TDRA | هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

Annex (1) Digital Government Enablers

Version 2

For
RFP Title
Month, Year

Telecommunications and Digital Government Regulatory Authority
P O Box 26662
Abu Dhabi, United Arab Emirates
Tel: +971 2 6269999 Fax +971 2 6118209
www.tdra.gov.ae

TABLE OF CONTENTS

1. STATEMENT OF UNDERTANDING

The purpose of this document is to provide a clear outline of the United Arab Emirates Digital Government Enablers provided by the Telecommunication and Digital Government Regulatory Authority (TDRA); and to ensure vendor's alignment in the Projects Design-build and execution to be inclusive of the below enablers for any infrastructure, Authentication, proactive services and any other related project requirement. The Digital Enablers includes multiple components across the Digital Government Enterprise Architecture which includes infrastructure, data, applications and services layers.

2. OVERVIEW

The Information and Digital Government sector of the Telecommunications and Digital Government Regulatory Authority (TDRA) is responsible for supporting infrastructure and strategies that drive smart transformation process of UAE government entities through the implementation of the digital Government's plans, Government Services Strategy and National Digital Government Strategy; aiming to continually provide the appropriate environment delivered according to the best practices and global standards through secure emerging technologies and cyber resilience, to drive the required digital transformation via a world-class digital secure infrastructure with guaranteed privacy; to ensure a seamless and holistic digital transformation through uninterrupted digital platforms to raise government efficiency; and leverage digital capabilities & skills ensuring digital sustainability in all circumstances, and enhance planning & investing in future technology

Moreover; TDRA is committed to reinforce all sectors, drive towards building a knowledge-based economy; ensuring the quality of digital life for citizens and raising digital awareness for all segments of society, in addition to encouraging the purposeful use of technology & Digitalization

3. DIGITAL GOVERNMENT ENABLERS

Corresponds to the guidance of the UAE's leadership which stresses on the necessity to continue working as a unified national team with all federal entities aiming for the UAE to be at the forefront of the world in Digital services index.

Whereas the federal entity is managing to provide digital platform for internal or external use ,or develop digital and proactive government services; the proposed solutions is to be built upon and compatible with the below mentioned enablers, as indicated in the UAE's 'Digital Customer and Digital Government Service Policy' that has been approved by the UAE Cabinet on 31 March 2021.

3.1. INFRASTRUCTURE ENABLERS

3.1.1. Federal Network (FEDnet)

Overview

The primary purpose of FEDnet is to provide a private & secure network connectivity for the Federal Government Entities (FGEs) as well as provide them with the opportunity to connect with local networks of any of the seven emirates through the local digital government authorities. In addition, FEDnet Smart Cloud is a private cloud allowing the provisioning of multiple shared services such as GSB and hosting capabilities for use by the entities. FEDnet Smart Cloud is highly available, secure, and resilient. Services are highly available through a Main site and a Disaster Recovery site.

FEDnet covers two Data Centers with growth considerations for many years to come using design and technology solutions providing secure, virtualized private infrastructure for each government entity using latest management platforms to manage the security and provide access control. The

Private Cloud design solution caters for self-service multi-tenant private Virtual Data Centers (VDC) for government entities and allows FEDnet to provide shared and hosting services to these government entities utilizing the same virtualized infrastructure.

FEDnet provide all monitoring capabilities required as well as Service Desk to manage the shared services.

FEDnet Services

FEDnet provides number of services that support application hosting including:

- Infrastructure Cloud services, based on VMware technology:
  - Infrastructure as a Service: offer resources of vCPUs, RAM, and Storage. This is for all environments including production, staging testing, development and Disaster Recovery.
  - Load Balancer and firewall: virtual load balancer and firewall are provided per virtual data center.
  - Disaster Recovery (DR) as a Service: offer replication of all VMs from production to the DR site.
  - Backup as a Service: Periodical backup for applications and databases.
- Managed Services (available only for Windows and Red Hat): Managed Services includes OS management, load balancing and firewall configuration, patching, backup and Monitoring.
- Around the clock Service Desk support.

