MINISTÉRIO DAS FINANÇAS E DO FOMENTO EMPRESARIAL

REPÚBLICA DE CABO VERDE

TERM OF REFERENCE

Implementation of an Interoperable Cloud Governmental Platform

1. Background

The Republic of Cabo Verde has requested a $20 million loan from the World Bank to finance the Digital Cabo Verde project DCV. The project aims to support the Government of Cabo Verde in the implementation of the main priorities initiatives of the national ICT and e-governance policy implementation strategies, as well as continue to support the strengthening of the national telecommunications sector and contribute to transform the country into a regional digital hub to accelerate its digital economy through an improved digital infrastructure and strengthened demand for digital services and skills.

The digital transformation of a region does not depend solely on the work done by the administration, nor on the work of private entities. In order to undertake the digital transformation of a region with guarantees, both parties are required, as well as public-private cooperation between them. The administration should provide resources that promote this collaboration, in addition to providing services that facilitate the transformation. All this is what motivates this tender.

In its Digital Public Services and Marketplaces component 3, the Project will support the GovCV in its recent efforts to support activities aimed at increasing the GoCV's capacity to deliver digital public services in the domains: G2G; G2B and G2P, in a context where user's digital maturity to access online services continues to pose challenges.

Cape Verde aspires to become a technological referent in the Central Africa region through a digital transformation. This digital transformation will be realized through many technologies, among we highlight cryptography-based technologies. The migration of the Public Key Infrastructure (PKI) to a national infrastructure is a requirement, as well as the use of Blockchain technology and the digital identity based on verifiable credentials.

The objective of the Government of Cape Verde is to make these technologies available to public and private entities in the region, in order to enable the construction of solutions that accelerate the digital transformation of the region. Currently, there are several international initiatives and alliances that were born around these technologies and that promote public-private collaboration, such as: EBSI (European Blockchain Service Infra): an initiative of the European Commission and the European Blockchain Partnership ; LACChain: a Global Alliance integrated by different actors in the blockchain environment and led by IDB Lab; and Alastria: a neutral meeting point for responsible, trusted and regulation-aligned knowledge generation, innovation and blockchain development that has over 500 members. The Government of Cape Verde intends to build an initiative that promotes public-private collaboration and makes resources available to entities.

Moreover, the Government of Cape Verde wants to build end-to-end solutions based on PKI, Blockchain and digital identity. Nevertheless, it also wants to make these technological resources available to private entities and citizens, so that they can build their own solutions. Public-private collaboration is necessary to move forward as a country. Because of that, it is required to open up these systems, for which NOSi is tendering this initiative.

In the near future, the most impactful e-Gov solutions will be redesigned based on these PKI systems and linked to blockchain technology, ensuring efficiency, flexibility and fastness. These solutions will be aligned with the needs of citizens and businesses. Moreover, private entities will build to foster innovation and reduce economic and social inequalities, as well as to promote financial inclusion.

The integration of PKI systems and digital identity it is fundamental. Blockchain-based digital identity solutions are currently increasing. In addition to the initiatives mentioned previously, the Cape Verde ComVida Health Passport - NHACard application is another example. This application would be considered as a starting point for the private-public collaboration.

Following, there are described the technological fundamentals that should be considered by the solution.

Public Key Infrastructure

Asymmetric cryptography has changed the field of cryptography since its inception. Asymmetric cryptography is the basis of a public key infrastructure (PKI), which it is a combination of hardware and software, security policies and procedures that enable the guaranteed execution of cryptographic operations such as encryption, digital signature or non-repudiation of electronic transactions.

The Government of Cape Verde has its own PKI[1], as well as a set of services built on top of this PKI. Thanks to it, it is possible to make use of electronic signatures and electronic contracting, regulated by Decree Law 33/2007, of 24 September, which regulates the recognition of their legal effectiveness.

However, each government or region of the world has its own regulations and PKI systems, among which we highlight the eIDAS regulation that defines a regulation for the European Union. The collaboration and usage of the solutions would be done, regardless which PKI system is used.

Blockchain bridge

Blockchain could be understood as an enabler that allows public-private collaboration. Although initially its nature corresponds to public networks or environments, international initiatives such as the EBP (European Blockchain Partnership) and

[1] https://pki.nosi.cv/web/guest/home

LACChain show us that the potential of this technology can be exploited in other more regulated and proprietary environments.

The Government of Cape Verde aims to build a Blockchain system for Africa. The Government of Cape Verde aims to lead a Blockchain initiative for Africa. The Government of Cape Verde should have its own Blockchain nodes. These nodes will be the origin of the African Blockchain.

The application of this technology will allow public and private entities to build an independent digital platform, which aims to provide the top layer of integrated and trusted services for government, businesses and citizens by increasing market demand and generating a reliable and innovative ecosystem. Furthermore, it is also necessary the application of the Smart Contracts, a foundational element in a Blockchain ecosystem. The Smart Contracts delivers decentralized and transparent business logic.

