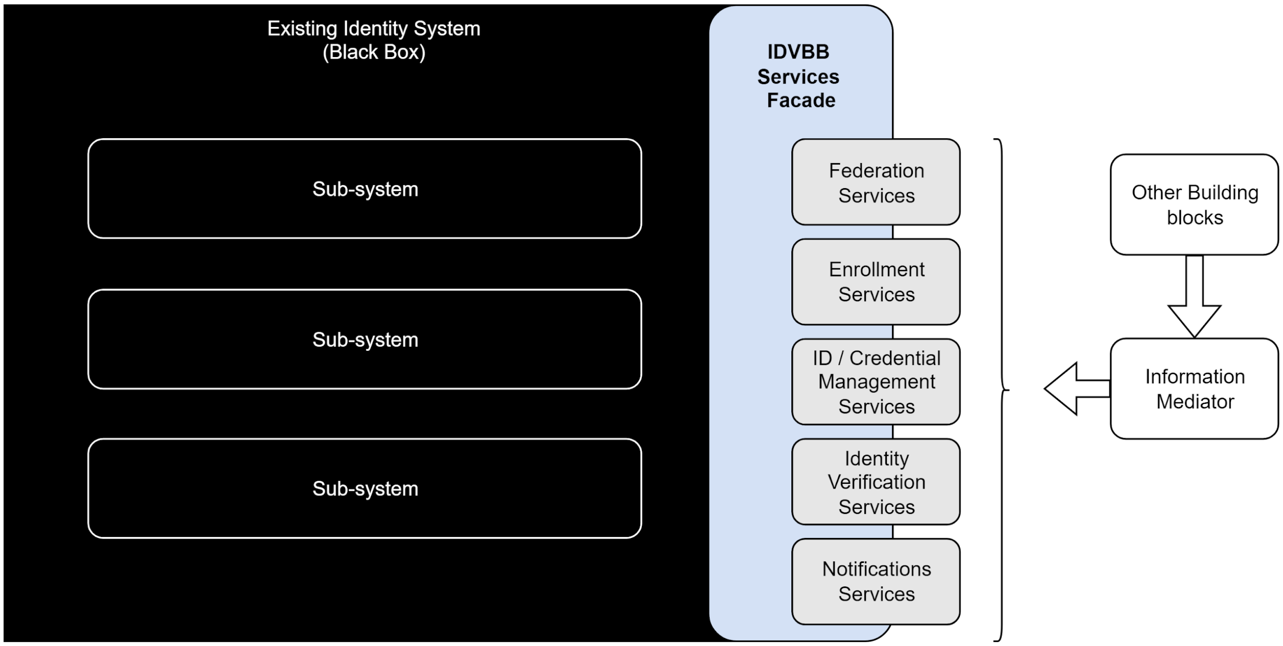
It might require secured biometrics and document capture capacities in order to limit the chance of fraud, although the use of biometrics is not recommended given the potential privacy implications. It can be compared at the entrance door of a secured site where security is particularly reinforced and the process takes necessary time to check all information, if compared to internal access control which can be lighter and based on short interactions. The Identity Registration system can be a single client Application, or web based application or even a client server application, it could be also online or offline.

If an identity registration client is confirmed to be an external building block it will most probably be more related to the Registration Building block. It must have its own APIs and own rules, tools and capture technologies compatible with the IDV BB OpenAPIs.

The client has to deal with secure interfacing; where biometrics is being used with biometrics capture devices, and performing some operations on the biometrics such as quality checks, liveness checks etc. These interfaces will be part of the biometric services. The data capture formats for biometrics will also have to be based on open standards to ensure compatibility and portability.

4.3 Integration with an Existing Identity System

It happens that some countries have an existing identity system they choose to reuse, like for example a National Population Register, a Civil Register or ID Document system. In that case the existing system will need to be equipped with the IDV BB Services Facade which will make its integration transparent toward the remainder of the GovStack.



5 Cross-Cutting Requirements

The following requirements should be added to other BB cross cutting requirements.

5.1 Consent Management

Whilst ID and Verification as defined and understood in this Building Block should be supported by local or supranational laws and regulations (like internal security or global AML rules), translation of the appropriate use in reality is complex and hardly enforceable. Hence, we recommend that any solution should have a defined consent management mechansîsm by design. The specifications for such mechanisms are out of scope for this Building Block, but should follow the following requirements:

1. Consent should be created in the context of the user and should be available to the user.

2. Take consideration of consent receipts (Greig, S. (2017). Kantara Initiative Releases the First Open, Global Consent Receipt Specification, Kantara (available at https://kantarainitiative.org/kantara-initiative-releases-first-open-global-consent-receipt-specification/)

3. Following the logic that a user is asked to give consent for a particular activity / data share. (Some other system is linking the user with the activity). Assuming that the overall system sends the consent request to the appropriate user then their response (I give consent) is stored and managed in the consent management BB or any other responsible party). If the user is a mother who does not yet have a registered identity they can still be the 'person' who is asked for their consent.

4. Address ownership of register and access questions: presumably the consent register is only held by the data controller who is acting on the basis of the consent.

5. Purpose limitation of the consent.

6. A request response approach or a link to a transaction ID and parties and date would also help.

7. An assisted model would also be required, where 3rd party agencies can come in to collect consent from the user.

8. Apart from technical requirements, it is helpful to differentiate between consent as an ethical process versus consent as a legal basis for processing personal data (certainly under GDPR).

5.2 Security Requirements

The Cross-cutting requirements described in this section are an extension of the cross-cutting requirements defined in the Security requirements. They can be found in the section 3.5 Digital ID/Certificate Functional Requirements:

Functional Requirement	**Type (Must/ Should/ May)**	**Build/ Deployment/ Both**
3.5.1 Enrollment Services Enrollment services for a digital ID in the form of a certificate using the physical credentials of the enrollee (a human citizen subject) and the process of the Identity BB (see the functional requirements for Identity in the Identity BB Definition). A feature for invalidating, locking or disenrollment/revocation of the digital ID shall also be provided as a response measure to both human citizen subjects leaving the system and responding to security breaches encountered. Digital certificate enrollment must be provided by the solution but is not required for every human citizen subject (see below). Note that it is anticipated that the Identity BB will call this feature either directly via API or indirectly via the IAM features of the Security BB for users electing to use an electronic ID consisting of certificates as a part of the account provisioning process. The digital ID will then be stored with the physical ID records in the	MUST	Build

identity BB and sent to the new user via secure means (probably installed on their device). Note that simple numerical digital IDs will also be supported for human citizen subjects as an option where users are unable to leverage certificates based digital ID. The requirements governing this are to be stipulated by the Identity BB (see the Identity BB Definition) . Note that 3rd party organization and internal subjects (both human and non-human) MUST be issued valid signed digital certificates in order to establish and maintain secure inter-organization and internal communications.		
3.5.2 Multi-Factor Authentication The overall solution suite shall also be able to implement multi-factor authentication using simple numeric digital IDs for human citizen subjects such as their tax file or social security number of the user. A selection of various alternatives for digital ID is required in order to cater for more or less digitally-savvy citizens. Various token types are also required to be optimally supported such as HOTP and TOTP tokens, SMS, email, push notifications, SSH keys, X.509 certificates, Yubikeys, Nitrokeys, U2F and WebAuthn. Vendors of solutions SHOULD articulate the benefits of what they propose in their solution. Note that multi-factor authentication must be able to be implemented for both external and internal subjects (people, systems, components etc.) but is not necessarily required for internal non-human subjects (such as building block components) as they communicate via the information mediator BB (see the InfoMed BB Definition).	MUST	Deployment
3.5.3 Numerical Digital ID Attribute Where human citizen subjects adopt the use of a simple numerical digital ID, the multi-factor authentication process MUST include a time-sensitive credential (AKA OTP or one time PIN)	MUST	Both

5.3 Trust Framework

Trust Frameworks can be considered a mechanism to enable the trusted exchange of information between sovereign partners. The Trust Framework is a much discussed concept and this report recommends including the specifications in the second iteration as a sub-Building Block whereby additional experts should be included.

