



Implementation of Lebanon's National Digital Transformation Strategy

Workshop 1

June 12, 2024

DAY 2

AGENDA

A Introduction to e-signature

B Domain 1: Public Sector

C Domain 2: Private Sector

D Domain 3: Financial sector

OVERVIEW OF THE ELECTRONIC SIGNATURE LANDSCAPE IN THE PUBLIC AND PRIVATE SECTORS







INTRODUCTION TO E-SIGNATURE

Introduction to e-signature



LEVELS OF ASSURANCE IN PRACTICE

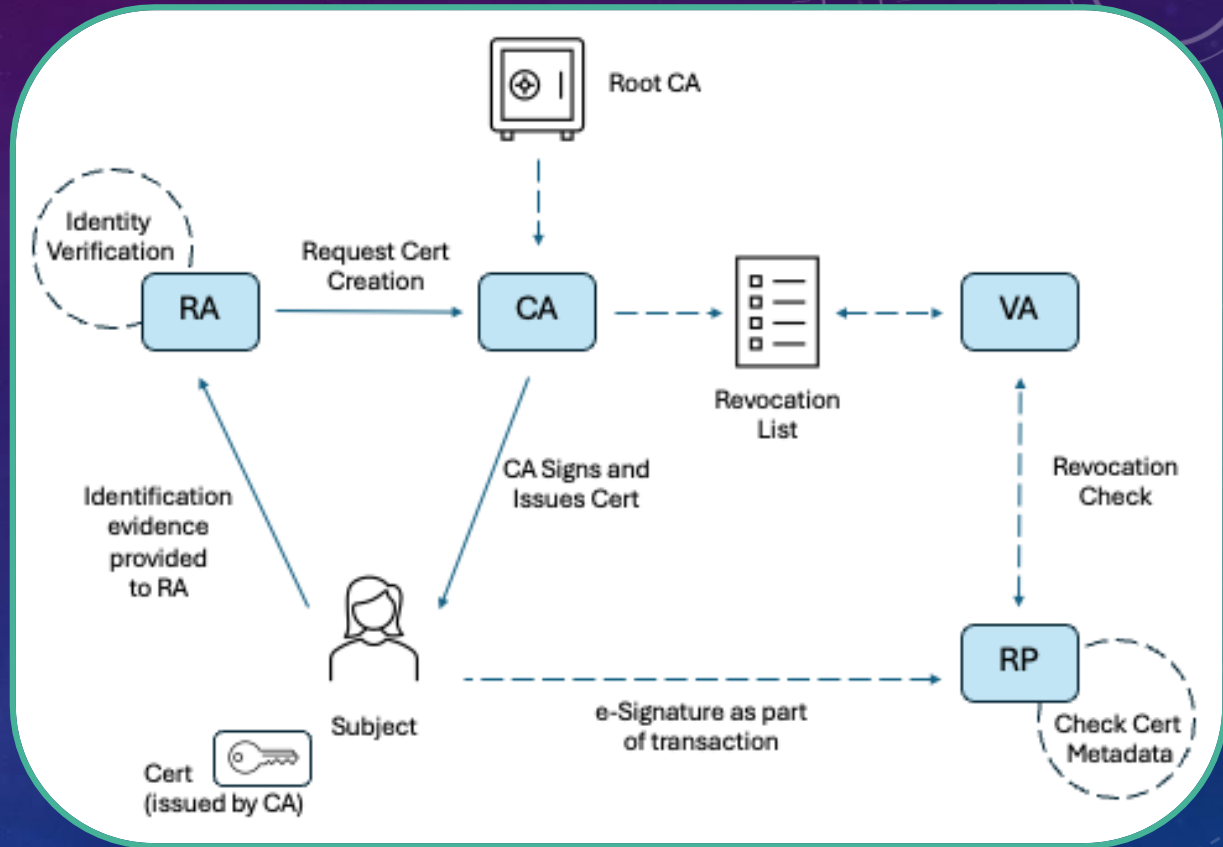
The example of the European eIDAS regulation

		Level of assurance		
		Low	Medium	High
	Signer identity	none	Signer can be identified	Signer can be identified
	Data integrity	none	Modifications after signing detectable	Modifications after signing detectable
	User onboarding	none	none	Identity verification done face to face
	Technology	none	none	Digital certificate (PKI)
	Certificate issuer	none	none	Audited for compliance with rigorous standards
	Signing device	none	none	High security device from approved list

IMPLEMENTING QUALIFIED E-SIGNATURE

Data integrity is a common use of e-signatures to ensure that transactions are tamper evident.

E-signatures also form the basis of privacy preserving technologies and digital proofs for verifiable credentials.



INTRODUCTION TO E-SIGNATURE

Certificates can be issued by a government CA or a commercial CA depending on the Trust Framework.

THE E-SIGNATURE OF OFFICIAL DOCUMENTS SERVES AS A PIVOTAL CATALYST FOR THE DEVELOPMENT OF DIGITAL SERVICES IN THE PUBLIC SECTOR

Presentation of example use cases

Non-exhaustive

→ Use cases addressed refer to the signature of public administration documents and certificates




Civil status



-  **Identity documents** (passport, national ID card issuance and renewal forms, driver's license applications and renewals...)
-  **Life events** (signing, approving and issuing birth certificates, marriage certificate, criminal records.....)
-  **Civic acts documents** (voter registration forms o, voting records, residency permit applications...)

Certificates & recognition documents



-  **Healthcare documents** (signing social security card applications, approving vaccination records...)
-  **Education** (signing diplomas and academic certificates, approving school certificates and transcripts...)
-  **Licensing & permits** (approving professional license applications, signing building permits and other construction-related documents...)

Judiciary & notary



-  **Court documents** (signing court settlements and affidavits, approving and issuing court orders...)
-  **Notary documents** (signing wills and testaments, approving powers of attorney...)

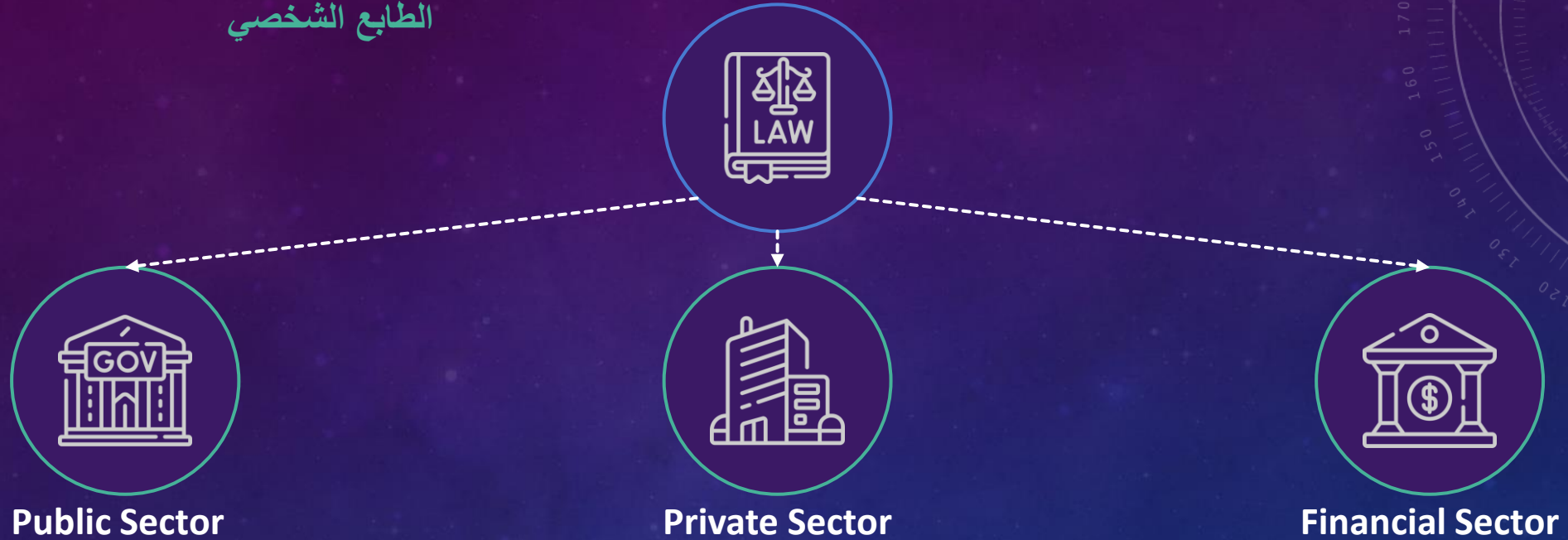
Administration



-  **Public contracts** (signing procurement contracts, approving tenders & PPP agreements...)
-  **HR management** (signing employment contracts for civil servants, approving NDAs...)
-  **Official correspondence** (signing internal communications between public administrations, official correspondence with embassies...)

