Digitizing a Nation: Technology is only one piece of the puzzle
DIGITALISATION IN THE UAE IS DRIVING PROGRESS ACROSS THE SPECTRUM

Health, Education, Government Services, Transportation, Financial Services and more...

Stretches across the Digital Economy
OVERALL, THIS IS IMPROVING QUALITY OF THE DIGITAL ECONOMY

- Increasing Productivity
- Improving Economic Opportunity
- Higher Quality of Life

(There is a reason the UAE has a Ministry of Happiness)
HOWEVER, THIS IS ONLY POSSIBLE IF PARTICIPANTS HAVE CONFIDENCE IN THE SYSTEM ITSELF

We need to establish **TRUST**
ESTABLISHING **TRUST**

**Trust:**
Confidence or assurance that a person, system or thing will behave exactly as you expect, or alternatively, in your best interests.

As more and more interactions between entities take place in a virtual environment, how can we trust that we are dealing only with who or what we expect?

"The key to high-quality communication is trust, and it's hard to trust somebody that you don't know."

-- Ben Horowitz (VC firm Andreessen Horowitz)
To send any type of data across open public networks like the internet securely

To create and send reliable digital signatures instead of handwritten ones

To reliably know who you are dealing with for transactions in cyberspace
PKI IS MORE THAN JUST TECHNOLOGY

Although PKI requires the use of the strongest validated encryption technologies, **TRUST** cannot be achieved by technology alone.

A strong **governance structure** for how the technology will be deployed, operated, used and relied upon is necessary. Policies and processes are defined, implemented and audited.

Clarity on relationships and responsibilities of users, service providers and relying parties are published and enforced.
IDENTITY ASSURANCE

• Identity Assurance (IA) is a foundational element of effective security and TRUST

• Knowing who is at the other end of a transaction event is key to Digital Trust

• Identity Assurance is a measure of confidence in the true identity of the entity at the other side of a transaction
... dictates the strength of an authentication event. It asks the following questions:

- How was the original identity verified?
- What processes were used to ensure the subscriber/user is the rightful owner of their claimed identity?
- Was trusted biometric verification used, such as a photo ID or fingerprint from a trusted authority?
- How reliable are the sources of identity information?
- What type of credential was issued?
- Is it resistant to tampering, counterfeit or exploitation?
To Successfully Digitize a Nation Requires several elements to be present:

• National PKI service to enable digital Trust Services (Confidentiality/Integrity/Assurance)
• National Certification Policy (CP) to define the basis upon which the NPKI operates
• National Digital Identity services to enable the highest assurance of participants in the digital economy
• National Digital Signature services to facilitate digital processes and transactions
• Legal Recognition of Digital Identities and Digital Signatures as equivalent to their analog counterparts
INTRODUCING UAE PASS
WHAT IS UAE PASS

• Smart Dubai, in collaboration with the Telecommunications Regulation Authority (TRA), has inaugurated UAE PASS, a National Digital Identity and Signature Solution for all citizens, residents and visitors of the United Arab Emirates.

• UAEPASS provides a single digital identity that allows the user to access services for both local and federal government entities, in addition to other service providers. The solution introduces mobile based authentication to users who can simply validate their sign in using their smartphone. It also allows users to digitally sign and validate documents, in order to minimize their visits to service centers to sign important and time-sensitive documents.
WHAT IS UAE PASS

• **Mobile based ID**
  – PKI-based authentication
  – Keys in TEE/SE protected by PIN or TouchID
  – Easy enrollment through Emirates ID, Dubai ID, SmartPass, and other Trusted IdPs

• **Cloud based ID**
  – Keys stored in cloud HSM protected by user password
  – Under the sole control of the user

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

• **Transaction and Document Signing**
  – Provide recognized digital signature for documents and transaction
  – Enable service providers to easily integrate digital signing services
WHAT IS UAE PASS
UAE PASS Objectives