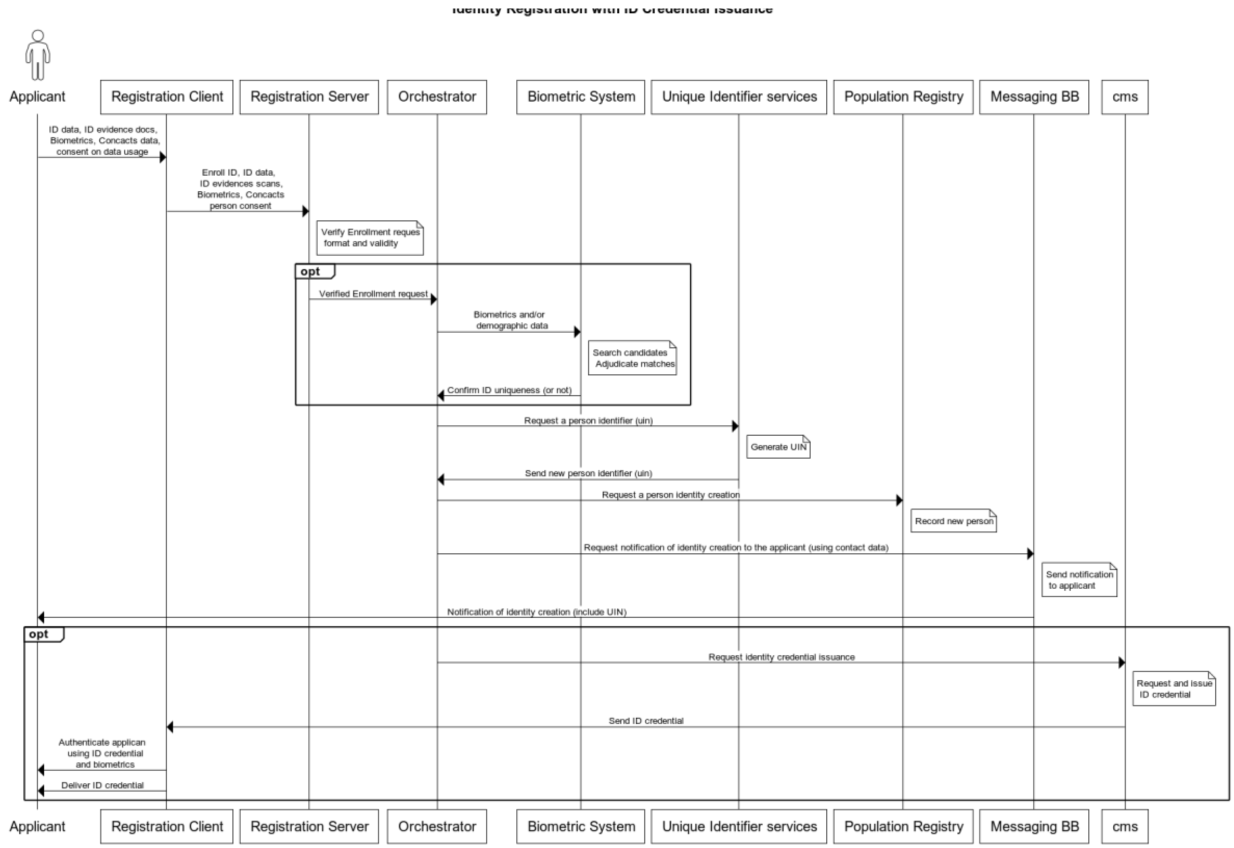
6 Functional Requirements

6.1 Identity Registration

The following UML sequence diagram shows a simple classical identity registration followed by issuance of an identity credential.

It could be detailed more around how the registration appointment is taken, how the data reaches the registration server, include creation of token identifiers, manage collection of person consent, determine options for format of the ID credential (physical or digital) and its sending back to the applicant..

Purpose of that diagram is to illustrate the key steps of the process and services involved.


Identity Registration with ID Credential Issuance
Applicant
Registration Client
Registration Server
Orchestrator
Biometric System
Unique Identifier services
Population Registry
Messaging BB
cms
ID data, ID evidence docs, Biometrics, Concacts data, consent on data usage
Enroll ID, ID data, ID evidences scans, Biometrics, Concacts person consent
Verify Enrollment reques format and validity
opt
Verified Enrollment request
Biometrics and/or demographic data
Search candidates Adjudicate matches
Confirm ID uniqueness (or not)
Request a person identifier (uin)
Generate UIN
Send new person identifier (uin)
Request a person identity creation
Record new person
Request notification of identity creation to the applicant (using contact data)
Send notification to applicant
Notification of identity creation (include UIN)
opt
Request identity credential issuance
Request and issue ID credential
Send ID credential
Authenticate applican using ID credential and biometrics
Deliver ID credential
Applicant
Registration Client
Registration Server
Orchestrator
Biometric System
Unique Identifier services
Population Registry
Messaging BB
cms

Edit diagram

6.2 Identity Verification

Identity verification can be performed in several ways and based on several inputs depending on various criteria.

For example, Identity verification will be performed according to:

- **Context of identity verification** : online, face to face by third party, self identity verification, in the absence of infrastructure and technologies.

- **Capacities given to the individual**: having an ID Card, a person Identifier, a password or PIN code, using its biometrics, mobile subscription or smartphone.

- **Status of the individual**: can he/she read ? Does he have usable fingerprints ? Is he/she old enough to have an ID Card?

- **Level of trust required**: according to sensitivity of the operations, level of assurance required, policies established by the state or by the service provider, multiple factor identity verification.

- **Business constraints**: does the use case require to be very fast, touchless, seamless, physical or digital

- **Local laws and regulations**: the identity verification could differ according to local regulations and laws which may indicate specific ways to perform identity verification.

6.2.1 Capabilities

Below shown table will list the different capabilities that can be used to perform an identity verification, the Identity & Verification Building Block may use any of them including combination of several of them to verify a person identity.

Capability	Description	Recommended Use	Level of Trust	Requirements for individual or for the Context of Use
Login/ Password	Previously given login/password are typed in a login form to verify person identity	For online access on web site or in mobile application	**Medium** (What you **KNOW** only)	Require the individual to have access to a digital device having network connectivity and sufficient power stability.
Visual physical identity credential identity control	National ID card provided to the individual includes security features allowing to verify the document is genuine	For fast verification in public place, or when there is no digital identity verification available or no	**Low** (What you **HAVE** only)	Having been issued and delivered a physical identity credential.

	and data printed on it allow to know the identity of the individual.	connectivity to network		
eID card identity data control	National ID card provided to the individual includes a chip in which its identity information is securely written allowing them to get them and make sure about their authenticity.	For identity verification in face to face control.	**Medium** (What you **HAVE** only)	Having been issued and delivered a physical identity credential with a chip (eID card), having access to a digital identity verification device. No need for network connectivity.
eID card based identity verification	National ID card provided to the individual includes a chip in which its identity information is securely written allowing them to get them and make sure about their authenticity. Those same data can be used for a match versus other information like who the person pretends to be, what is printed on the document or it's biometrics captured live.	For identity verification in face to face control.	**High** (What you **HAVE** and what you **ARE**)	Having been issued and delivered a physical identity credential with a chip (eID card), having access to a digital identity verification device which can perform a matching between person attributes and chip stored attributes.
Fingerprint 1:1 matching versus ID credential	The individual live capture fingerprint will be compared to its fingerprint(s) captured during its identity creation. Those original fingerprints being stored on or within its Identity credential.	For identity verification in face to face control or self-control of identity (ie airport eGates)	**High** (What you **ARE**)	Having been issued and delivered a physical identity credential including a digital ID into a chip (eID card) or in a cryptogram, having access to a digital identity verification device which can perform an ID Credential reading, fingerprint(s) capture and matching with attributes stored in ID credential.