INTRODUCTION TO E-SIGNATURE IN LEBANON: 3 DOMAINS

قانون رقم ٨١ / ٢٠١٨ المعاملات الإلكترونية والبيانات ذات الطابع الشخصي
Law 81-2018 /



Examples:



Official document



Contract



Payment

Annex: Translation of key technical terms from Law 81/2018

Original Arabic (in law 81)	Arabic Transliteration	Original English (in law 81)	SMEX unofficial translation ¹⁶	Standard English terminology	Standard English definition
شهادة مصادقة	shahadat moussadaqa	N/A	"Certificate of Authentication"	Digital Certificate	Digital documents (issued by CAs/TSPs) that securely associate cryptographic key pairs, which can be used for digital signing, with identities, such as individuals or organizations.
مقدم خدمات مصادقة	mouqaddem khadamat moussadaqa	"Certification Service Provider"	"Service Provider" and "Authentication Service Provider" used interchangeably	Certification Authority (CA)	A Certification (or Certificate) Authority (CA/TSP) is a trusted entity that issues digital certificates.
شهادة اعتماد	shahadat i3timad	N/A	"Accredited certificate"	Accreditation	The process through which a CA/TSP is receives accreditation as per law allowing it to issue trusted digital certificates in a given regulatory environment. Not all regulatory frameworks require an <i>ex-ante</i> accreditation process as a condition for digital certificate issuance for all levels of assurance.
مقدم خدمات مصادقة معتمد	mouqaddem khadamat moussadaqa mou3tamad	N/A	"Authorized Authentication Service Provider"	Accredited (or Authorized / Approved) Certification Authority ¹⁷	Accredited (or Authorized or (Approved) CAs (or TSP), which can issue certificates that can be used for electronic signature creation. The approval may require a formal accreditation process depending on regulation.
مقدم خدمات مصادقة غير المعتمد	mouqaddem khadamat moussadaqa ghayr al mo3tamad	N/A	"Unauthorized Authentication Service Provider"	Certification Authority (that has not undergone an accreditation process)	CAs (TSP) that have not undergone an accreditation process to issue high-trust digital certificates. Accreditation may not be a requirement to provide e-signature services in a given regulatory regime.

DEMYSTIFYING LAW 81'S TERMINOLOGY

DOMAIN 1: PUBLIC SECTOR

WHY IS THE LAW IMPORTANT FOR E-SIGNATURE ANYWAY?

لماذا يعتبر القانون مهماً للتوقيع الإلكتروني؟

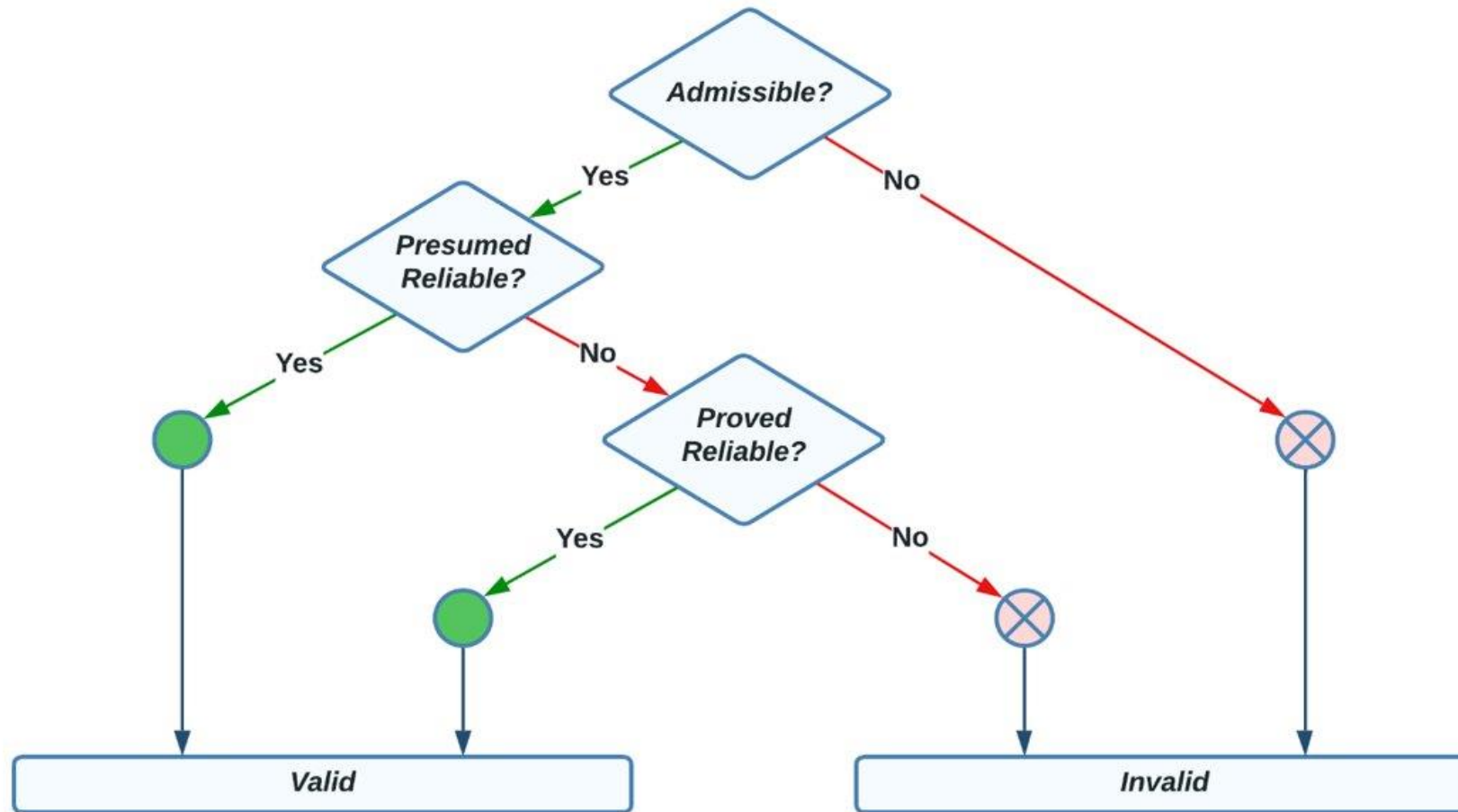
قبول التواقيع
الإلكترونية كدليل
في المحكمة

*Admissibility
of Evidence*

ضمان موثوقية
التواقيع
الإلكترونية
Reliability

اعتبارها موازية
للتواقيع اليدوية
*Functional
equivalence*

TECHNICALLY, COURTS WILL LOOK AT IT THIS WAY:



RELEVANT ARTICLES FROM LAW 81-2018

المادة ٤:

تنتج الكتابة والتوقيع الإلكتروني ذات المفاعيل القانونية التي تتمتع بها الكتابة والتوقيع على دعامة ورقية أو أي دعامة من نوع آخر، شرط أن يكون ممكناً تحديد الشخص الصادرة عنه، وأن تنظم وتحفظ بطريقة تضمن سلامتها.
يمكن أن تعتبر بداية بيئة خطية كل كتابة الكترونية لا تتوافر فيها الشروط المذكورة اعلاه.