Illustrative Graphs

Figure (1): Unmanaged Services

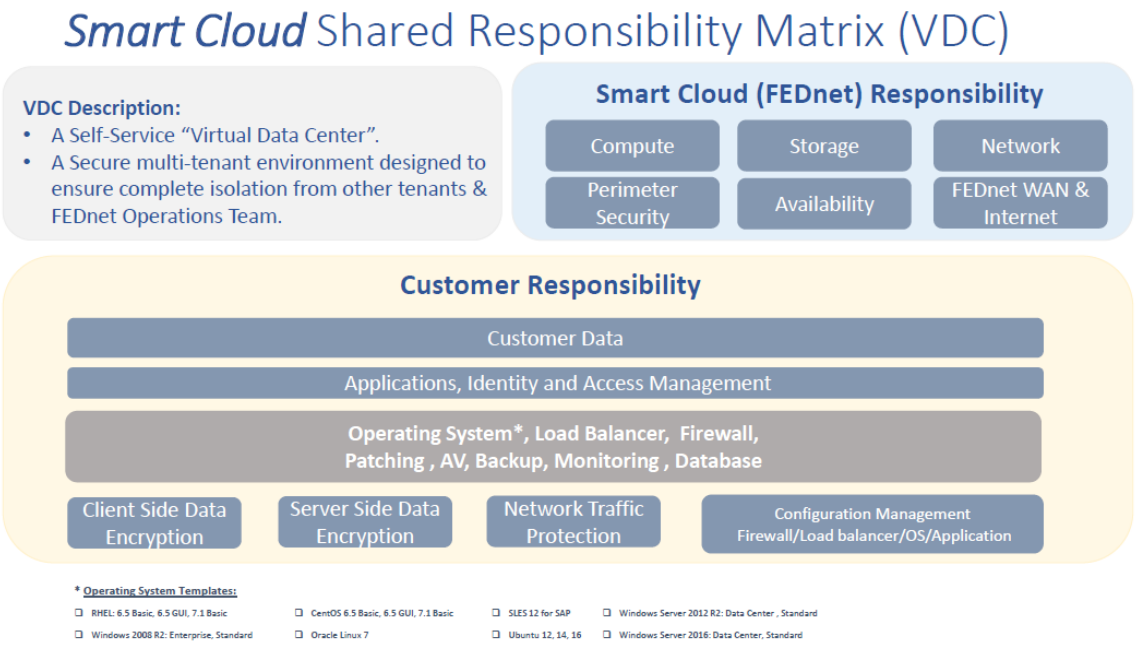
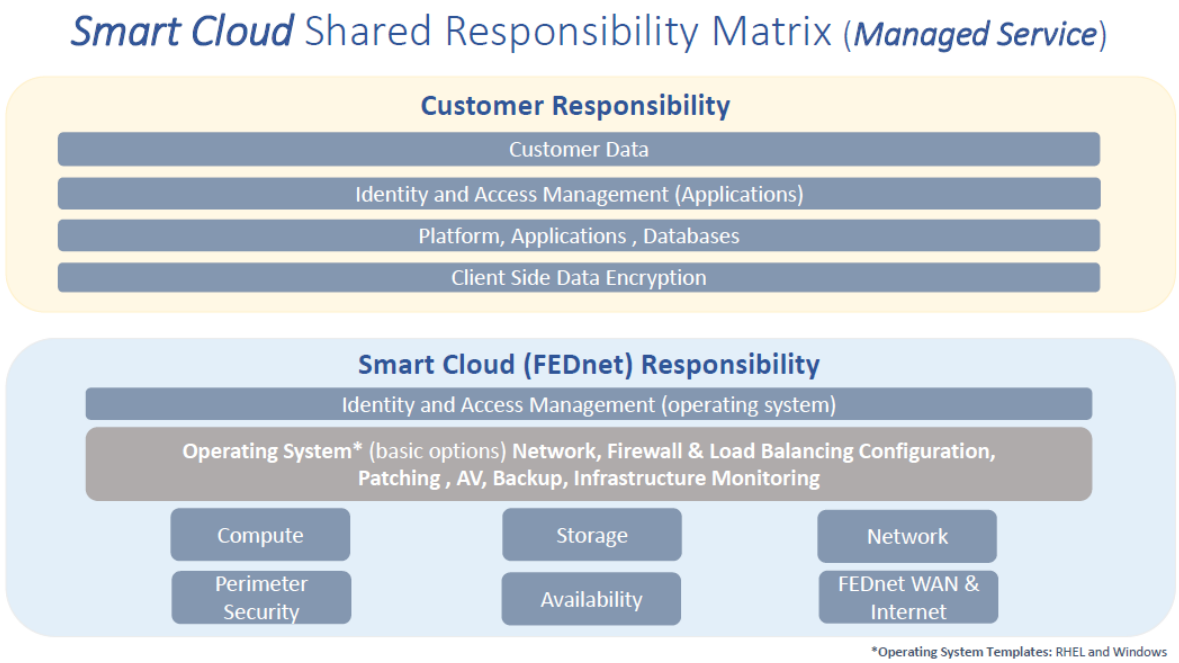


Figure (2): Managed Services

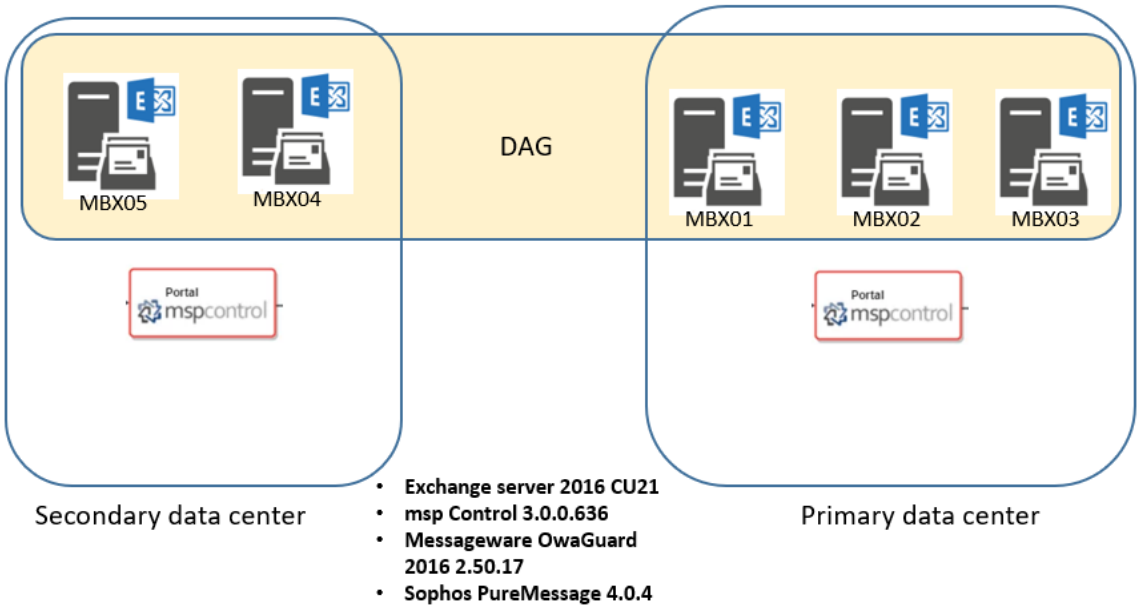


3.1.2. Collaboration

3.1.2.1. Email as a Service

Email as a Service is a multi-tenant shared email service offered to Government Entities. It provides a centralized email environment based on Microsoft Exchange. It offers a self-service portal for the entities to manage their email accounts. The solution is highly scalable and with full redundancy to ensure high availability. Emails incoming and outgoing are scanned and filtered through FEDnet Email security controls.