Fingerprint 1:1 matching online	The individual live capture fingerprint will be compared to its fingerprint(s) captured during its identity creation. The fingerprints are verifiable using an online service.	For identity verification in face to face control or self-control of identity (ie airport eGates)	**High** (What you **ARE**)	Having been registered to a state recognized identity provider, having access to a connected digital identity verification device which can perform fingerprint(s) capture and access to online identity verification services.
Fingerprint recognition	The individual doesn't provide its identity, a search based on its fingerprints is performed against a database of known identities in order to identify him/her.	NOT RECOMMENDED FOR CIVIL USE. This capability is rather to be used for security purposes in criminal or border control systems or secured building access.	**High** (What you **ARE**)	Having been registered (or not) to a state recognized identity database, having access to a connected digital identity verification device which can perform fingerprint(s) capture and access to online identification services.
Facial 1:1 matching versus ID credential	The individual live face capture will be compared to its face captured during its identity creation. That original face capture may be stored on or within its Identity credential	For identity verification in face to face control or self-control of identity (ie airport eGates) A face liveness detection is recommended.	**High** (What you **ARE**)	Having been issued and delivered a physical identity credential including a digital ID into a chip (eID card) or in a cryptogram, having access to a digital identity verification device which can perform an ID Credential reading, face capture and matching with attributes stored in ID credential.

Facial 1:1 matching online	The individual live face capture will be compared to its face captured during its identity creation. The face is verifiable using an online service.	For identity verification in face to face control or self-control of identity (ie airport eGates) A face liveness detection is recommended.	**High** (What you **ARE**)	Having been registered to a state recognized identity provider, having access to a connected digital identity verification device which can perform face capture and access to online identity verification services.
Facial recognition	The individual doesn't provide its identity, a search based on its face is performed against a database of known identities in order to identify him/her.	NOT RECOMMENDED FOR CIVIL USE. This capability is rather to be used for security purposes in criminal or border control systems or secured building access.	**High** (What you **ARE**)	Having been registered (or not) to a state recognized identity database, having access to a connected digital identity verification device which can perform face capture and access to online identification services.
Iris 1:1 matching versus ID credential	The individual live iris captured will be compared to its iris captured during its identity creation. That original iris capture may be stored on or within its Identity credential	For identity verification in face to face control or self-control of identity (ie airport eGates) Liveness detection is recommended.	**High** (What you **ARE**)	Having been issued and delivered a physical identity credential including a digital ID into a chip (eID card) or in a cryptogram, having access to a digital identity verification device which can perform an ID Credential reading, iris capture and matching with attributes stored in ID credential.
Iris 1:1 matching online	The individual live iris capture will be compared to its iris captured during its identity creation. The iris is verifiable	For identity verification in face to face control or self-control of identity (ie airport eGates)	**High** (What you **ARE**)	Having been registered to a state recognized identity provider, having access to a connected digital

	using an online service.	Liveness detection is recommended.		identity verification device which can perform iris capture and access to online identity verification services.
Iris recognition	The individual doesn't provide its identity, a search based on its iris is performed against a database of known identities in order to identify him/her.	NOT RECOMMENDED FOR CIVIL USE. This capability is rather to be used for security purposes in criminal or border control systems or secured building access.	**High** (What you **ARE**)	Having been registered (or not) to a state recognized identity provider, having access to a connected digital identity verification device which can perform iris capture and access to online identification services.
OTP	The individual needs to type in a form (online or app) a One Time Password (OTP) received from the identity provider.	Can be used when needing to access an online service. To be used a second factor of authentication, for example with a login password)	**High** (What you **KNOW** and what you **HAVE**)	Having been registered to a state recognized identity provider, owning a mobile subscription, being in capacity to receive messages (SMS, messaging, email), having access to service provider online services. It is important to acknowledge different patterns of phone ownership (individual, household, community).
Online ID credential matching	The individual will authenticate versus himself its ID credential online. The process may include biometrics control versus data printed or stored in the Identity credential, together with genuity check of the document using security features and	Can be used to perform remote on-boarding of persons in services. To be noted it anyway required a face to face on-boarding to enroll for the Identity credential. Ensuring the document is genuine can be a	**High** (What you **HAVE**, what you **ARE**, what you **WERE**)	Owning an ID Credential registered for online services verification, having a connected smartphone eventually capable of reading a chip.

	eventually control of document authenticity versus database of issued documents.	challenge, unless an ID credential secured chip is involved as part of the process.		
Online PKI based identity verification	The individual uses its identity credential or a digital device to encrypt or sign identity verification data which can then be verified on server side. A PIN code is requested.	Can be used if ,and only if, a specific PKI infrastructure is in place to issue, read and verify online	**HIGH** (What I **HAVE**, what I **KNOW**)	The individual own an identity credential or a digital device storing personal cryptographic secrets
Behavior based identity verification	The individual is authenticated seamlessly based on its context and behavior following an evaluation of the risk he/she not be himself/herself.	To be used for very frequent access control (i.e. control of office workers) when security and convenience are both importants. Requires solid on-boarding before.	**MEDIUM** (What I **DO,** Where I **AM**)	Having been screened and tracked on normal habits, locations, behaviors to be used for evaluation of fraud risk Being online.
Token based identity verification (SSO)	The individual has already been authenticated to a third party system allowing him to avoid a new identity verification and reuse the token. This mechanism is also named Single Sign On (SSO)	To be used for online identity verification is usage of a digital identity	Depends on previous identity verification	Having been previously authenticated by a third party system and obtained a verifiable authentication token.
Verifiable Credential	The individual has shared a verifiable credential to a third party system which allows its identity verification.	Can be used in various contexts online/offline. Can be related to one or several attributes of Identity.	**High** (What you **HAVE**, what you **ARE**, what you **WERE**)	Require an electronic or physical support to verify the credential. If a verifiable credential can be verified offline, connectivity is required to verify the security chain.

Through this list of capabilities we can see there are numerous but limited options for Identity Verification that can be combined or not, this list allows us to normalize them all into the following inputs for an identity verification:

1. **Identifier**: identifier referring to a digital retrievable identity which can give access to an individual's attributes for verification. To be noted that several kinds of identifier could be used to refer to the same person, which is particularly important to preserve privacy (see glossary).

2. **Set of attributes**: attributes provided by the individual or retrieved on/within its Identity credential for purpose of a matching versus a reference (online or ID credential), those attributes can be biographic data, biometrics data or scan of identity evidence.

3. **Authentication token**: A previous identity verification token can be used for identity verification, this token would allow the current service provider to verify against the authenticating system the genuinity of the token.

6.3 Use Cases

6.3.1 Use Case 1: Identity Enrollment

Enrollment to a National Digital Identity is a sensible process as the created digital identity will be recognized by law and then consequence of its use.

