Programme des Nations Unies pour le développement

-

TOR DIGITAL IDENTITY PILOT IN MAURITANIA

Version: 12 June 2022

CONTENTS

Background

Mauritania is determined to accelerate its efforts in the field of digital transition to improve the quality and accessibility of public services. In this context, the government has developed the "Digital Agenda 2022 - 2025". The *Agenda* describes how the Mauritanian government is committed to developing its e-government services in order to achieve:

- Inclusive access to government services for all citizens and residents: Ensure that all citizens and residents of Mauritania - including the most vulnerable - benefit from effective government services.
- Economic growth: Reduce the cost of doing business to increase GDP growth and individual well-being.
- Efficiency gains: Governments and citizens/residents can save time and money.
- Enhanced cybersecurity and integrity: Reduce the risk of fraud in digital transactions. Traceability reduces the risk of corruption.

A secure, user-friendly, and privacy-preserving digital identity is a necessary precondition for eGovernment services, as it enables trusted interactions between citizens, government authorities and the private sector. This need is recognised in the Digital Agenda 2022-2025, the 10 quick wins identified by MTNIMA and the results of the joint UNDP-MTNIMA Digital Readiness Assessment 2021.

Objectives

The pilot seeks to achieve the following high-level objectives:

Functional objectives

1. **Identity verification (identity proofing) with auto-ident process**
   - Following NIST identity proofing process (resolution, validation, verification)
   - Testing face-match (ID photo vs. face) and livness check: reliability
2. **Authentication with future citizen services portal**
   - OpenID Connect flows, including QR-code scanning
   - Separating IdP/ authentication server from Agency managing civil registry (double blindness principle)

Non-functional objectives

1. **Management of an open source / digital public good solution**
   - Prevents premature selection of a specific supplier/technical solution
   - Allows all interested parties to consider the solution (building trust).
2. **Evaluate governance models for future digital identity**
   - Identify the main security and personal data/privacy protection challenges and ensure that they are properly addressed by the appropriate legislation and architecture of the "production" solution.
   - Distribution of roles between ecosystem actors: Identify and mobilize key stakeholders (government administration, parliament, private sector, civil society) and foster support for the adoption of digital identity legislation and the mobilization of the necessary funds.
3. **Evaluate possible architectures of the future digital identity**
   - Test and validate key elements of the future digital identity solution/architecture: 'interoperability with existing IT infrastructure (upstream: e.g., ANRPTS population database / downstream: e-government portal under development by Ministry of Digital Transformation). Identifying and correcting problems in the pilot phase is probably 10x cheaper than in the production phase.

Current status

Foundational identity: Civil registry

Population register (ANRPTS)

- Mauritania already has a basic prerequisite: a well-established civil register (IDEMIA solution). Since 2010, the National Agency for Population Registration and Security Documents (ANRPTS) has been carrying out the biometric enrolment of Mauritanian citizens and managing the corresponding database.
- Currently, around 80% of the Mauritanian population is registered in the ANRPTS database and around 24% of children between zero and five years old receive a birth certificate (UNDP consultant discussion with the Secretary General of the ANRPTS on 27 May 2021).
- Mauritania's population registry offers web APIs which allows authorized entities (outside the Ministry of Interior, these are: national election commission but also mobile operators and financial institutions) to connect.
- On a recent visit to ANRPTS, the Minister of Interior insisted that the civil registry is the 'single source of truth' for all identity related services and applications (see: https://fr.ami.mr/Depeche-64004.html)

National ID card (ANRPTS)

- Mauritanian's ID card does not offer NFC interface. Reading out data requires authorized card readers as well as access to the population registry through web API.
- Discussions with mobile operators and ANRPTS have shown several challenges related to the use of the national ID card for authentication:
  - One mobile operator estimated that ca. 30% of the cards can no longer be read out by a card reader due to damaged chips or antennas.
  - Mobile operators and ANRPTS also pointed out that biometric identification using fingerprints also poses challenges as manual labour by card holders often leads to degraded skin on the fingers making it difficult to match.
  - Currently up to one million ID cards in circulation are due to expire and need to be replaced before next year's elections.

Relying parties

Citizen portal MTNIMA

- MTNIMA is currently developing a citizen portal. Go live is planned for summer 2022. The portal is developed in cooperation with the Saudi company ELM and the Mauritanian company SMART MS.
- The portal will allow citizens in a first step to order key documents from civil registry (birth certificate, etc.)
- The portal uses KeyCloak as IAM.
- UNDP closely coordinates its work MTNIMA's PoC for the citizen portal as well as ELM and SMART MS.