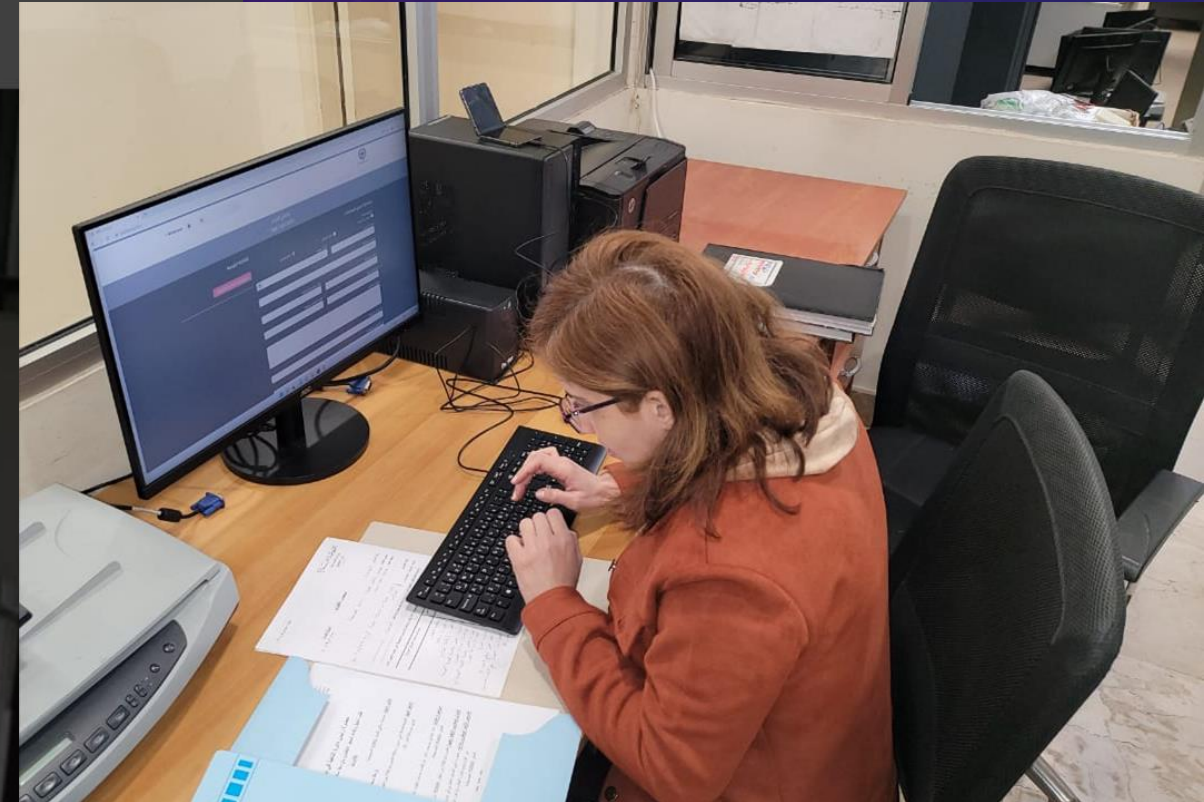
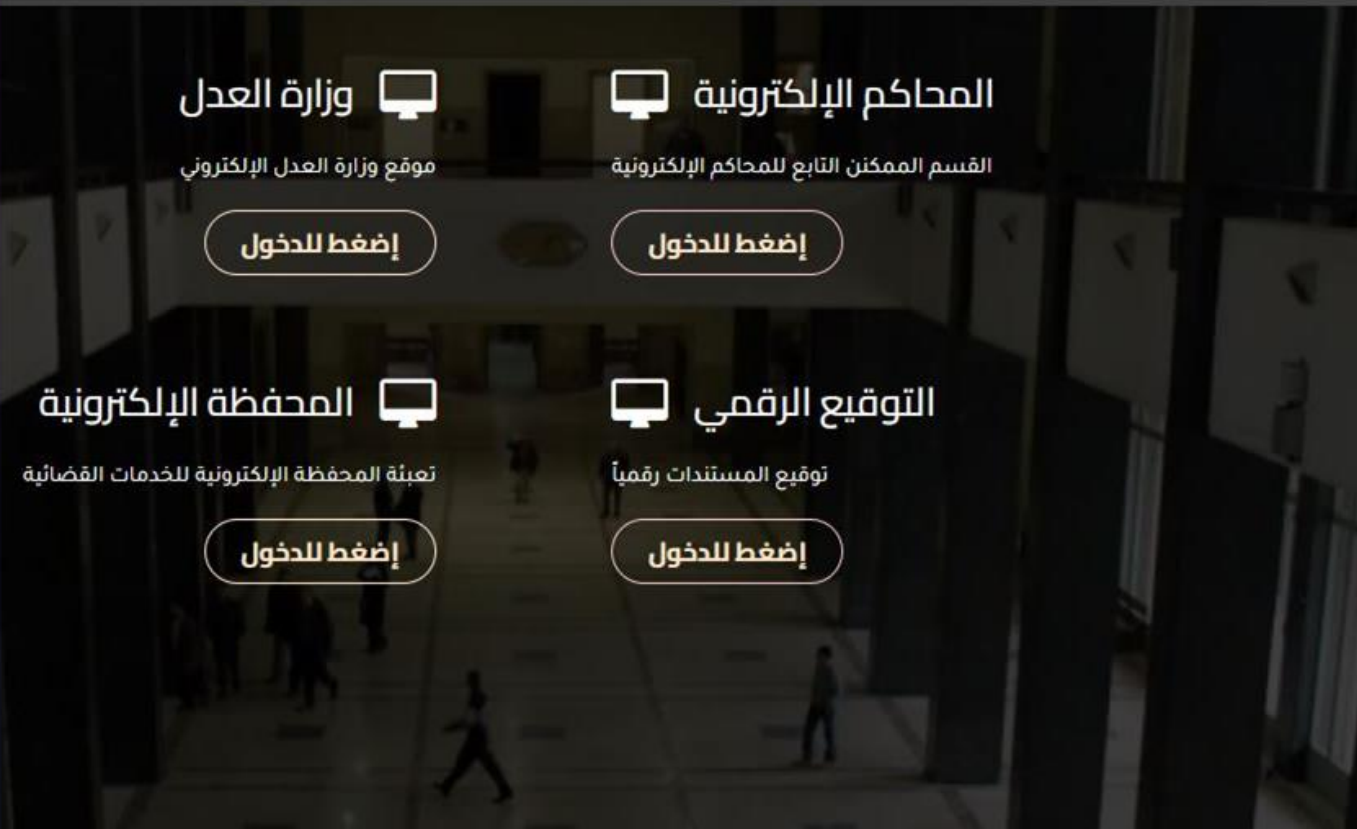
المادة ٨:

لا تنتج الاسناد الرسمية الإلكترونية أية مفاعيل قانونية إلا بعد إقرارها وتنظيمها بمرسوم يتخذ في مجلس الوزراء بناء على اقتراح وزير العدل.
ينظم هذا المرسوم الإجراءات الخاصة والضمانات المتعلقة بهذه الاسناد ونطاقها.