In some countries, it's possible to enroll a National Digital Identity remotely based on an existing form of identity like for example an ID card. If they are convenient they open the risk for fraud or identity theft.

For all these reasons, it appears that an identity enrollment has to be rolled-out in a face to face proces, with collection of identity attributes being demographic, biometrics or related proof of them.

This process will be developed later, for now we can list its main steps for the face process::

1. Explanation of purpose of process and usage that will be made of data
2. Identity verification: process start by providing evidence of identity (birth certificate, or previous ID card, passport, ..)
3. Collection of demographic data (confirmed with evidences provided)
4. Collection of biometric data including
    a. Generally a portrait capture which will be used to visually recognize the person, for example printed on a ID card
    b. Sometimes fingerprints and iris are captured for identity deduplication purpose or for further biometric authentication
5. Scan of identity evidences to sustain the identity attributes certification
6. Collection of external identifiers (Birth ID number, Social security card number, ..) to establish links with external pre-existing forms of Identity
7. Verification of the data captured by the individual
8. Consent collection to launch registration process
9. Delivery of a registration number
10. In case Enrollment process be synchronous issuance and delivery of a unique identity number

These are only the steps visible by the individual and the process will pursue within IDV BB notably with following steps:

1. Packing and securing the data (signature & encryption)

2. Transport of data to identity registration system
3. Control of format and origin of data collected to ensure their authenticity
4. Control of eligibility criterias
    a. Could include biometrics unicity in case of centralized identity
    b. Could include additional checks like nationality, age, (but those ones are not recommended to ensure an inclusive system)
5. Generation of a Unique Identity number
6. Storage of identity data by respecting privacy by design principles
7. Communication of the Unique Identity Number to the individual
8. Eventual issuance of a physical or digital credential
9. Optionally notification of the systems around having subscribed to identity creation events (ie social security, health, finance, education, ..)

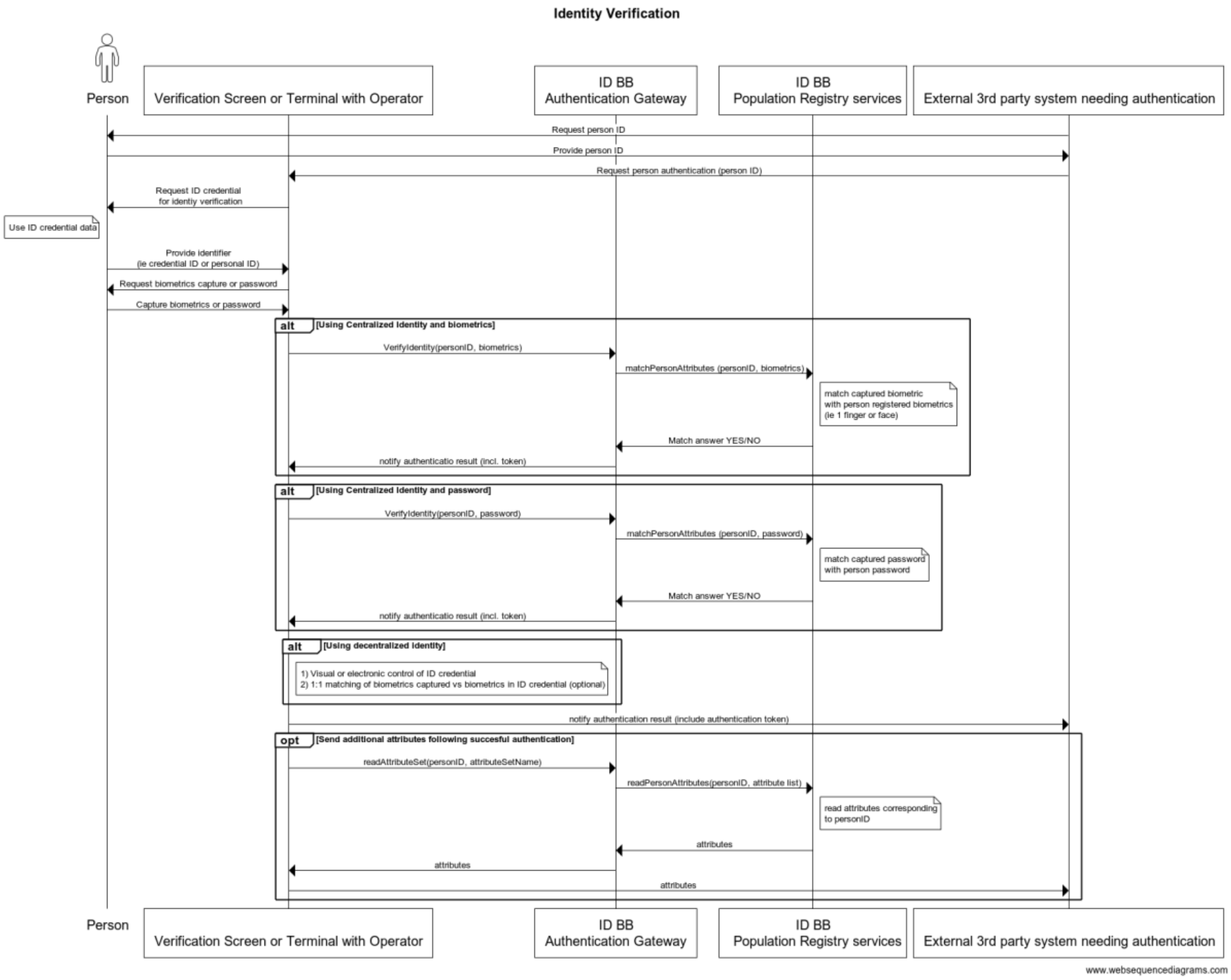
6.3.1 Use Case 2: Identity Verification Generic

The following diagram introduces what are the different steps, interactions and stakeholders of generic use cases of identity verification.

The possible inputs being what the capabilities just presented in the Capabilities section and the output being an authentication token.

It's to be noted that the identity verification is generally a stop point as part of an overall business process which is expecting to perform afterward

1. Control of authorization of the verified identity to access to some services
2. Eventually collection of some attributes related to the identity. After individual consent (managed with Consent Building Block) and under authorization of access to the requesting services provider.


Identity Verification
Person
Verification Screen or Terminal with Operator
ID BB
Authentication Gateway
ID BB
Population Registry services
External 3rd party system needing authentication
Request person ID
Provide person ID
Request person authentication (person ID)
Request ID credential
for identiy verification
Use ID credential data
Provide identifier
(ie credential ID or personal ID)
Request biometrics capture or password
Capture biometrics or password
alt
[Using Centralized Identity and biometrics]
VerifyIdentity(personID, biometrics)
matchPersonAttributes (personID, biometrics)
match captured biometric
with person registered biometrics
(ie 1 finger or face)
Match answer YES/NO
notify authenticatio result (incl. token)
alt
[Using Centralized Identity and password]
VerifyIdentity(personID, password)
matchPersonAttributes (personID, password)
match captured password
with person password
Match answer YES/NO
notify authenticatio result (incl. token)
alt
[Using decentralized Identity]
1) Visual or electronic control of ID credential
2) 1:1 matching of biometrics captured vs biometrics in ID credential (optional)
notify authentication result (include authentication token)
opt
[Send additional attributes following succesful authentication]
readAttributeSet(personID, attributeSetName)
readPersonAttributes(personID, attribute list)
read attributes corresponding
to personID
attributes
attributes
attributes
Person
Verification Screen or Terminal with Operator
ID BB
Authentication Gateway
ID BB
Population Registry services
External 3rd party system needing authentication
www.websequencediagrams.com

Edit diagram

6.3.2 Use case 3: Cross-Border Recognition of Professional Jobs

As regional member states' economies become more integrated, the need for cross-border recognition of professional jobs has increased. There is a desire to boost intra-African trade and the African Continental Free Trade Agreement (AfCFTA) seeks to create an integrated market of 1.7 billion consumers by 2030 with an aggregated GDP of up to US$3.4 trillion[1].