Figure (3): Managed Services



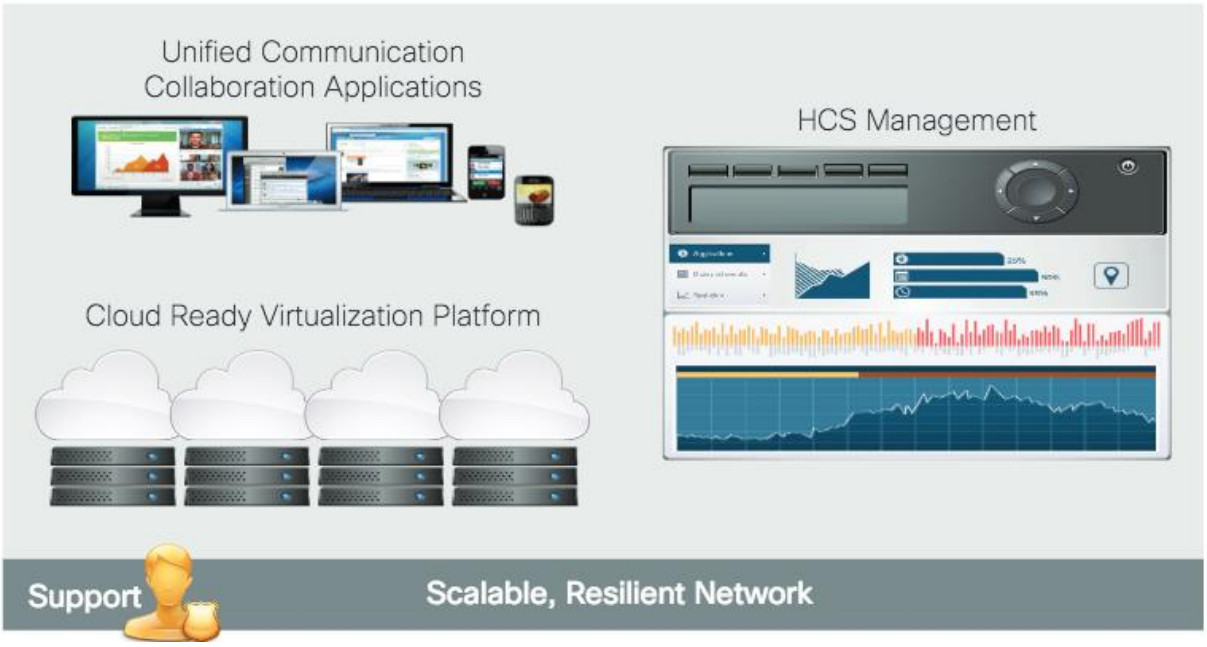
3.1.2.2. Unified Communication

Hosted Collaboration Services (HCS) provides multi-tenant hosted collaboration services from FEDnet Datacentre based on Cisco HCS platform. With HCS, entities can deploy Audio (IP telephony) & Video capabilities based on their need.

It Includes Unified Communications, Corporate telephony and Conferencing. The solution is highly scalable and with full redundancy to ensure high availability.

Federal government entities will connect their endpoint devices to the call managers hosted at the FEDnet.