Digital identity

The Government of Cape Verde aims to implement a digital identity model, as in the ComVida Health Passport - NHACard project. The implementation of a decentralized and user-centric digital identity model will improve public-private collaboration and facilitate the use of different services to citizens.

The digital identity should be integrated with PKI systems. The different cryptography operations (identification, authentication, authorization, signature...) should also be considered, including specifically the linkage between digital identity model and verifiable credentials based on PKI.

2. Objective(s) of the Assignment

The main objective of the following assignment is to build the Interoperable cloud governmental platform of the government of Cape Verde. This platform will be a site

where public and private entities could publish their services and collaborate through it. Moreover, the platform should allow to third parties the usage of the published services.

This platform could be used by physical and legal entities both from Cape Verde and from other countries through their applications. The authentication and validation of them should be done through their digital certificates. In the case of Cape Verdeans, it will be done with the PKI infrastructure (Public Key Infrastructure) currently owned by the Government of Cape Verde.

Once the entities have been authenticated, they will be able to operate on the platform according to their role. The platform should allow the administrator the management of roles and permissions.

Identification and authentication

PKI systems are widely used around the world. At Cape Verde it is implanted the Chave Móvel de Cabo Verde (CMCV), which it is a solution that guarantees Single Authentication and Digital Signature, through the National Identification Card (CNI) or Foreigner's Residence Permit (TRE). The citizens and entities from Cape Verde will use the CMCV.

The solution should be also available for citizens without CNI or TRE. The platform will also be compatible for the authentication of international entities. So, it should be proposed a solution that will enable both tourists and foreign entities to use the system. The Interoperable cloud governmental platform aims to be a referential solution so, the integration of external entities and tourists will be appreciated.

The contractor should propose the design of the Interoperable cloud governmental platform. The contractor will include a relation and describe each of the components of the platform. The functionality of each component should be described, as well as the integrations among the internal and external components.

Trust, collaboration and interoperability

The users and entities could use the platform once they are authenticated. Both public and private entities will be able to publish their services. Users could use the services published by the entities. Thanks to it, the users will have available a ubiquitous platform, so the Interoperable cloud governmental platform will be a referential platform for them.

Entities will use the platform to publish and provide their services to the users. Thanks to the collaboration among entities and the Cape Verde government, entities will be able to reach more users. It is required to propose a solution that will make it possible the integration of the services of external entities, so the platform will be interoperable.

The platform should provide mechanisms for tracking and tracing the activities and operations so, transparency is guaranteed. The contractor should propose the solution and approach will be used at the project.

Finally, the platform should have a user interface to manage it. The user interface will facilitate the management and administrative tasks, as well as those related to the authorization and approval of entities and credentials. In addition, entities will have access to an interface to propose the publishing of new services.

Pilot scope

Below are described the use cases in which the platform will be validated in a real environment involving different types of entities and users:

- Identification and authentication through CMCV: it will be ensured that users who have this application can access and make use of the platform.
- Identification through PKI infrastructure: in this case, the aim is to guarantee that users and entities that do not have the CMCV can also access and make use of the platform.
- Once private and public entities have been authenticated, the administrators can manage the permissions of each entity. So, the onboarding process could finalize successfully.

- Private and public entities can enter to the platform, and they can publish new services. Also, they can query the services published by other entities and which ones could be used by them.

In addition to the functionalities associated with the identification, authentication and authorization of users and entities, the following use cases will also have to be validated in the context of the project:

- Updating and hosting of the NhaCard (COVID Certificate).
- Electronic prescriptions
- Birth certificates, school certificates, professional cards, etc.
- Local and International public procurement

3. Scope of Services, Tasks (Components) and Expected Deliverables

The following section lists the set of services and tasks that the Consultant will have to perform.

Update the Design of the interoperable cloud governmental platform

- A detailed design of the platform (at least: technical architecture, system use case diagrams, sequence diagrams, components diagram, deployment diagram, trust and security framework, data model)
- Service design of the key platform interfaces including but not limited to:
    - User research to inform the design
    - Prototyping of user journeys
    - User testing (with the prototype solution) to inform the detailed design

Development of the Interoperable cloud governmental platform

- Development of the administration platform for the operations required: publishing services, identification, authentication, authorization, interoperability,

credential issuance, credential verification, key management, use of services... as well as the integration with the specified and existing systems.