Services are an essential part of integration efforts, as recognized by governments in the context of the African Continental Free Trade Agreement (Mohamed, 2020). Trade in services can help economies achieve more rapid growth, enhance domestic firms' competitiveness, and promote inclusiveness in terms of skills, gender and the location of economic activity. Trade in services also promotes a more efficient allocation of resources and greater economies of scale. It can lead to an increase in the variety of services available to consumers and producers. Beyond these usual sources of gains, some services sectors have special or unique features that may amplify how an economy

[1] United Nations Conference on Trade and Development. 2019. East African Community Regional Integration: Trade and Gender Implications. [online] Available at: https://unctad.org/system/files/official-document/ditc2017d2_en.pdf [Accessed 6 July 2021].

can benefit from trade in services. In focus here, services sectors have an outsized impact on factors of production, like labour. For example, the productivity of an economy's labour force depends on how educated, skilled and healthy it is, attributes which hinge crucially on the quality of that economy's educational and health systems, as well as the ability to enable cross border exchange of labour[2].

This use case examines the recognition of high-skilled jobs.

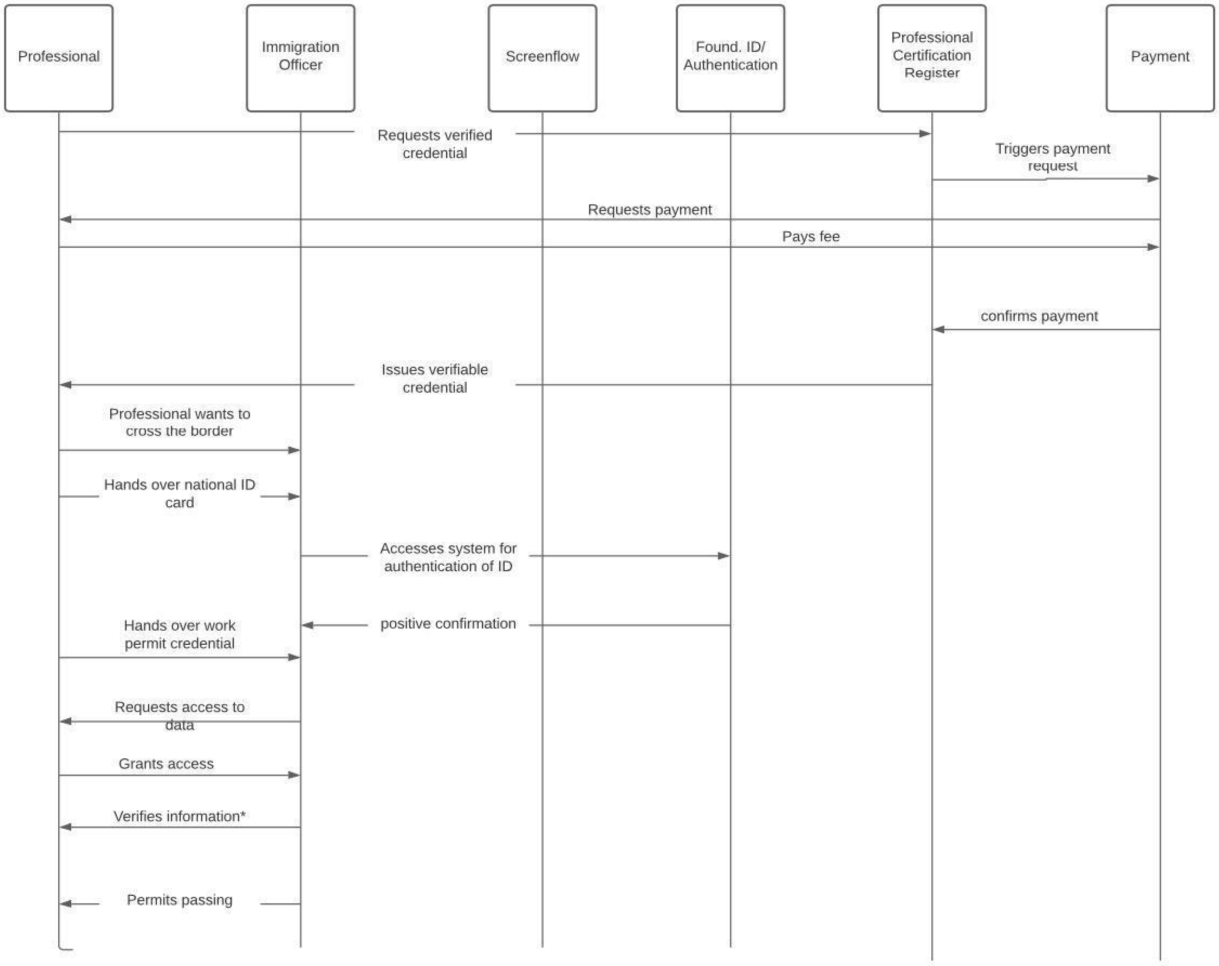
Title	Cross-border recognition of professional jobs as promoted by a regional mutual recognition agreement, focusing on the verification of the professionals' credentials to enable the crossing at the border.
Description	Facilitate the free movement of certified professionals by streamlining and digitizing the verification processes for cross-border work permits. In this case, the professional will provide the credential of the work permit (a card, barcode or other credential) and the national digital ID credential. The national digital ID will be verified through biometrics. The work permit is a verifiable credential, issued by the certifying authority and verified by the border control officer. (See verifiable credential as defined by open standard developed in the W3C)
Trigger	Individual travels to border intending to cross for work purposes and provides their work permit credential and national digital ID

[2] WTO, 2019. World Trade Report 2019: The future of services trade, Executive Summary. [online] Available at: https://www.wto.org/english/res_e/booksp_e/executive_summary_world_trade_report19_e.pdf

Preconditions	**Requirements (will vary per country and profession and are only examples):** ● Bachelor's degree in the respective profession. ● Diploma in the respective profession, successful completion of Certification professional course. ● Practicing certificate awarded by the Institute of Certified Professionals body (will existing for each profession) ● Successful application for a job in a neighboring country ● Received a valid work permit and a credential that can be verified by the border control officer **Professional Certificating Register:** ● Training institutes from involved countries collect information about their trained professionals that have successfully finished the training and received a diploma/ degree at their institute. ● National Institutes of Certification collects information about professionals that have successfully finished the certified exam and received the certification. ● Establish a regional agreement allowing the sharing of data of professionals for the purpose of transparency and ease of verification. ● Establish data access rules based on a clear need-to-know basis, including consent management for the professional every time the data is being accessed.
Data Input	● The national training institutes capture information about professionals (according to local laws) that successfully finish the education and receive a diploma/ degree at their institute. ● The National Institutes of Certification collects information about professionals that have successfully finished the certified exam and received the certification. ● To achieve a regional technical architecture that facilitates the movement for professionals, there is a need for a regional information exchange that is based on the respective professional bodies (professional certification register). ● This register should indicate: full name, registration number, year of registration, category (profession), practicing status, Continuous Professional Development points earned per annum (this data is for illustration purpose only and needs to be developed with each country).