Figure (4): Managed Services



3.2. SERVICES' INTEGRATION

3.2.1. Government Service Bus

Overview

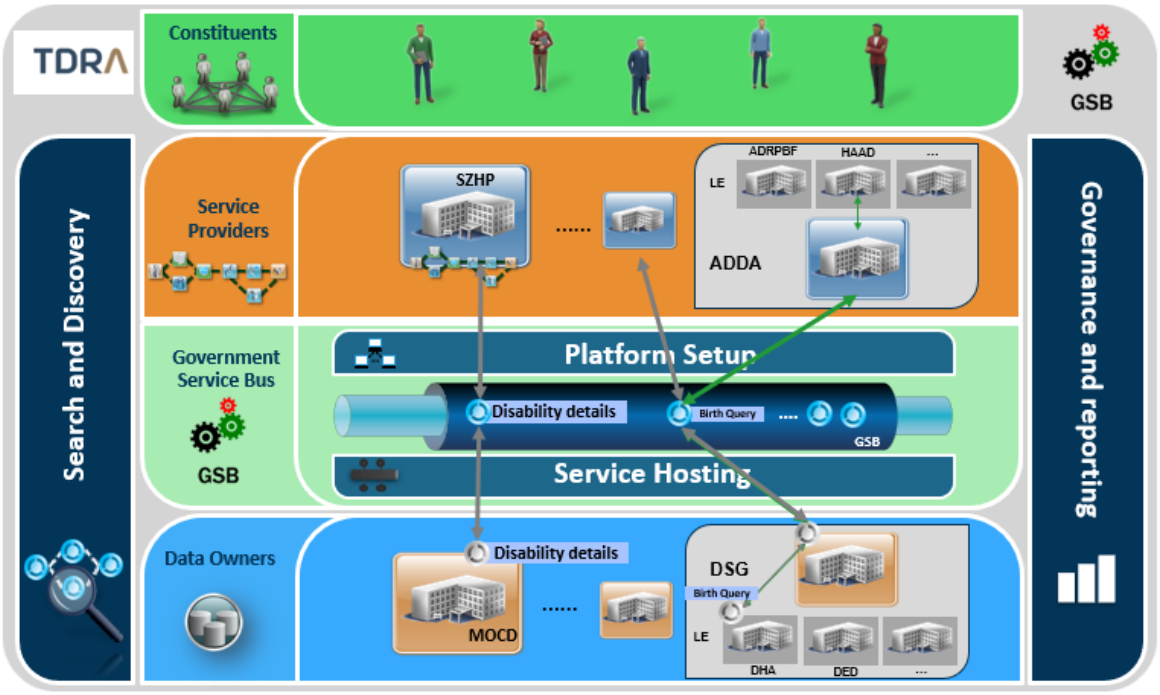
The Government Service Bus (GSB) provides a platform for Federal Government Entities (FGEs) to integrate with each other. It also facilitates the integration with Local Government Entities (LGEs) through the Local Service Buses (LSBs) for each of the respective Emirate. In addition, GSB has enabled the integration between Federal and private entities by availing the Government Services (GS) from either (Federal/Local) entities via External Gateway through the internet. Also, GSB has allowed the File Based as well as Batch Processing Integration between the entities. The GSB enables GEs to optimize their services through sharing of data. The GSB is aligned with the overall objective of the UAE government because it has a "whole of government" approach to constituents' services and their supporting ICT infrastructure.

The GSB will consist of the following key components:

- Service registry and repository
- Service governance
- Service monitoring
- Integration platform

Illustrative Graph

Figure (5): GSB High Level Architecture



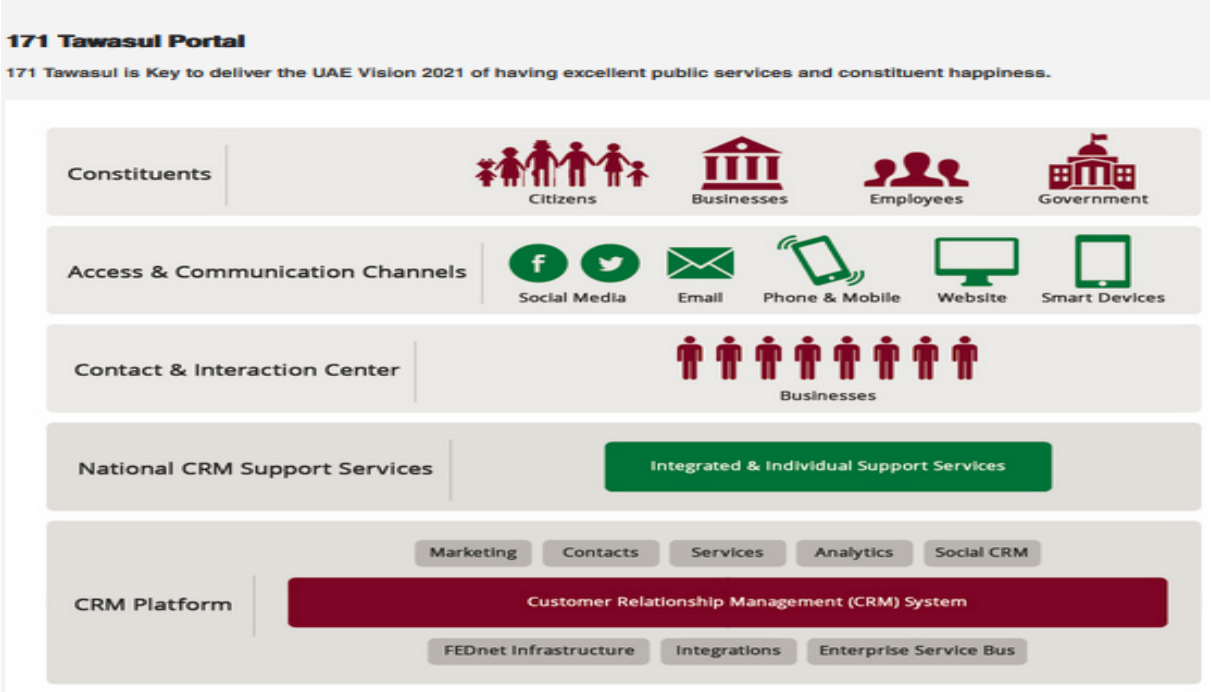
3.2.1. National Customer Relationship Management System (171.ae)

Overview

The NCRM stands for the National Customer Relationship Management system, it is a digital enabler which forms a centralized system to capture customers' complaints, suggestions, inquiries and compliments. It has two technical implementation model to cater for FGEs with existing local CRM systems as well as FGE without. It provides reporting capabilities to provide FGEs with information about their logged cases as well as their status. To use this enabler FGEs must acquire licenses for its customer service agents.

Illustrative Graph

Figure (6): Tawasul Portal



3.2.2. National Digital Identity- UAEPASS (uaepass.ae)

Overview

UAE PASS is the first national digital identity for citizens, residents and visitors enabling them to access to many services across various sectors of the UAE and allowing them to digitally sign and authenticate documents. It also enables users to request a digital version of documents issued to them and to use the same to access services by integrating with the Digital Vault.