Private sector: Mobile phone operators

- As of May 2022, all three mobile operators in Mauritania are required to verify identities of new subscribers (as well as subscription vendors) using biometric authentication (reading ID card with authorized card reader + fingerprint authentication). Operators are struggling with:
  - sort notice (2 months)
  - elated costs (card reader costs ca. USD 600-700 – one operator estimated that they need approximately 5'000 devices to cover Mauritania)
  - obstacles (defect ID cards / fingerprint authentication not possible due to degraded skin on fingers)
- Thus, there is a strong interest in a national digital ID offering eKYC (to create synergies/ reduce costs).

Private sector: FinTech

- There are a few emerging fintech companies (mobile banking). They expressed a strong interest in remote customer onboarding solutions and eKYC.

Target status

The pilot seeks to demonstrate the following three elements:

1. Secure and trusted identity proofing of test users
2. Secure and trusted user authentication for e-government application (future ELM.SA application)

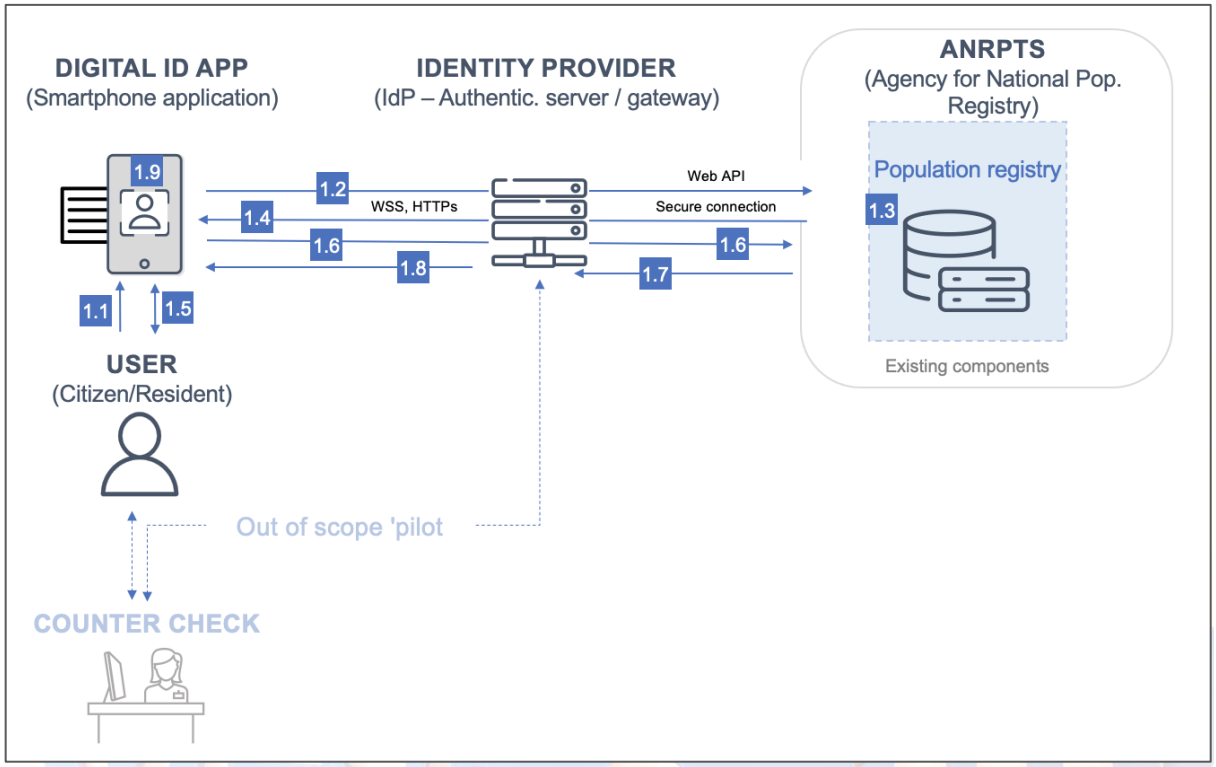
Functional & non-function requirements

ID	Requirement	Type
R.1.	**(Remote) Identity Proofing**	
R.1.1.	User scans MRZ zone of Mauritanian ID Card with Digital ID App	F
R.1.2.	Digital ID App sends <national identity number>, <name>, <first name> and <date of birth> via Web API/ Identity Provider (IdP) to Civil Registry Authority (CRA).	F
R.1.3.	CRA conducts lookup with data received (NIST steps: Resolution & Validation).	F
R.1.4.	If match, CRA sends back <ID photo> to Digital ID App (via Web API / IdP)	F
R.1.5.	Digital ID App initiates auto-ident process (Verification): - face-match (comparison <ID photo> vs. selfie) - liveness detection (real person) *Note: GUI does not show <ID photo> received from CRA at this stage*	F
R.1.6.	If ok, Digital ID App sends "ok" message (app (via Web API / IdP) to CRA	F
R.1.7	CRA sends all attributes visible on Mauritanian ID Card to IdP (via Web API to IdP). IdP signs attributes with private key / stores attributes on its database	F
R.1.8.	IdP sends signed attributes to Digital ID App	F
R.1.9	Attributes are displayed on Digital ID App (as well as status 'verified')	F
R.2	**Password less remote authentication (login) using Digital ID App** (User can authenticate/login to test environment of future e-Gov portal using OpenID Connect)	F
R.2.1.	User initiates the login on e-Gov portal in the browser by clicking on the "Login" button.	F
R.2.2.	User is redirected to the IdP	F
R.2.3.	User's browser loads the login page on IdP, which is a QR code	F