E-COURTS SERVICES

DIGITAL ID - QUALIFIED SIGNATURE

IMPLEMENTATION OF QUALIFIED SIGNATURE IN COURTS



Service Provider

- Digital ID
- Digital Signature
- Cyber Security

E-Court System

- Case Management
- Court E-Wallet
- Portal Access

Inter-Operability

- Ministry of Finance
- ISF
- NSSF
- Others

Service Provider

- Digital ID
- Digital Signature
- Cyber Security

The screenshot displays the CIELTEC user interface. At the top, there are navigation links for "Groups" (52), "Access Rights" (1,182), and "Record Rules" (222). The user is logged in as "SJC ADMIN". The main menu includes "Access Rights", "Preferences", and "Account Security". The "LOCALIZATION" section shows "Language" set to "English (US)", "Timezone" set to "Asia/Beirut", and "Notification" set to "Handle by E". The "Email Signature" field is currently empty, with a placeholder text "Administrator". The "DIGITAL SIGNATURES" section shows a "Digital Signature" field with a large, stylized blue signature "SJC ADMIN". On the right side, there is a "Log in to Ciel" section with fields for "Username" and "Password", a "LOG IN" button, and a link for "Forgot Password?". Below the login section, there is a link for "Don't have an account? Sign Up".

- Case Management
- Court E-Wallet
- Portal Access

القضايا
القضايا والمعاملات المرتبطة بالحساب
الإلكتروني



المحاكم
المحاكم ذات الصلة بالحساب الإلكتروني



Courts

دائرة تنفيذ بيروت

Set Status

Search...

1-80 / 776

< >

Menu Icons

العناوين
قم بإضافة



الموظف	D	القاضي	تاريخ الورد	الأساس	Title	Tags	Stage
<input type="checkbox"/> محمد الحلبي	<input checked="" type="checkbox"/>	مريانا عناني	06/06/2024	304	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> أحمد كالوت	<input checked="" type="checkbox"/>	مريانا عناني	09/05/2024	304	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> أحمد فواز	<input checked="" type="checkbox"/>	نجاح عيتاني	06/06/2024	303	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> نسرين حصروني	<input checked="" type="checkbox"/>	كالين عبد الله	09/05/2024	303	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> نسرين حصروني	<input checked="" type="checkbox"/>	كالين عبد الله	05/06/2024	302	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> نسرين حصروني	<input checked="" type="checkbox"/>	ميرنا كلاب	09/05/2024	302	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> زكية عيسى	<input checked="" type="checkbox"/>	فيصل مكى	09/05/2024	301	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> رنا بدر	<input checked="" type="checkbox"/>	نجاح عيتاني	05/06/2024	301	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> نبيل ناعوس	<input checked="" type="checkbox"/>	ميرنا كلاب	05/06/2024	300	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> زكية عيسى	<input checked="" type="checkbox"/>	مريانا عناني	09/05/2024	300	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> ودي القرى	<input checked="" type="checkbox"/>	فيصل مكى	04/06/2024	299	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> إزدهار عاصي	<input checked="" type="checkbox"/>	ميرنا كلاب	08/05/2024	299	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> أحمد فواز	<input checked="" type="checkbox"/>	مريانا عناني	04/06/2024	298	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> شفيق جوزو	<input checked="" type="checkbox"/>	نجاح عيتاني	08/05/2024	298	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة
<input type="checkbox"/> رنا بدر	<input checked="" type="checkbox"/>	نجاح عيتاني	04/06/2024	297	شاتيل / حامد	حج تنفيذي	☆ معاملة جديدة
<input type="checkbox"/> زكية عيسى	<input checked="" type="checkbox"/>	كالين عبد الله	08/05/2024	296	شاتيل / حامد	احال, شخصية	☆ معاملة جديدة

المعرفة
إليك كافة



New Webhook Automations
New ⚙️

☰ Logs

Inter-Operability

- Ministry of Finance
- ISF
- NSSF
- Others

Support flow

Model ? Project

Trigger ? On webhook ▼

Target Record ?

URL ? <https://www.courtlb.org/web/hook/b3ee8e85-9a34-4a3e-b1fa-dc2af532356e>

📄 Copy

🔒 **Keep it secret, keep it safe.**

Your webhook URL contains a secret. Don't share it online or carelessly.

🔄 Rotate Secret

Log Calls ? ☐

Actions To Do

Notes

Add an action



E-COURTS SERVICES LAUNCH DATE

15/9/2024

DOMAIN 2: PRIVATE SECTOR

THE E-SIGNATURE OF OFFICIAL DOCUMENTS SERVES AS A PIVOTAL CATALYST FOR THE DEVELOPMENT OF DIGITAL SERVICES IN THE PRIVATE SECTOR

Presentation of example use cases

Non-exhaustive

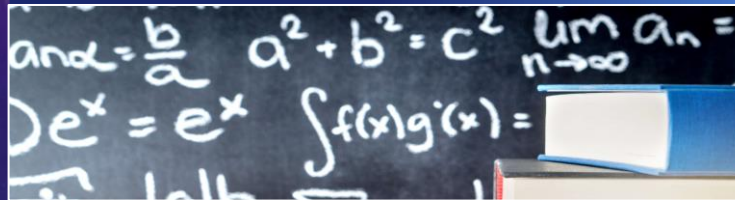
→ Use cases addressed refer to the signature of private sector documents and contracts

Health



- **Health screenings** (health history questionnaires, surveys)
- **Consent for medical procedures**
- **Prescriptions** for controlled substances
- **Consent for medical directives with legal implications** (end-of-life decisions, complex directives)
- **Agreements for clinical trials or medical research**
-

Education



- **Course enrollment**
- **Student registration forms**
- **Online exam submissions**
- Approving **student loan applications** and financial aid documents
- Signing **internship agreements & placement forms**
- Approving and submitting **academic research papers and thesis documents**
- ...

Commerce



- **Online order confirmations**
- Acknowledging and accepting **terms and conditions**
- Signing **non-disclosure agreements (NDAs)**
- Signing and executing **typical contracts**
- Signing **deeds, mortgages, or other real property documents**

ZOOM ON GOVERNANCE

SOURCES OF TRUST

Pre-existing trust



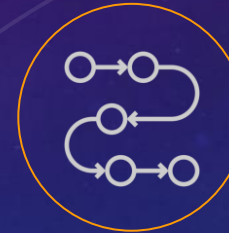
- Do I know you offline?
- Have we interacted successfully online before?
- Do we have a pre-existing contractual relationship?
- Are we members of the same professional body?
- Are we transacting on a secure communication channel?

Extension of trust



People

Providers of e-signature services are trusted and vetted.



Process

Identity checks carried out when onboarding a signer.



Technology

Technical measures to protect the integrity of the signed document

Extension of trust



People

Providers of e-signature services are trusted and vetted.



Process

Identity checks carried out when onboarding a signer.



Technology

Technical measures to protect the integrity of the signed document

TRUST FRAMEWORK

- Set **standards**
- Balance security and **usability**
- Clarify **roles** and responsibilities
- Promote **adoption**
- Risk-based **levels of assurance**
- **Flexible** to allow innovation
- Technology **neutral**