UAE PASS is collaboration between TDRA and Abu Dhabi Digital Authority and Dubai Digital Authority, aiming to provide a single trusted digital identity solution for service providers in the UAE, while maintaining a high level of security assurance and seamless user experience. UAEPASS is a fundamental enabler for digital transformation initiatives, and a contribute towards achieving the UAE Centennial 2071, and sustainable development.

UAEPASS allows users to securely identify themselves to service providers through smartphone based authentication. It also enables users to digitally sign, validate documents, request & share data/documents while maintaining a high level of trust and security assurance.

UAE Pass Features

- Mobile based ID
  - PKI-based authentication
  - Mobile App based Digital-ID solution with PKI Authentication certificates
  - Keys in TEE/SE protected by PIN or Touch ID
  - Easy enrollment through Emirates ID and facial recognition

- Contextual Authentication
  - Standardize service providers (e-government, e-commerce, etc.…) user authentication
  - Secure and recognized user identity based on 2FA on PKI credentials and out-of-band verification

- Transaction and Document Signing
  - Enable service providers to easily integrate digital signing services
  - Provide recognized digital signature for documents and transaction
  - PKI Certificates issued from UAE PKI Infrastructure. For the Emirates of Dubai certificates are issued by Dubai Electronic Security Center. For Federal Entities the Certificates are issued by Authority for Identity & Citizenship, Customs and Port Security.
  - Digital Signature service is integrated with the Timestamping service from PKI Certificate Authority
  - Different types of User Profiles and PKI Certificates like Advanced Signing Certificates, Qualified Signing Certificates based on the Identity Proofing of customer during UAEPASS user registration.
  - Currently PKI certificates are issued to Natural Person and eSeal PKI certificates are issued to Entities

Illustrative Graph

Figure (7): UAE PASS Authentication

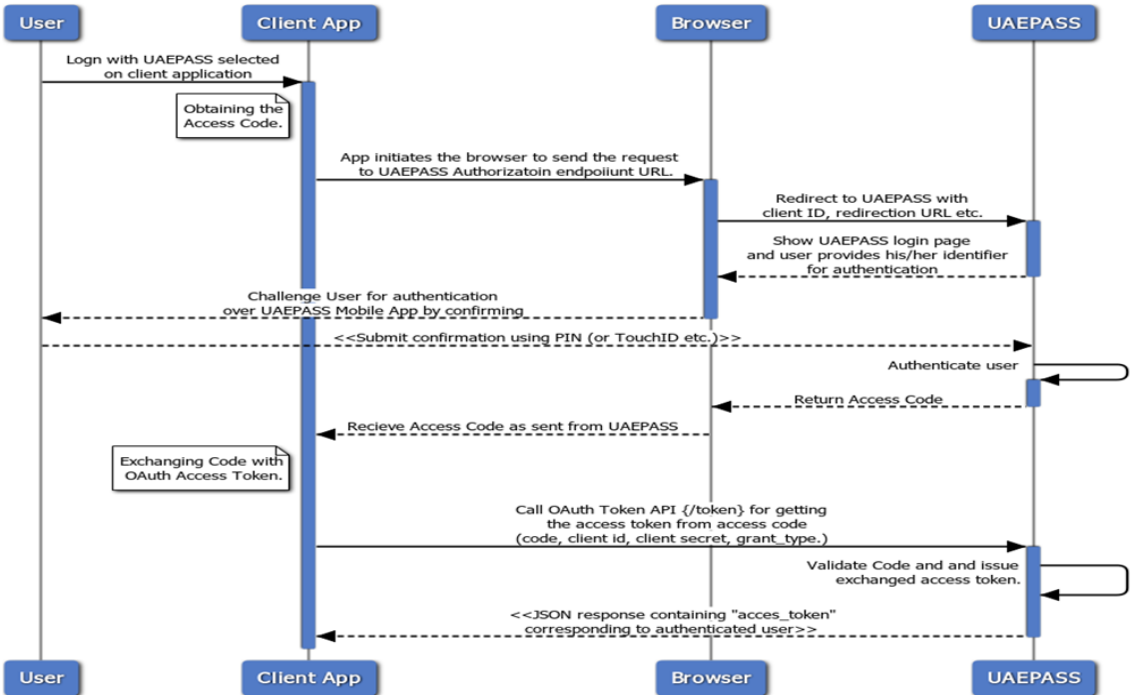
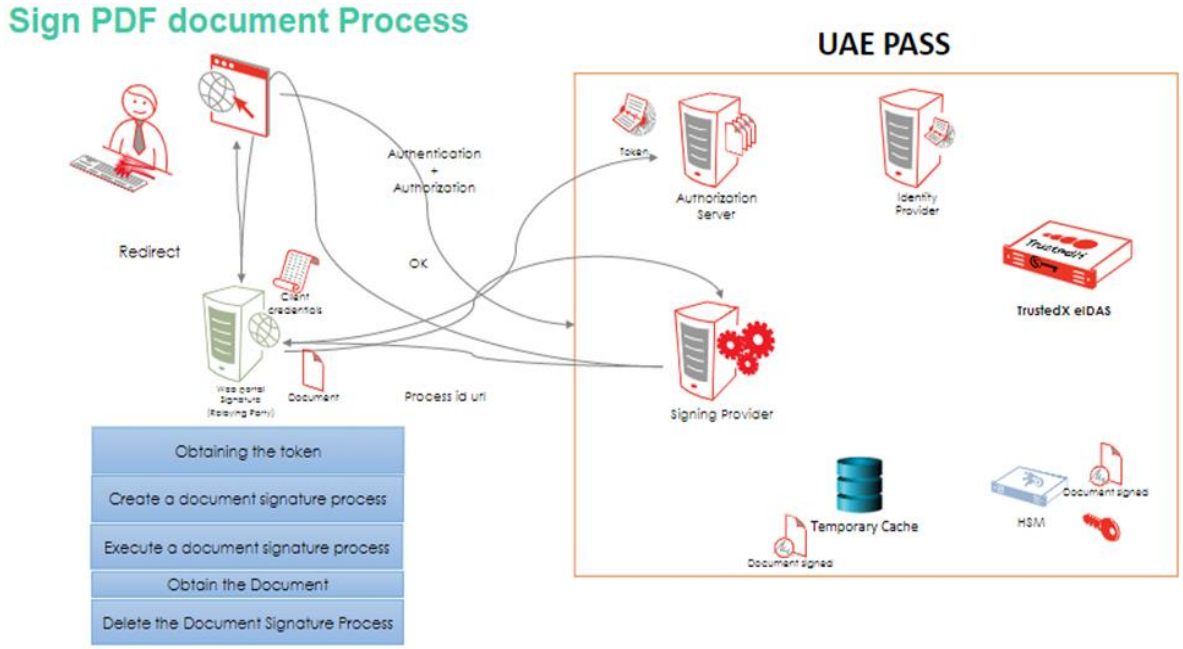