- Streamline the usability, availability and security of government services
- Facilitate an assured single unified digital identity and authentication module
- Improve customer service and satisfaction
- Integrate interoperability of government service delivery
- Implement Digital signatures recognized by the UAE legal system
WHAT ARE THE KEY SERVICES
UAE PASS OVERVIEW

HOW IS WORKS - 1

Service Provider
Example Online banking

Authentication query sent to Mobile ID platform

Login Page

UAE Pass Platform

UAE Pass App

Authentication Confirmation from UAE Pass app
Service Provider
Example Online banking

UAE Pass App

Document for signing

Document signature initiated from web portal to Mobile ID platform

UAE Pass Platform

Document signature performed on Mobile device
UAE PASS OVERVIEW

HOW IS WORKS - 2

Standard-Compliant Qualified Signature

Visual appearance of the digital signature PDF-embedded
WHO ARE THE USERS
## TYPES OF USERS

<table>
<thead>
<tr>
<th>User Types</th>
<th>Enabled Services</th>
<th>Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verified Users</strong></td>
<td><strong>Online Authentication</strong></td>
<td><strong>Mobile Certificate</strong> (ECC / RSA based)</td>
</tr>
<tr>
<td>(e.g. Resident, Nationals)</td>
<td><strong>Online Document Signing Mobile Based Signing</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cloud Certificate on HSM</strong> (RSA based)</td>
<td></td>
</tr>
<tr>
<td><strong>Unverified Users</strong></td>
<td><strong>Online Authentication</strong></td>
<td><strong>Mobile Certificate</strong> (ECC / RSA based)</td>
</tr>
<tr>
<td>(e.g. Visitors)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## User Types

<table>
<thead>
<tr>
<th>UAE CP Levels</th>
<th>User Types</th>
<th>Enabled Services</th>
<th>User Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 4</strong></td>
<td>EID Verified Users (Valid Emirates ID)</td>
<td>Online Authentication, Online Document Signing - /High</td>
<td>Mobile based Authentication</td>
</tr>
<tr>
<td>In-person proofing, no in-person antecedent - KIOSK -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td>Verified Users (Valid government ID)</td>
<td>Online Authentication, Online Document Signing - /Medium</td>
<td>Mobile based Authentication, Cloud based signing</td>
</tr>
<tr>
<td>In-person proofing, in-person antecedent - Remote -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td>Unverified Users (e.g. Visitors)</td>
<td>Online Authentication</td>
<td>Mobile based Authentication</td>
</tr>
<tr>
<td>Remote proofing using 2 IDs, confirmed address / phone number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirmed email address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Mobile based Authentication, Cloud based signing - consistent user experience.*
### High Level Description of Assurance Levels

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmed email address</td>
<td>In-person proofing, in-person antecedent - Remote -</td>
<td>In-person proofing, no in-person antecedent - KIOSK -</td>
</tr>
</tbody>
</table>

#### Enrollment channels

<table>
<thead>
<tr>
<th>Collected Attribute Categories*</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Basic personal Info</td>
</tr>
<tr>
<td>• Contact info (Email + Mobile)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example of Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Informative services</td>
</tr>
<tr>
<td>• Public services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signing Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• N/A</td>
</tr>
</tbody>
</table>

#### Requires remote or agent validation

<table>
<thead>
<tr>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and laptop requires validation APIs, and/or remote agent validation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA agent and Kiosks requires Emirates ID card readers and validation with ICA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step-up Approach*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires Kiosk enrollment or RA with biometric</td>
</tr>
</tbody>
</table>

*) Details provided in subsequent pages

**Details:**
- **Level 1**
  - Confirmed email address
  - **Enrollment channels:**
    - Mobile and laptop
    - **Collected Attribute Categories:**
      - Basic personal Info
      - Contact info (Email + Mobile)
  - **Example of Use Cases:**
    - Informative services
    - Public services
  - **Signing Enrollment:**
    - N/A