Legal effect

- Enforceability
- Admissibility as evidence
- Presumption of validity

Legal Framework



Trust Framework



Laws
Regulations

Mutual recognition

- Interoperability across sectors
- Scaling trust across borders

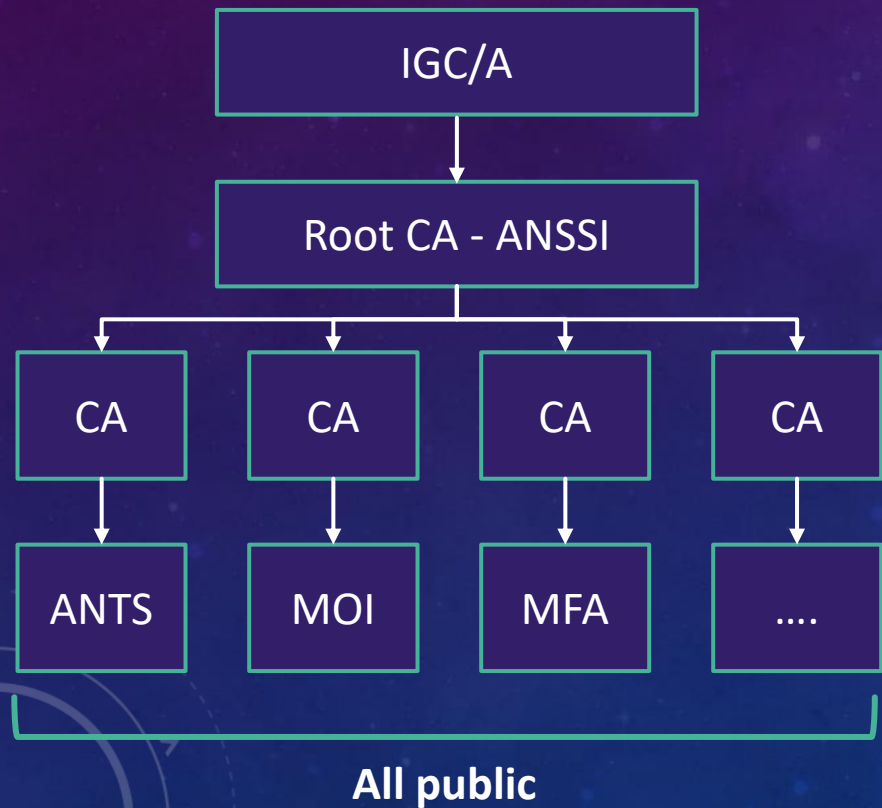
GOVERNANCE REGIME

Dimension		Authority level 	Example 
Law		 EU	eIDAS: Electronic Identification, Authentication and Trust Services.
Standards/guidance			ETSI: European Telecommunications Standards Institute
Supervisor		 France	ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information (National Agency for the Security of Information Systems).
Accreditor			COFRAC: Comité Français d'Accréditation (French Accreditation Committee)
Auditor			3 private providers
Certification authority			30 private and public providers
Certificate			User

FRANCE CASE STUDY

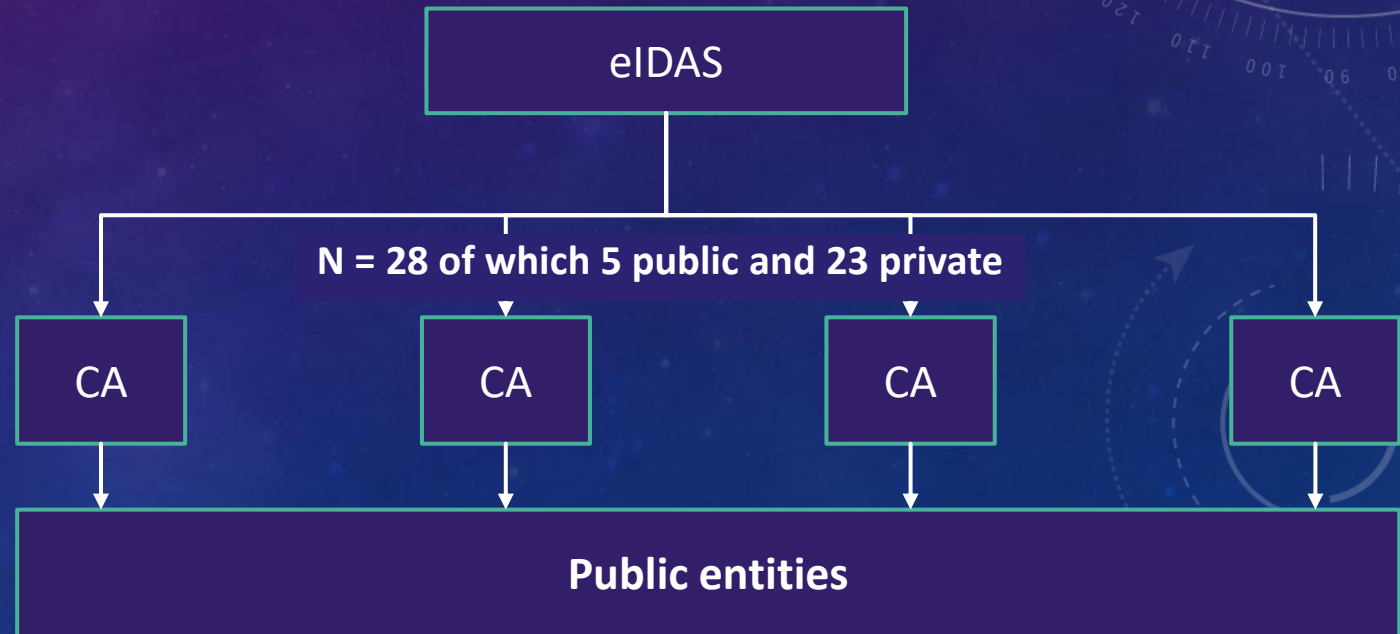
Minority use cases for example inter-ministerial communications