Figure (8): UAE Pass Signing



3.2.3. Digital Trust Platform

Digital Trust Platform (DTP) is a platform built on blockchain technology, that is based on international standards to ensure privacy, trust, security and the decentralization of data. DTP enables the transformation of digital government documents into secure and digitally trusted documents (Credentials) equal to its physical counterpart. DTP offers two applications, the first application is Digital Vault which is enabled through UAEPASS app and the second application is UAE VERIFY which is an independent verification portal for the digitally trusted documents.

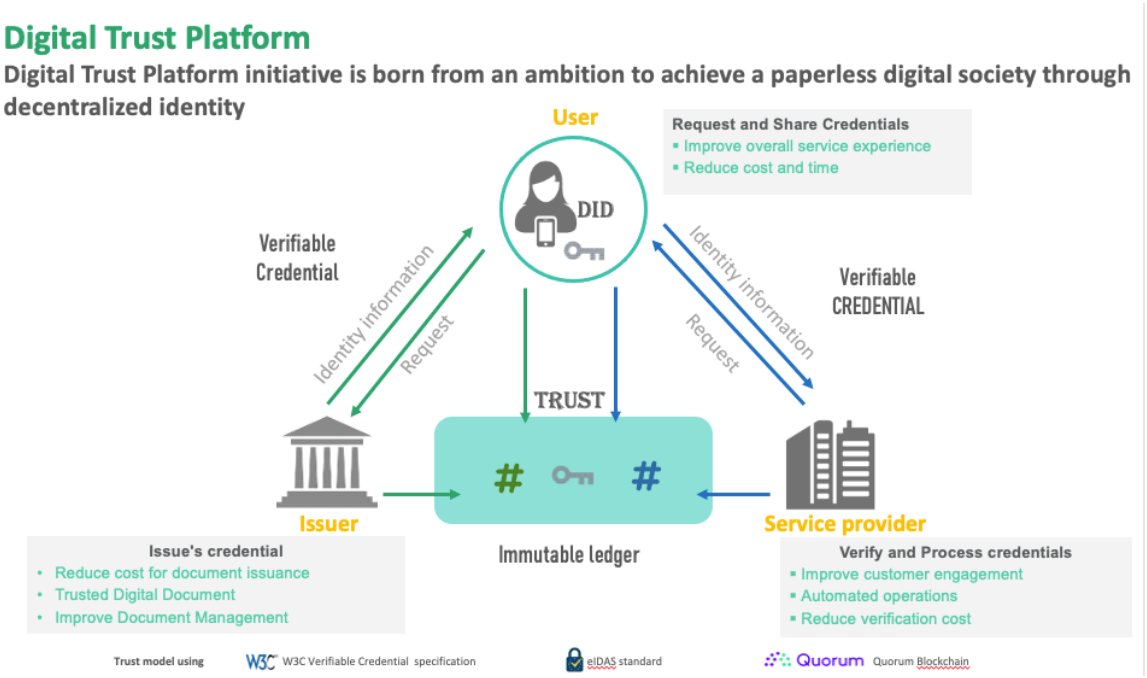
3.2.3.1. Digital Vault

Overview

Digital Vault enables citizens and residents in UAE to digitally request their digital document issued to them by Federal and local government entities through the UAEPASS app and the ability to share documents with the user's consent, through a safe environment with service providers to avail services. Empowering a seamless digital transformation journey across different channels such as digital services, digital on-boarding and eKYC. This is done by sharing official digital documents and their electronically sealed meta data directly from the issuing governmental entity as well as self-signed documents uploaded and digitally signed by the user. Digital Vault has been added to UAE PASS as an extended feature eliminating the need for physical identity verification and the need for physical document citation. Providing higher data quality and enabling service automation. All while maintains optimum privacy.