- **Level 3**
  - In-person proofing, in-person antecedent - Remote -
  - Requires remote or agent validation
    - Mobile and laptop
    - **Collected Attribute Categories:**
      - Basic personal Info
      - Identification document info
      - Contact info (Email + Mobile)
  - **Example of Use Cases:**
    - Rentals, e.g. cars, apartments
    - Select government services
    - Using the any verified user authentication

- **Level 4**
  - In-person proofing, no in-person antecedent - KIOSK -
  - Requires Kiosk enrollment or RA with biometric
    - RA agent and Kiosks
    - Requires remote or agent validation
    - Mobile and laptop
    - **Collected Attribute Categories:**
      - All data from Emirates ID
      - Contact info (Email + Mobile)
      - Additional bespoke data, e.g. AD gov data
  - **Example of Use Cases:**
    - Establishing business, e.g. EODB
    - High values assets transfer, e.g. real estates
    - Banking
    - Emirates ID Biometric verification

---

*) Details provided in subsequent pages*
Kiosk authentication enrollment for Level 4 users

Verified Authentication Credentials

User visits a kiosk for high level of authentication

User authenticates with his fingerprints

Kiosk allows for increase in assurance or new user

User add email and phone numbers

User gets his enrollment code ...

... and enroll the device

Multiple steps

Authentication keys activated
**Level 4 Signing keys enrollment – For verified users (Level 4) only**

**High Level Signing Credentials**

- **User selects to create a High level of assurance signature**
- **User enters the his signing password**
- **User creates his signature credentials – Signing keys pending kiosk activation**
- **User visits a kiosk for signing key activation**
- **User authenticates with his fingerprints**
- **Kiosk detects pending signing key for confirmation**

**Level 4 Signing keys enrollment**

- For verified users (Level 4) only
Authentication enrollment for Level 3 users – Example of remote verification

Verified Authentication Credentials

User fills the required information, click on next

User makes a copy of the ID using the mobile camera

User makes a selfie picture or video

User receives a notification, along with the enrollment code

Remote agent checks and approve the user

User enters the enrollment code to get the credentials
Level 3 Signing keys enrollment – For verified users (Level 3-4) only

Medium Level Signing Credentials

User selects to create a Medium level of assurance signature

User enters the his signing password

User creates his signature credentials ready to be used – **Signing keys enabled**

Prerequisites:
- Verified user with mobile enrolled
ICA Toolkit enrollment for Level 1 users

Mobile Enrollment – Level is based on ICA SDK

Using Emirates ID, user can enroll with an NFC enabled mobile.

The mobile load the user information

The user confirms the information (or cancels)

The user enters their email and mobile numbers for verification

The user is enrolled with basic level of assurance – **Authenticate enabled**

Prerequisites:

- ICA SDK for android phones
- Android phone with NFC
Kiosk upgrade to Level 4 users

Verified Authentication Credentials

User visits a kiosk for high level of authentication

User authenticates with his fingerprints

Kiosk allows for increase in assurance or new user

User authenticates and confirm profile upgrade

User gets new enrollment code ...

... and enroll the device

Certification Authorities issues new keys and certificates
To Successfully Digitize a Nation Requires several elements to be present:

• National PKI service to enable digital Trust Services (Confidentiality/Integrity/Assurance)

• **National Certification Policy** (CP) to define the basis upon which the NPKI operates

• National Digital Identity services to enable the highest assurance of participants in the digital economy

• National Digital Signature services to facilitate digital processes and transactions

• **Legal Recognition** of Digital Identities and Digital Signatures as equivalent to their analog counterparts

• An **Accreditation and Audit scheme** to ensure the veracity of TRUST in the system
DIGITALTRUST : UAE TRUST SERVICES PROVIDER

• DigitalTrust is appointed by TRA as the UAE NPKI Operator

• DigitalTrust was the Solution Architect and System Integrator for TRA & Smart Dubai’s implementation of UAEPASS

Scott Rea
Head of DigitalTrust
Level 12, Aldar HQ
PO Box 113979
Abu Dhabi, UAE

https://digitaltrust.ae
scott.rea@digitaltrust.ae