Actors	Employee, in possession of: ● A professional education verification ● A national digital ID ● Professional certification card Professional Certification Register (central or federated): ● Managed by a regional agreement and in compliance with the national legal and regulatory requirements ● Has an API function and can be queried. Certification credential (verified credential): ● Necessary information for authentication purposes made available by the data subject to those with authorization from the relevant regional body. (Incl. offline capacity) Border control: ● The border control officer validates the individual's identity and purpose for crossing through the digital ID and certification credential.
Action Course	1. A professional with a job contract wants to cross border. 2. Their national ID facilitates their smooth movement across the border as an individual. 3. Their professional certification credential provides information to prove that they have a work permit. 4. The border control authority has permission to verify the validity of their national ID as well as ask for verification of the work permit. 5. Successful border crossing. 6. Professional will practice in the host country as per the domestic laws.
Alternate use*	Two countries have a mutual recognition of both IDs and certification, free movement of labor occurs without the need for a work permit. The validation takes place with a paper-based work permit. The validation takes place against a paper-based passport.

Data output	Motivate professionals to register and be certified so they can take advantage of cross border work opportunities. Increased research and analysis capacity (e.g., how many certified professionals are crossing the border and benefitting from the advantages)
Post conditions	A streamlined certification and registration process resulting in a higher number of registered professionals that benefit from a larger market access and a decrease in unregistered (quacks) operating across the region


Professional
Immigration Officer
Screenflow
Found. ID/ Authentication
Professional Certification Register
Payment
Requests verified credential
Triggers payment request
Requests payment
Pays fee
confirms payment
Issues verifiable credential
Professional wants to cross the border
Hands over national ID card
Accesses system for authentication of ID
positive confirmation
Hands over work permit credential
Requests access to data
Grants access
Verifies information*
Permits passing

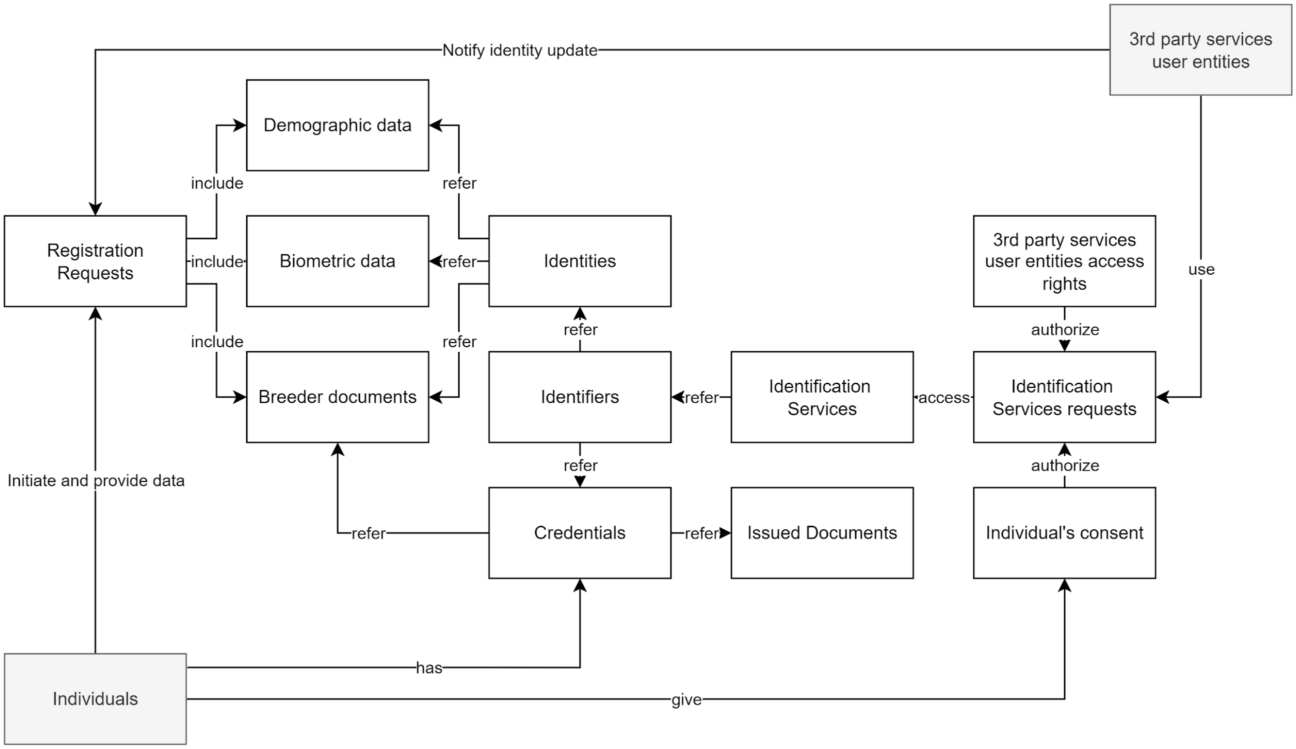
*This includes two verification steps: 1. manually authenticate owner through match of name , 2. verify validity of card (electronically)

7 Data Structures

IDV BB requires data objects, below are the main ones involved listed:

- **Identities** of individual identified by a unique identifiers
- **Identifiers**:
    - Token number associated uniquely to a set of data, identifiers are used to refer to those data without having to actually copying them
    - They can be stored then in separate repositories with specific restricted access.
    - Identifiers can be used to uniquely identify Foundational ID or Functional IDs.
    - Token identifiers can be used to avoid data aggregation and ensure capacity to forget an identity.
    - As identity data should be stored in different storage to ensure privacy protection allowing then data separation and data minimization principles, it's necessary to use different identifiers for different types of data.
- **Credentials**:
    - Issued for individuals or presented by them, ID Credentials related to an individual should be traced and accessible in the system in order to have capacity to identify fraud and do investigation on them, so has performing auditing.
- **Registration requests**
    - Requests will be received by the IDV BB, for example identity enrollment request or identity data update registration request, those requests will be then managed by the different subsystems and the workflows of IDV BB.
- **Identification Services**
    - A set of services will be offered on top of identities to identify a person, check some of his/her attributes (ie age) or obtain some certified personal information when needed and authorized.
- **3rd parties services user entities**
    - External entities which could be GovStack building blocks or not, will have access and use the services, for that purpose their access will be granted, consent may be given by the individuals and their activities will be logged.

Schema below shows their interactions and bring more details on involved data objects



8 APIs and Services

The following **external** APIs must be implemented by the *Identity & Verification* building blocks:

- **Enrollment Services** : Registration of Identity and applications services
- **ID Usage (Identity Verification)** : Identity verification Services
- **Credential Services** : Issuance and management of identity credentials
- **Notifications**: Subscription and notifications of event

The following **internal** APIs could be implemented by the *Identity & Verification* building blocks:

- **Data Access**: Access and management of identity data
- **Biometrics**: Interoperability API for ABIS systems, Interoperability with devices, operations on biometric data (Segmentation, Quality Check, Templatization, Format Conversion, Matching, Liveness Check, Compression, Attribute Annotation)
- **Population Registry services** : Access and management of persons in Population registry
- **UIN Management**: Generation of Unique Identity Numbers
- **Data Portability**: The ability to migrate from one implementation of Identity and Verification Building Block to another. The identity data and associated transaction history should be portable.

8.1 External APIs

8.1.1 Enrollment API

The Enrollment APIs are a set of OpenAPI specifications exposed by the Identity and Verification Building Block (IBB) ‘Enrollment Server’ service to any enrollment client.