Illustrative Graphs

Figure (9): Trust Model



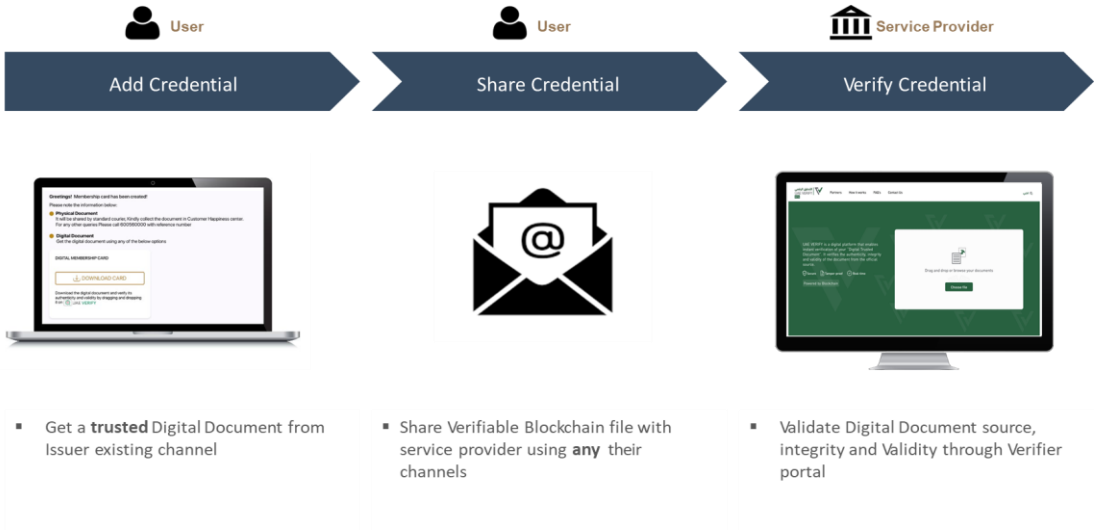
3.2.3.1. UAE Verify (*uaeverify.gov.ae)*

Overview

UAE VERIFY enables government entities of issuing and attesting digital trusted documents for individuals & companies and directly register them on the blockchain. UAE VERIFY also enables instant verification of the digital trusted document registered on the blockchain, through an independent verification portal. It verifies the source, integrity and validity of the document. which enables service providers to verify the authenticity of the digital documents shared with them.

Illustrative Graph

Figure (10): UAE Verify Model



3.2.3.2. Digital Trust Blockchain Network

The Digital Trust Blockchain Network is a federal blockchain network established on Quorum enterprise blockchain platform, acting as the trust anchor of the Issued Digital Documents (Credentials) and providing an audit trail on key transaction of the DTP such as requesting and sharing of credentials. Federal blockchain network envisages all Issuers and Service Providers to be part of the blockchain network to have Decentralization and enhance the Trust Quotient.

3.3. SERVICE DESIGN

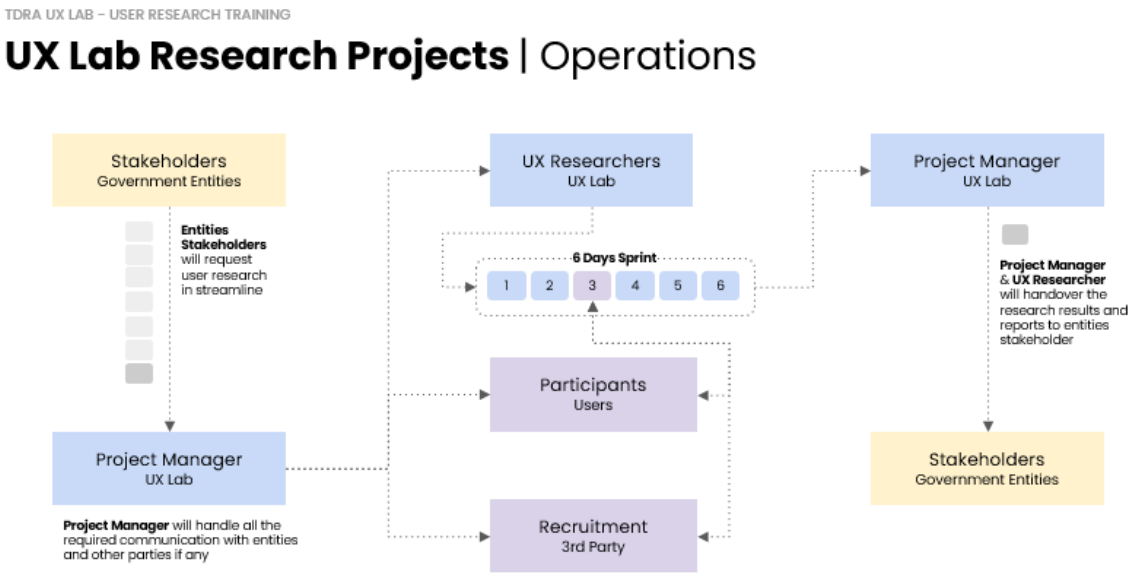
3.3.1. User Experience lab

Overview

The UX Lab is a digital enabler which aims to assess and evaluate the user experience of platforms and services (web and mobile apps) at all stages. It implements advanced scientific concepts and methods, focusing on improving and enhancing websites and smart applications, based on the behaviour and preferences of the users, and taking into account the entities' needs to raise the services to the highest levels of ease and smooth use.

Illustrative Graph

Figure (11): UX Lab



3.3.2. Website Design Guidelines (DLS)

Overview

The Website Design Guidelines are a collection of reusable design templates and components with specific set of guidelines that enable federal entities to create a seamless user experience for users, in order to unify the digital presence while improving the user experience.

DLS provide guidelines, components, and templates to create a consistent federal website experience.

DLS Link

https://dls.government.ae/

3.4. Capacity Building

3.4.1. Digital Enablers Training Program (*academy.tdra.gov.ae/detp)*

Overview

Digital Enablers Training Program is an interactive training program for digital enablers to equip trainees with necessary knowledge and skills needed to adopt and implement digital enablers. The Digital Enablers Training Program offers comprehensive training packages for 10 major digital enablers in UAE. Each enabler training comprises a foundation course (what and why of the enabler) and some related use cases that focus on a specific role or task.