France



Majority use cases

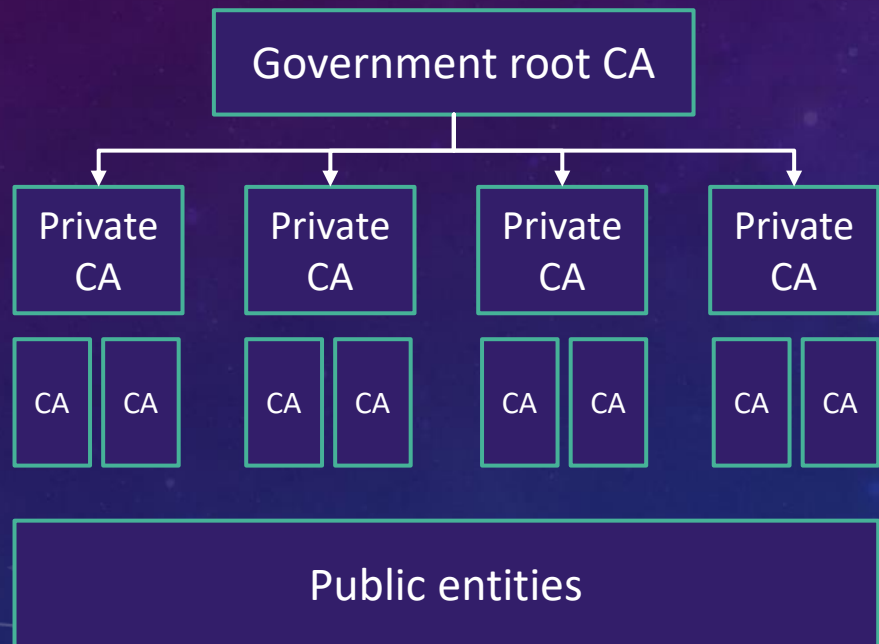
European Union



NETHERLANDS CASE STUDY

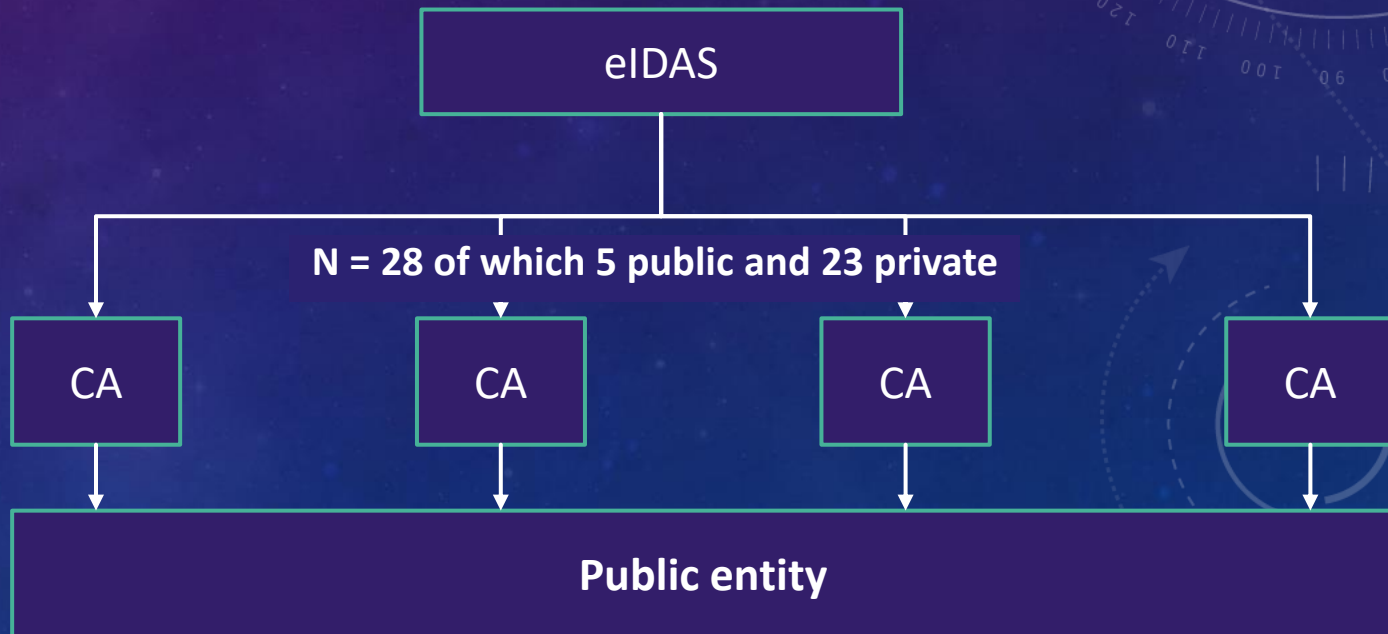
Public Sector

Netherlands



Private Sector

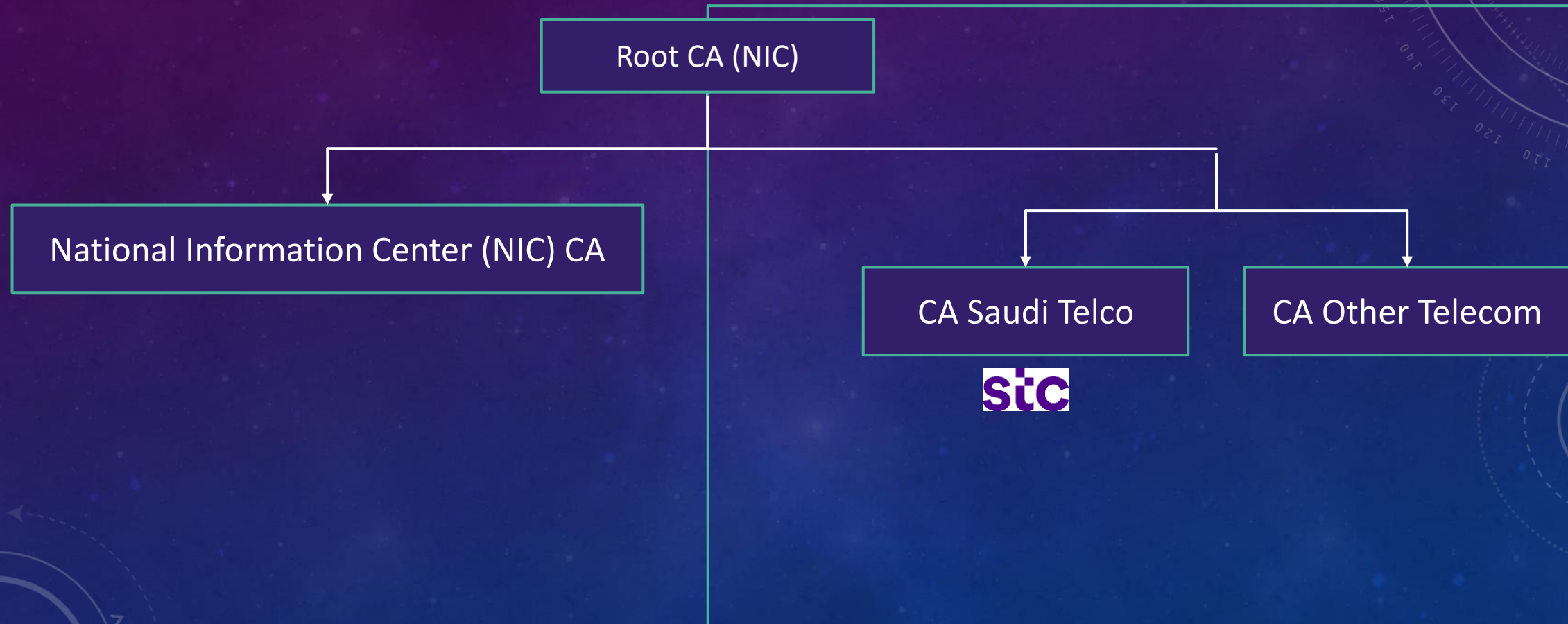
European Union



SAUDI ARABIA CASE STUDY

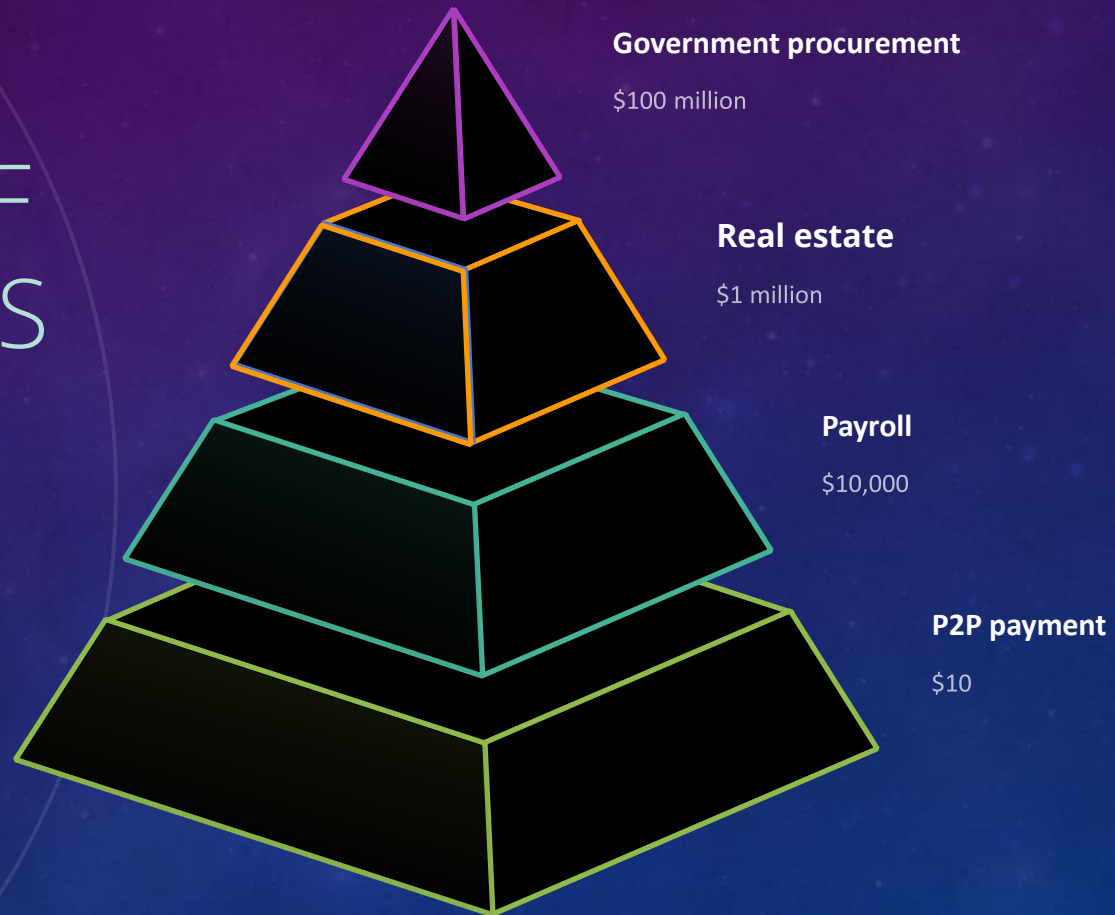
Public Sector

Private Sector



USE CASES OF E-SIGNATURES

The majority of e-signature use cases are relatively low risk. However, very high value transactions can also be signed electronically if there is enough trust.