The Enrollment APIs are based on the following principles:

- When enrollment is done in one step, the CreateEnrollment can contain all the data and an additional flag (finalize) to indicate all data was collected.
- During the process, enrollment structure can be updated. Only the data that changed needs to be transferred. Data not included is left unchanged on the server. In the following example, the biographic data is not changed.
- Images can be passed by value or reference.
- Existing standards are used whenever possible, for instance preferred image format for biometric data is **ISO-19794**. The underlying data should be of open mime types that offer good compression without loss of data (for example JPEG2000 for images).

Any implementation of the Identity and Verification building block must support these Enrollment APIs documented at this site: link to GovStack API portal.

The API definition file can be found here:

- Technical description
- Yaml file

8.1.2 Identity Verification API

The Identity verification API is an OpenAPI specification exposed by the Identity and Verification Building Block (IDV BB) ‘Identity Verification’ service to relying parties. The scope of the API is to allow the verification of an Identity credential and a set of identity attributes. Verification is strictly matching all provided identity attributes to compute the global Boolean matching result.

This service brings:

- the ability to use multiple identity verification factors
- security features:
  - verification and response can be bound to one transaction,
  - verification factor data can be signed and encrypted,
  - requests can be checked for integrity.
- privacy features:
  - the consent on usage of its data of the citizen/user can be provided,
  - selective disclosure of attributes based on authorization given for the use case to the relying party.
  - Supports tokenization of the response by including a pseudonymous customer reference (Token ID).

Any implementation of the Identity and Verification Building Block must support the identity verification APIs documented at this site: GovStack API portal

The API definition file can be found here:

- Technical description
- Yaml file

8.2 Building Block API Requirements

This section lists the GovStack Identity & Verification building block high level and generic requirements to be followed by the candidate implementations of Building Blocks.

Those requirements are there to guide the building block implementers in making their components match the needs of the GovStacks. We aim here to be specific enough in the requirements to allow a seamless integration of the candidate building block in the GovStack and at same time to keep latitude for the diversity of needs of countries, including for the resources constrained environments.

For each of them it is indicated if the requirement is Mandatory (M), Recommend (R) or Specific (S)

- To be recognized by GovStack, each building block will have to implement at minimum 'Mandatory' requirements.
- A 1 to 5 stars score will be established for the building block according to the ratio of 'Recommended' requirements implemented.
- 'Specific' requirements are generally required as mandatory by part of countries
  - They open the building block to diversity of needs, context and legacy in countries and are important for allowing the building block to match needs in some countries or regions.
  - Those requirements must be carefully considered by the Building Block providers (ie biometrics uniqueness, unique identifiers, ID cards with chip are mandatory in some regions and are not used in others)
  - In a further step this specification could attempt to define specific groups corresponding to countries having common constraints and needs, bringing to specific set of requirements (S1, S2, S3, ..)

Requirements have been grouped in domains for facilitating their use and evaluation.

8.2.1 Enrollment Services API Requirements

Name	Name/Description	M/R/S
Gov Stack recommended Open Standard Enrollment API	IDV BB must offer an API to Enroll persons following a Gov Stack recommended Open Standard API	M
One step Enrollment	IDV BB must offer capacity to perform an enrollment in one step	M
Multiple steps Enrollment	IDV BB must offer capacity to perform an enrollment in multiple steps (ie pre-enrollment and enrollment)	R
Enrollment management	IDV BB must offer capacity to search, retrieve and update and enrollment made (if it has not been committed yet)	S
Enrollment integrity	IDV BB must allow to control integrity and origin of an enrollment request by implementing enrollment meta-data about the context and actors of the enrollment, such as signature of data to ensure integrity. To ensure the integrity of the enrollment process, the BB must be able to implement technical controls so that only approved enrollment services can engage with the enrollment service. Cryptographic trust should be implemented.	M
Enrollment data encryption	IDV BB must support receiving encrypted data to ensure privacy protection and prevent data theft.	M
Offline Enrollment	IDV BB must offer capacity to perform an enrollment offline which means not expecting interactions in between registration client and server during the enrollment process, data being uploaded as a whole packet	S
Enrollment traceability identifiers	IDV BB must keep track of the enrollment request identifiers within its internal management in order to facilitate traceability and troubleshooting	R

8.2.2 Verification Services API Requirements

Name	Name/Description	M/R/S
Gov Stack recommended Open Standard Identity Verification API	IDV BB must offer an API to verify Identities following a Gov Stack recommended Open Standard API	M

Verify Identity (Authenticate)	IDV BB must offer an API to Verify Identity of an individual based on one of its known identifiers and or more of his attributes.	M
Identity Attributes sharing	IDV BB must offer an API to retrieve personal attributes of an individual from one of its identifiers. To be noted that this service will be subject to preliminary access granted by the system and by the individual (informed consent). Authorized access control should be part of API as opposed to external configuration alone. This ensures that relying parties are verified by the API before sharing sensitive data.	M
Identification of an individual	IDV BB must offer an API to identify an unknown individual, which means retrieve an identity identifier from a set of personal attributes sent. This service is normally to be used for security/law enforcement purposes and must be limited to registries of wanted people. For privacy and security reasons, this feature should only be considered where clear and accountable security/law enforcement rules are in place.	S
Claim a characteristic	IDV BB must offer an API to verify one characteristic of an individual without having to disclose actually the recorded related attributes. Typical request response is Yes or No (sample use case: age verification, is person older than 18 > Yes to No)	R
Identity Verification capabilities	IDV BB must offer Identity Verification services based on capabilities listed in present document (TBD developed more, include the different capabilities, all optionals) following a Gov Stack recommended ORen Standard API	S

8.2.3 Credential Management Services API Requirements

This section introduces the requirements regarding the Credential Management Services API which will allow BB users to request issuance, manage, share and get status of ID Credentials.

Name	**Name/Description**	**M/R/S**
Gov Stack recommended Open Standard Credential Management API	IDV BB must offer an API Standard to request issuance, get status and manage Identity Credentials, following a Gov Stack recommended Open Standard API	M
Credential Life Cycle Management	IDV BB must offer an API to manage the full life cycle of credentials related to an identity in an issuing system. The related credential must keep a strong and verifiable link with the individual identity and with the issuer.	M

Digital Credential	IDV BB API must manage Digital Credentials	R
Physical Digital	IDV BB API must manage Physical Credentials	S
Credential Issuance	IDV BB must offer an API allowing to request an identity credential issuance to a 3rd party credential management system.	M
Data for Credential issuance	IDV BB must offer APIs to either push data for credential issuance in an issuance request or to be requested by the issuing system.	M
Credential Renewal	IDV BB must offer an API allowing to issue a similar credential to the one already issued before based on the credential ID number.	S
Credential Revocation	IDV BB must offer an API allowing to revoke an issued ID credential. This will be used, for example, when a document is damaged, stolen or definitely lost.	M
Credential Temporary Suspension	IDV BB must offer an API allowing to temporarily suspend then un-suspend an issued ID credential. This will be used to disable an ID credential which has been lost, it's holder suspending it the time to search for it. After retrieval the document should be unsuspended and usable again. If not retrieved after some time, the document should be revoked. An API must be also available to check suspension status of a document.	S
Credential status request	IDV BB must offer an API to request status of ID credentials. Status being related to their production, their delivery or their activation status.	R
Credential Search	IDV BB can offer an API to search for ID credentials using some of its attributes. The output must be restricted to being a document number which can facilitate an access request only. No information can be shared directly.	S
Credential Retrieval	IDV BB must offer an API to retrieve a new copy of an ID credential already issued in case the current document has expired. The copy may be received through electronic way if being digital or delivered physically in case of a physical ID document.	S
Credential Download	IDV BB must offer an API to download a newly generated digital ID credential	S
Credential Sharing	IDV BB must offer an API to share to a 3rd party a Digital ID Credential.	S