It is recommended that any stakeholder who would be working on integrating with digital enablers mentioned in this document to attend the corresponding training track within the program.

Enrollment to the training program is available through TDRA Academy website (click here).

Illustrative Graphs

Figure (12): Digital Enablers Training Program

4. DIGITAL GOVERNMENT ENABLERS REQUIREMENTS

Section	Bidder's solution shall address the following requirements:
	Federal Network
1	Solution shall leverage FEDnet architecture to provide access to government entities inside and outside FEDnet; meaning solution consider any additional design principle required to maintain aspects of security, reliability, etc. between government entities inside and outside FEDnet

2	The Bidder shall submit to the TDRA as part of their proposal specifications for all necessary hardware, software and tools for the environments; the Bidder can propose to combine certain environments, where appropriate; these environments, to the extent possible, shall be built using the FEDnet infrastructure capabilities; the six (4) environments include: • Production • Staging • Training • Disaster Recovery (DR) The components should be segregated based on: • Environment • Project (Blockchain and Citizen Vault) • Capacity for initial load vs growth The Bidder should highlight different hosting i.e. FEDnet vs 3rd Party if applicable. Bidder should submit as a component of proposal specifications all software, hardware, and tools that would be inclusive of a full Software Development Lifecycle (SDLC) for government entities to build service integrations.
3	The Bidder shall develop a technical infrastructure document which describes all of the hardware, system software, and tools necessary for each of the environments proposed; the document should be based on the FEDnet architecture; any component which is not offered by FEDnet would have be purchased, installed, and managed by the Bidder until the handover phase
4	Bidder shall work closely with FEDnet to identify any configuration changes required to FEDnet for solution to operate
5	The Bidder is responsible for installing and configuring all software and tools purchased under the contract
6	The Bidder shall submit a Service Desk Support Plan for use by the existing FEDnet service desk addressing the following: • Overview of support strategy assuming TDRA and Bidder will provide tier 2 and tier 3 service desk support • Service desk operations (e.g., processes and procedures) • Incident Management procedures and processes, including escalation and problem management procedures and processes
7	The Bidder is responsible for maintaining all software and tools purchased under the contract
8	The Bidder should provide an expansion manual
9	Bidder should provide capacity planning including the threshold growth model and defining a response strategy for growth

10	The Solution should pass the security testing from delivered by aeCERT and any other third-party security company assigned by TDRA within the timeframe provided by the team and be compliant with International Organization for Standardization (ISO) 27000 – Information Security and ISO 22301 – Business Continuity

Section	Bidder's solution shall address the following requirements:
	Government Service Bus
1	The bidder shall use the Government Service Bus (GSB) which provides an Integration middleware for Federal Government entities (FGE) to integrate with each other. GSB facilitates the integration with Local Government Entities (LGE) through the Local Service Bus (LSBs) operated by the smart government of each emirate. The GSB enables Federal Government Entities (FGEs) and Local Government Entities (LGEs) to optimize their service through sharing of data through service integration.

Section	Bidder's solution shall address the following requirements:
	National CRM
1	The bidder shall integrate with the National CRM to capture complaints, suggestions, inquiries and compliments related to FGE services

Section	Bidder's solution shall address the following requirements:
	UAEPASS
1	The solution should integrate with UAEPASS for authentication of all User segments – individuals & cooperate
2	The solution should integrate with UAEPASS for digital signature & eSeal use cases
3	The solution should integrate with UAEPASS for Data/document (Digital Vault) sharing with the private sector

Section	Bidder's solution shall address the following requirements:
REQ	**Digital Trust Platform**
1	The solution should integrate with Digital Trust Platform for Issuance of all the Digital Document (Credentials) to the users
2	The solution should integrate with Digital Trust Platform to support <Name of Federal Government Entity> Customers to retrieve their Digital Documents (Credentials) through UAEPASS Mobile App.
3	The solution should integrate with UAEPASS to apply UAEPASS Digital eSeal Signature on Credential shared with Digital Trust Platform.
4	The solution should support tracking amendments and cancellation of Issued Credential with Digital Trust Platform.
5	The solution should support the revocation of Issued Credential on any amendments and cancellation of Issued Credentials by integrating with Digital Trust Platform
6	The solution should support verification and validation of <Name of Federal Government Entity> Issued Credentials from <Name of Federal Government Entity> eChannels by integrating with Digital Trust Platform.
7	The solution should be compatible and compliant with Digital Trust Platform Technical Standard Formats.
8	[Optional – if Federal Entity would like to host a blockchain node] The solution should be hosting Quorum Ethereum blockchain nodes which are integrated with UAEPASS Blockchain Quorum Network. UAEPASS Blockchain Quorum Network support RAFT consensus algorithm.

Section	Bidder's solution shall address the following requirements:
	Service Design
1	The service shall adhere to the Service Design principles & standards
2	The service shall adhere to the one digital channel integration strategy
3	The service shall adhere to the API First Guideline
4	The service shall take into consideration the accessibility standards

Section	Bidder's solution shall address the following requirements:
	Digital Enablers Training Program
1	The bidder shall attend the Digital Enablers training program. The bidder can register to be a trainee through the following link: https://academy.tdra.gov.ae/detp

Note: The above Enablers will be updated by the Telecommunications and Digital Government Regulatory Authority from time to time.

To get the latest version of the document, visit the following link:

https://dgov.tdra.gov.ae/regulations/digital-government-enablers-annex

For more information on the enablers, kindly contact the entity who issued the RFP.