R.2.4.	User scans the QR code with the Digital ID App.	F
R.2.5.	Digital ID App retrieves the information for the desired login from the IdP (*required attributes, recipient of the data)* and obtains consent from User. Once consent has been given, the Digital ID App sends the desired attributes from User to IdP.	F
R.2.6.	IdP verifies the cryptographic signature of the identity information.	F
R.2.7	IdP verifies the status and correctness of the data against own records (*see R.1.7*).	F
R.2.8	IdP issues an OIDC (OpenID Connect) authorization code, which is sent back to the browser.	F
R.2.9	Browser sends the received OIDC Authorization Code (JWT or similar) to the e-Gov portal. e-Gov portal checks the received OIDC Authorization Code against the IdP.	F
R.2.10	If check is successful, User is granted access to the services authorized for him/her on the eGov-portal.	F
R.3	**Non-functional requirements**	
R.3.1	User has mobile (limited – 3G) internet connection (e.g., R.1.2., R.1.4, R.1.6, R.1.8)	NF / O
R.3.2.	Scan of MRZ: reading ISO 9303 compliant documents	C
R.3.3.	Digital ID App and IdP are interoperable with both OIDC and W3C VCs/ DID based third-party applications.	C
R.3.4.	Connections between Digital ID App and IdP / IdP and CRA are secured using HTTPS, TLS, WSS	S/ C
R.3.5.	Backend components run on Kubernetes/Docker environments	O
R.3.6.	Solution needs to build on / extends functionalities of MOSIP's open-source mobile app:	C

	1. Architecture of the Mobile Application: https://github.com/mosip/documentation/blob/develop/docs/mobile-application.md 2. User Guide for the Mobile Application: https://github.com/mosip/documentation/blob/develop/docs/mobile-id-app-user-guide.md 3. Demo Video for the MOSIP Mobile Application: https://drive.google.com/file/d/11U-jmHhhHJpqGqMeo2xK4pt4pkTLZt-K/view?usp=sharing The code base for the application is available here: - "Inji" is the android application : https://github.com/mosip/inji/tree/develop - "Mimoto" is the app backend : https://github.com/mosip/mimoto/tree/develop	
R.3.7.	Code is published on Github under MPL 2.0 open-source license (same as MOSIP) / Design and UX under appropriate CC license.	NF / C
R.3.8.	App is available at least for Android (Google Play Beta) and iOS (TestFlight) and in French/English language.	NF /C
R.3.9.	Face-match / liveness detection is performed 'on device' (reason: limited mobile internet / bandwidth outside major population centers).	NF / O
F = functional requirement, NF = non-functional requirement, S = security, C = conformity (norms, standards, legislation), O = operations,		