8.2.4 Notification Services API Requirements

Name	Name/Description	M/R/S
Gov Stack recommended Open Standard Notification API	IDV BB must offer an API for notifying change on identity to subscribed external Building Blocks, following a Gov Stack recommended Open Standard API	R

8.2.5 Security and Access Control Requirements

Name	Name/Description	M/R/S
Unauthorized users	MIDV BB must prevent any user unauthorized system or user to get access to data	M
Registered users	IDV BB must offer identity verification services only to registered system or users	R
Granted access	IDV BB must offer capacity to grant access to specific verification services for specific or all individuals that are data subjects and hence owners of that data..	S
Individual consent	IDV BB must offer identity verification services only with preliminary informed consent on personal data usage of the concerned individual	R
Data Security	IDV BB must respect principles of data security by design in order to maximize protection against hackers: data encryption, data isolation, data separation, data anonymization, data minimization	R
System Security	IDV BB systems must implement security best practices in order to ensure the Identities it manages can be trusted.	M

8.2.6 Privacy Protection Requirements

Name	Name/Description	M/R/S
Sharing unnecessary information	IDV BB must not disclose any personal unnecessary information as part of its services API, and when possible prefer Yes/No answer rather than sharing attributes. All Sensitive Personal Information / Personally Identifiable Information must not be written to logs / reporting databases.	R

8.2.7 Identity Management Requirements

Name	Name/Description	M/R/S

Enrollment of Identity	IDV BB must allow to enroll an identity in one or several steps following a Gov Stack compliant Open Standard API	M
Update of Identity attribute	IDV BB must off APIs to update attributes of identities and to attach a legal evidence of that identity change approval (often delivered by justice)	M
Request for Identity Credential	IDV BB must allow to trigger issuance of an Identity credential	R
Revoke Identity Credential	IDV BB must allow to disable an Identity credential in case it has been lost or stolen. This can apply to physical or digital credentials.	R
Get Status of Identity credential	IDV BB must offer a set of services for checking status of an Identity credential for use of its owner or for a side system. Objectives being mainly to know if it has been issued or not, if has been disabled (lost/stolen), if its genuine or has been modified by a fraudster	S

8.2.8 Identifiers Management Requirements

Name	Name/Description	M/R/S
At least one identifier per identity	IDV BB must assign at least identifier and possibly several identifiers to each identity allowing to use it/them when requesting services on that identity	M

8.2.9 Identity Uniqueness Requirements

Name	Name/Description	M/R/S
Unique identity	An identity must be unique as part of the IDV BB, this unicity can be established based on identity attributes such like biometrics when available or biographic data.	R

8.2.10 Auditability Requirements

Name	Name/Description	M/R/S
Auditable history	A history of change for any identity must be retrievable and auditable by authorized users to investigate suspicious cases.	R

*O/R/M: Optional/Recommendation/Mandatory

9 Workflows

If GovStack will offer global workflow management for cross-building block use cases, IDV BB will have its internal workflows for its own internal business flows execution.

Non exhaustive list of example :

- For on-boarding a new individual
- For managing identity changes after an event on a person's identity (name change, death, ..)
- For life cycle management of individuals identity evidence (ie ID Cards)
- For management of access rights to services on individuals data.

Those workflows will be described in later version, but some of them are already available as flow diagrams in this document (see Use Cases section)

10 Other Resources

The results presented here benefit from publicly available sources that are referenced here. This report is recommending the use of open standards throughout any implementation. For this purpose, the team is suggesting the following already available and recognized open standard providers:

- APIs: OSIA: https://osia.readthedocs.io/en/latest/
- Federation protocol: Open ID Connect https://openid.net/developers/specs/
- Image format for biometric data: ISO-19794 https://www.iso.org/search.html?q=ISO%2019794
- Verifiable credentials (to be covered in the next iteration of this document in more details): W3C https://www.w3.org/TR/vc-data-model/
- ISO/IEC 24760

Equally, a future implementor might look for open source options for the modules introduced in this document. In this case, the team is suggesting:

- Modular Open Source Identity Platform (MOSIP): github.com/mosip, which also includes information about their APIs: MOSIP: https://docs.mosip.io/platform/apis

11 Key Decision Log

11. 1 Out of Scope

1. Recommendation to add a comment on general use of UIN across Europe
    a. Rational: the BB had many discussions on the use and applicability of UINs. Outcome was that not everyone was convinced that an UIN is the best approach and concerns about privacy and security were raised that were accepted by all participants.
2. General recommendation to visualize how this BB is embedded in the whole GovStack approach.
    a. Rational: This is not something that is being done at the level of each BB but for GovStack at large. Please consult the GovStack management for such an overview which was done previously.

11.2 Next Phase

1. Development of internal workflow
2. Definition of internal APIs which will address the question of domain allocation as well.
3. Implement SMART requirements to have easy identification and assessment for BB procurement purposes..

11.3 Adjusted

1. Formatting changes to introduction
2. Added Version History
3. Index was added
4. Clarifying 'Description' by removing text from 'Introduction'
5. Alignment of Glossary to
    a. added sources where applicable
    b. sorted by alphabetical order
    c. added definition of 'credentials'
    d. added definition of 'digital identifier'
6. Added Cross-cutting requirements section with content from Security BB.
7. In section 'Key Digital Functionalities', a clarification of the three approaches (centralized, federated, distributed) was provided
8. Throughout the document, terminology of identity and verification was aligned to be uniform with either identity and verification BB or IDV BB
9. The diagram depicted five APIs and five "internal sub-building blocks/ modules" which were explained. However, the sixth module "UIN Generator" was missing and adjusted now.
10. Typing mistake on page 10 'Enrolment Service' was corrected.
11. Section 4.1 'Identity and Verification Building Block' - added more content to the module 'Federation Services'
12. Correction of title Design sub-section: "View as a component of an Identity System" to '4.2 Identity System Components'
13. Adjustment of diagram in that sub-section:
    a. to be color-coded as "gray coloured boxes" and the internal sub-building blocks/ modules as "black coloured boxes")

    b. general adjustment of the diagram to show all components including Federation Service

14. Adjustment of diagram in section 4.3 'Integration with an existing Identity system' to be clearer and to add the module 'Federation Services'
15. Formatting: Removed a 'Summary Box' that contained no information
16. Use Cases:
    a. added the generic use case of 'Identity Enrolment'. This use case is also covered in the previous section of Functional Requirements since it does not require any other BB to interact with. Nevertheless, the request to complete the use cases in addition to the 'identity verification' and 'cross-border recognition of professional jobs' made sense and was incorporated.
    b. added more context and introduction to use case 2.
17. The section '8.2 Building Blocks Requirements' was renamed to 'Building Blocks API Requirements'
18. All subsequent subsections to 8.2 'Building Blocks API Requirements' have been renamed to include API to maintain uniformity and common naming.
19. "Notification Services API Requirements' amended with content.
20. To maintain uniformity with the abbreviations used at the beginning of the section Building Block Requirements , the "O for Optional" in "*O/R/M: Optional/Recommendation/Mandatory" mentioned at the end of the Requirements was replaced by "S for Specific".
21. Added section and content 'Workflow'.
22. '10. Other Resources' ISO/IEC reference as added
23. Added section '7. Data Structures'

12 Future Considerations

The following themes will be covered in future version of that document:

- **Identity Credential** management and Interoperability
- **Notifications** on identity change event (Subscription and Publication event based mechanisms)
- **Distributed/ decentralized/ SSI**
- **Trust frameworks**