- The design and implementation of this platform should include (but is not limited to):
    - Design and specification of the technology platform and the offering model
    - Deployment of any technology components required by the design (e.g. Blockchain nodes)
    - Design of the governance model and definition of the extension Road Map

Integration and validation

- Deployment and Integration of the Interoperable cloud governmental platform
- Validation and piloting

Training and Handover

- Training regarding to the management of each component
- Handover of the Interoperable cloud governmental platform

4. Team Composition & Qualification Requirements

Experience Requirements and References

a) The assignment will require a consulting firm with at least ten (10) years of experience in the areas of technology, smartphone, and web application development, including integration services.

b) It must have experience working and deploying projects at Cape Verde.

c) Be familiar with challenges and opportunities in similar countries like Cabo Verde, other small island states, Africa, as well as the developed world.

d) They should have at least five (5) years of experience in deploying Blockchain or distributed ledger technology application on premise at public administration.

e) They should have at least three (3) years of experience in developing and piloting digital identity and verifiable credentials projects (no innovation projects):

- Two (2) of these projects must be done using two different digital identity and verifiable credentials models.
- One (1) of these projects must be related to health credentials.

The team should be comprised of the following three (3) key experts:

1) Team Leader

- Have at least ten (10) years of proven experience in managing a software development team driving full (and correct) adoption of modern software engineering and delivery practices;
- At least 5 years knowledge and experience in designing for and implementing solutions in the cloud and custom coding on IaaS/PaaS to SaaS solution integrations, with a strong track record in the analysis, planning, design, development, implementation and documentation of software solutions.
- Ability to work with proficiency in Portuguese and English.
- are required and with communication skills
- Project management experience.

2) Senior Blockchain Architect and Developer

- University degree in Computer Science, Engineering, or equivalent;
- Have at least five (5) years of proven practical experience in design and deployment of Blockchain networks and solutions using Blockchain open-source technologies.
- Have a track record of delivering Blockchain projects at public administration.

- Have experience as Blockchain trainer and leading technically Blockchain projects.
- Have experience on Blockchain project that integrates PKI systems.
- English language (read, write) are required;

3) Senior Digital Identity and Developer

- University degree in Computer Science, Engineering, or equivalent;
- Have at least three (3) years of proven practical experience in design and deployment of digital identity and verifiable credential solutions using open-source technologies.
- Have a track record of developing digital identity projects.
- English language (read, write) are required;

5. Duration of the Assignment

The mission will be carried out over a maximum period of fifteen (15) months from the date of signature of the contract.

6. Reporting Requirements and Time Schedule for Deliverables

The following outputs/deliverables are expected from the various tasks during the engagement.

Component	***Deliverable***	***Description***	***Type***	***Payment*** (*)	***Date***
Project	*E0. Inception report*	*Overview of the job to be done within the scope of work*	*Report*		*Signing of Contact (SoC) + 20 Days*
Interoperable cloud governmental platform	*E1. Specification of the platform*	*Specification of the Interoperable cloud governmental platform*	*Report*		*SoC + 3 Months*
	E2. Administration Interfaces	*Mock-ups*	*Report and SW*		*SoC + 4 Months*

Blockchain	*E3. Specification*	*Definition of the Blockchain and Smart Contracts solution*	*Report*		*SoC + 5 Months*
	E4. Blockchain network / nodes operation	*Startup of the required nodes*	*Report and SW*		*SoC + 7 Months*
	E5. Smart Contracts		*Report and SW*		*SoC + 9 Months*
Interoperable cloud governmental platform	*E6. Developments*	*Applications code*	*SW*		*SoC + 10 Months*
Integration and validation	*E7. Specification for new services*		*Report*		*SoC + 11 Months*
Training and Hand Over	*E8. Training plan*	*A plan with an organized description (what, when, who, how, etc) of the trainings to be carried out*	*Report*		*SoC + 12 Months*
Integration and validation	*E9. Pilot results*		*Report*		*SoC + 14 Months*
Interoperable cloud governmental platform	*E10. Administrative manual*		*Report*		
Training and Hand Over	*E11. Training material*	*Material used during training*	*Report*		*SoC + 15 Months*
	E12. Hand over material		*Report*		
	E13. Final report		*Report*		

(*) After approval by the Client

7. Client's Input and Counterpart Personnel

(a) The following infrastructures will be made available by Nosi

i. An infrastructure at its facilities that will host all the components to be developed and implemented.

ii. A code repository in which the Consultant will upload all the code and software developed, as well as configuration files and others.

(b) Services and Personnel Counterpart

i. A team of technicians will be available to support the Consultant in ensuring that Nosi's procedures and standards are in. Monthly meetings will be held between both parties.

ii. The necessary developments for the pilot of Interoperable Cloud Governmental Platform, such as the mobile application and the application for entities, will be taken over by Nosi.

iii. A team will also be made available to support the consultant in delivering the software. It is intended that, during development, the Scrum methodology

based on sprints will be implemented, where the Nosi team would validate the delivery after each sprint.

8. Organization of the assignment

The consultant firm shall undertake the assignments in close consultation with the NOSI, who will follow and support the assignment. The Consultant will report to *Unidade de Gestão de Projetos Especiais* (UGPE) for contract administration.

9. Contract

A Lump-Sum form of Contract shall be signed, payments to the consulting firm are linked to approval of deliverables, and the payment of reimbursable expenses are made upon presentation of the receipt of the expenses occurred at the real cost.