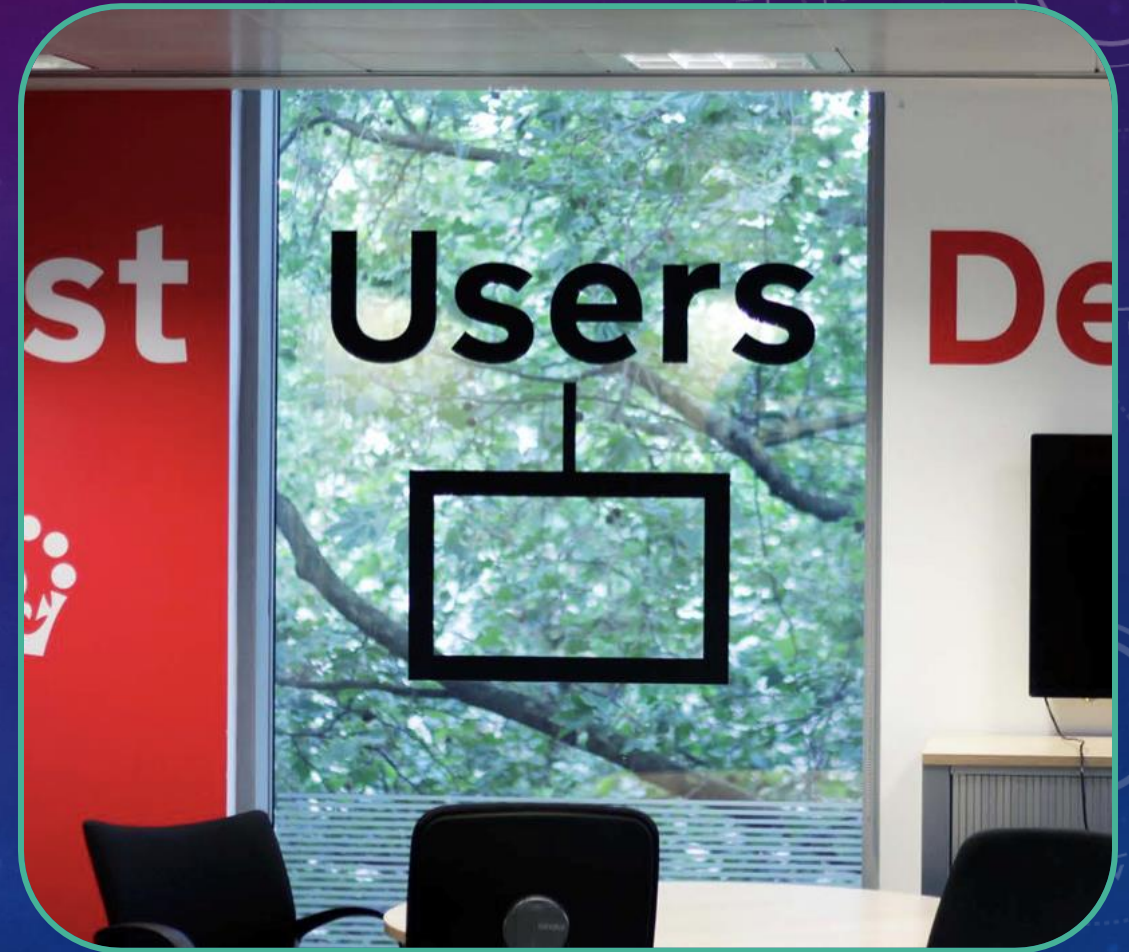


DOMAIN 3: FINANCIAL SECTOR

DIGITAL ID AS AN ENABLER FOR DIGITAL TRANSFORMATION

Digital ID is the great enabler. It makes it possible for individuals to engage with digital transactions remotely and at high levels of trust.

Being able to reliably prove who we are also means that **trusted data** can be shared as part of these **rich transactions**.



e-KYC and Digital Signatures Policy Aspects and International Experience

Fredesvinda Montes,
Senior Financial Sector Specialist, The World Bank

Lebanon, June 2024



FATF DIGITAL ID GUIDANCE: RECOMMENDATIONS

E-KYC means establishing business relationships and conducting customer due diligence (CDD) by way of electronic means, including online channel and mobile channels.



Authorities

1. Develop clear guidelines allowing the risk-based use of reliable and independent Digital ID systems by entities regulated for AML/CFT purposes.
2. Assess existing regulations so that non-face to face onboarding may be standard or low risk when a Digital ID with appropriate levels of assurance are used for remote identification/verification.
3. Adopt principles, performance, and/or outcomes-based criteria
4. Develop an integrated multi-stakeholder approach to understanding and mitigating risks.