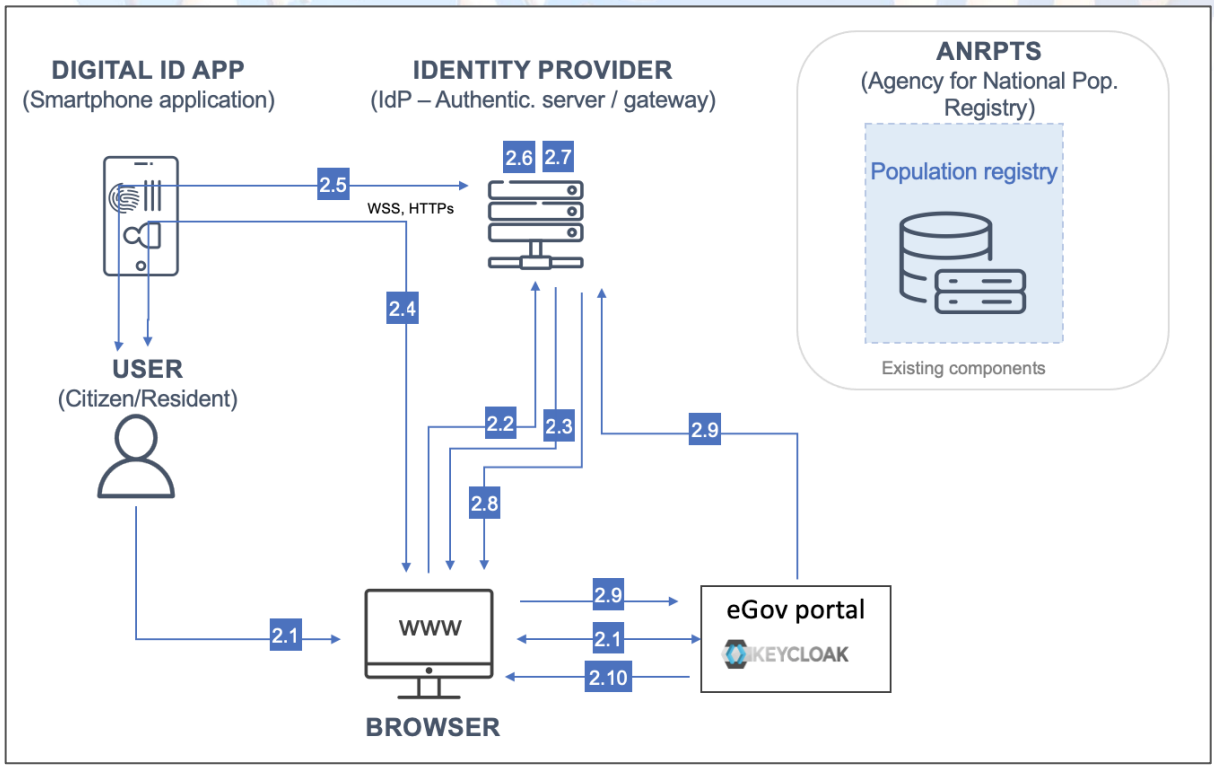
Targe architecture

R.1: Remote Identity Proofing



Note: Numbers refer to functional requirements (see 4.1)

R.2: Password less remote authentication



Note: Numbers refer to functional requirements (see 4.1)

Out of scope pilot

- Document authenticity check during identity proofing (only face match)

- Revocation management on IdP (e.g., revocation lists (of revoked ID cards) sent from ANRPTS to IdP / active revocation of digital ID)
- Arabic language (only French / English)

Required qualifications

Technical qualifications

- Proven experience in developing privacy-preserving digital identity solutions for government clients.
- Proven experience in technologies relating to identity and access management systems (IAM). Specific knowledge of KeyCloak is an asset.
- Proven experience with key digital identity standards, including OIDC, SAML, W3C's VC data model, W3C's DID standard and NIST Digital Identity Guidelines (enrolment and authentication).
- Proven experience in all aspects relating to open-source projects (technical, legal, community management).
- Proven experience with development of native mobile applications (and particularly wallets) for iOS and Android (react native, python, etc.).
- Proven experience with development and integration of Web APIs.
- Proven experience in deploying solution in various environments (TEST, DEV, PROD) using Docker/Kubernetes

Formal qualifications of vendor

- Proof of legal existence of the contractor (Trade Register extract, national identification number for companies and associations)
- Proof that contractor has already successfully delivered similar work for three clients.
- Proof of financial capacity of USD 30,000

Qualification of key personnel

The vendor should be able to demonstrate that the following key resources are available (please provide CVs or LinkedIn profile):

- Senior /lead system architect with minimum 5 years of experience in the field of identity and access management
- Front-end developer (3 years of experience)
- Back-end developer (3 years of experience)
- UX designer (3 years of experience)
- Senior project manager with minimum 5 years of experience in the field of identity and access management

Location, duration and time-frame of the work/deliverables/output

No.	Deliverables	Location (Remotely or on site)	Date
1	Detailed implementation concept	Remote	Max. 15 days after signature of contract
2	Fully functional test version of app + backend components (on vendors test environment)	Remote	Max. 60 days after signature of contract

No.	Deliverables	Location (Remotely or on site)	Date
3	Deployment on client infrastructure / incl app availability on Google Play Beta/ iOS TestFlight	Remote	75 days after signature of contract
4	Digital ID pilot fully functional / acceptance test passed	Nouakchott	90 days after signature of contract

Evaluation critiera

The proposals will be evaluated as follows:

- Administrative Evaluation (Qualification/Experience of the firm) 20%
- Technical implementation proposal 60%
- Qualification of key personnel 20%

Payment milestones

No.	Deliverables	% of payment
1	Detailed implementation concept accepted	25%
2	Fully functional test version of app + backend components (on vendors test environment)	25%
3	Deployment on client infrastructure / incl app availability on Google Play Beta/ iOS TestFlight	25%
4	Digital ID pilot fully functional / acceptance test passed	25%
	Total	_100%

_____