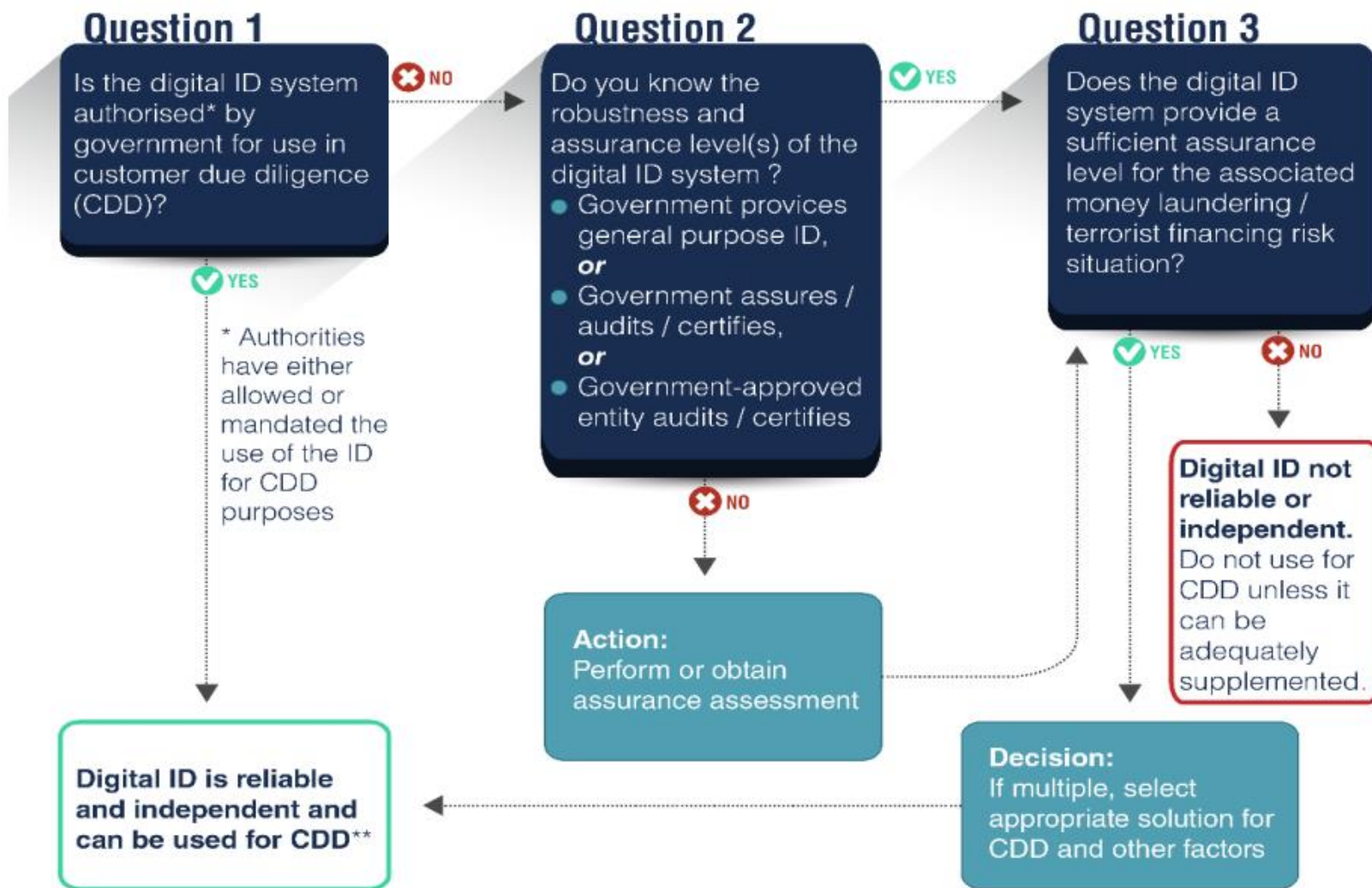
Regulated Entities

1. Take informed RBA to relying on Digital ID systems for CDD that includes;
 - Understanding LoAs for identity proofing and authentication
 - Ensuring that the LoAs are adequate to the jurisdiction, product, customer etc.
2. Consider if ID systems with lower LoA may be appropriate for SCDD in cases of low ML/TF risk.
3. Review policies if non-face to face onboarding or transactions are always considered high risk even when relying on Digital ID.
4. Adopt anti-fraud and cybersecurity measures
5. Enable a process for authorities to obtain, the underlying identity information needed for identification and verification of individuals.

ID Providers

1. Understand the AML/CFT requirements for CDD
2. Seek assurance testing and certification by the government or an approved expert body
3. Provide transparent information to AML/CFT regulated entities and foster federation and interoperability

DIGITAL ID GUIDANCE: ASSURANCE DECISION FRAMEWORK



** additional information or risk mitigation measures may be required

International harmonization of e-Commerce law

- **UNCITRAL Model Law on Electronic Commerce (1996)** text and list of enacting states available at www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
- **UNCITRAL Model Law on Electronic Signatures (2001)** text and list of enacting states available at www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- **United Nations Convention on the Use of Electronic Communications in International Contracts (2005)** text and list of signatory states available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Co

Types of Signatures



HANDWRITTEN SIGNATURE

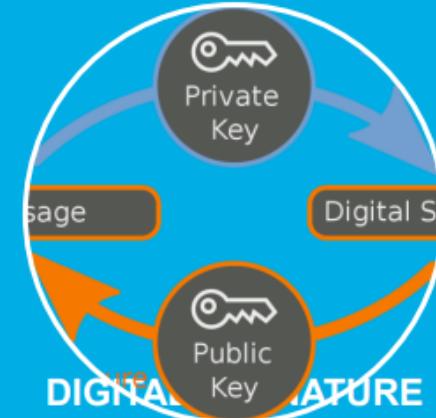
Objective; Proof the intent to approve the content of a document

- (i) Requires presence of the signee;
- (ii) Can be easily forged or tampered;
- (iii) Can be held upon in Court



ELECTRONIC SIGNATURE

- (i) Electronic representation of a signature
- (ii) does not confirm the content of the document
- (iii) does not provide security and assurance



DIGITAL SIGNATURE

(i) Scheme used to authenticate the sender of an electronic document

(ii) Requires a PKI Infrastructure

(iii) The document is authentic and comes from a verified source

(iv) The document has not been tampered with since being digitally signed as the signature would be displayed as invalid if changes were made

(v) The identity has been verified by a trusted organization (the CA)

Identification (=be recognized) Vs Authentication (=be in possession of credentials)

Key Elements of a Signature

- **ANALOGIC ENVIRONMENT-** When a document is signed before a notary public (notary or public broker), the signatures contained therein acquire a presumption of attribution and, therefore, the document as a whole obtains a presumption of integrity. It is considered complete and authentic. In other words, the **intervention of a public notary confers validity and authenticity to the document.**

- **DIGITAL ENVIRONMENT-** Model Law on Electronic Signatures, article 6(3) (Compliance with requirement for signature):
 - (a) signature creation data must be linked to the signatory and to no other person;
 - (b) signature creation data must be under the control of the signatory at the time of signing;
 - (c) alterations to the electronic signature made after the time of signing must be detectable;
 - (d) where legal signature requirement aims at assuring integrity of the information, any alteration to the information must be detectable.

Legal Approach to e-signature

Prescriptive

- Specific technology
- Typically, digital signature

Argentina, Brazil, Chile, Tunisia, South Africa, Japan

2 tier Approach

- Legal presumption on one technology
- Accepts others

Spain, UK, France, NL, Mexico, Singapore, Thailand

Principle Based

- Sets requirements
- Technology neutral
- Flexibility of adoption

Australia, Canada, New Zealand US

Levels of Digital Signature

1. **Digitized Signature** (so-called also electronic signature): an electronic representation (applied image) of a handwritten signature. The image may be created by various methods, such as a signature pad, scanning a wet signature, or digital photography. Lowest level of assurance
2. **Electronic Signature** means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. **Button, PIN, Biometric, or Token:** a frequently used e-signature methodology includes clicking a button or entering a unique personal identification number (PIN), electronic identification, token, or biometric scan at the completion of an entry for the signature process. Medium level of assurance. It very much depends on the authentication factors selected.
3. **Digital Signature:** a digital signature is a cryptographic signature (a digital key) that authenticates the user, provides nonrepudiation, and ensures message integrity. This is the strongest signature because it protects the signature by a type of tamper-proof seal that breaks if the message content were to be altered. Highest level of assurance

Authentication Mechanisms (ID4D)

Type	Mechanism	Compatible Credentials/Authenticators	System Requirements
Matching against a database	Comparison of authentication factors to references stored in a central system	Numbers, user names, etc. + authenticators (e.g., PIN, biometric, password)	Input devices (i.e., keypad/board and/or biometric scanners) and secure network connection of relying party to central system
Public key infrastructure (PKI)-based	Using public key encryption to authenticate against a server	Smartcard, card with 2D barcode, SIM card, or mobile device + authenticators (e.g., PIN, biometric)	Input devices (i.e., personal card reader/scanner, text pads and/or fingerprint scanners), PKI and secure network connection of relying party to central system
One-time passwords (OTP)	Password or PIN generated on demand for one-time use	Device that can receive the password (e.g., SMS on a mobile phone or smartphone/computer to receive an email or smartphone app that generates an OTP)	OTP infrastructure and secure network connection of relying party to central system
FIDO authentication	On-device match (fingerprint, iris, face, PIN) unlocks a private key used to authenticate against a server	FIDO-certified smartphone (e.g., Android, Windows) or external authenticator such as a FIDO Security Key + authenticators (biometrics or PIN)	FIDO-certified smartphone (e.g., Android, Windows) or external authenticator such as a FIDO Security Key, plus network connection between that device and the relying

Guidance on Authentication; How is it done in practice

Something a person ...

Has	Knows	Is
 <ul style="list-style-type: none"> • Card • Certificate • Security token • Mobile app • Access badge 	 <ul style="list-style-type: none"> • Password • Passphrase • PIN • Challenge-response • Other secret 	 <ul style="list-style-type: none"> • Fingerprint • Irises • Face • Behavior • Biographic data

Reduce Risk
of Fraud

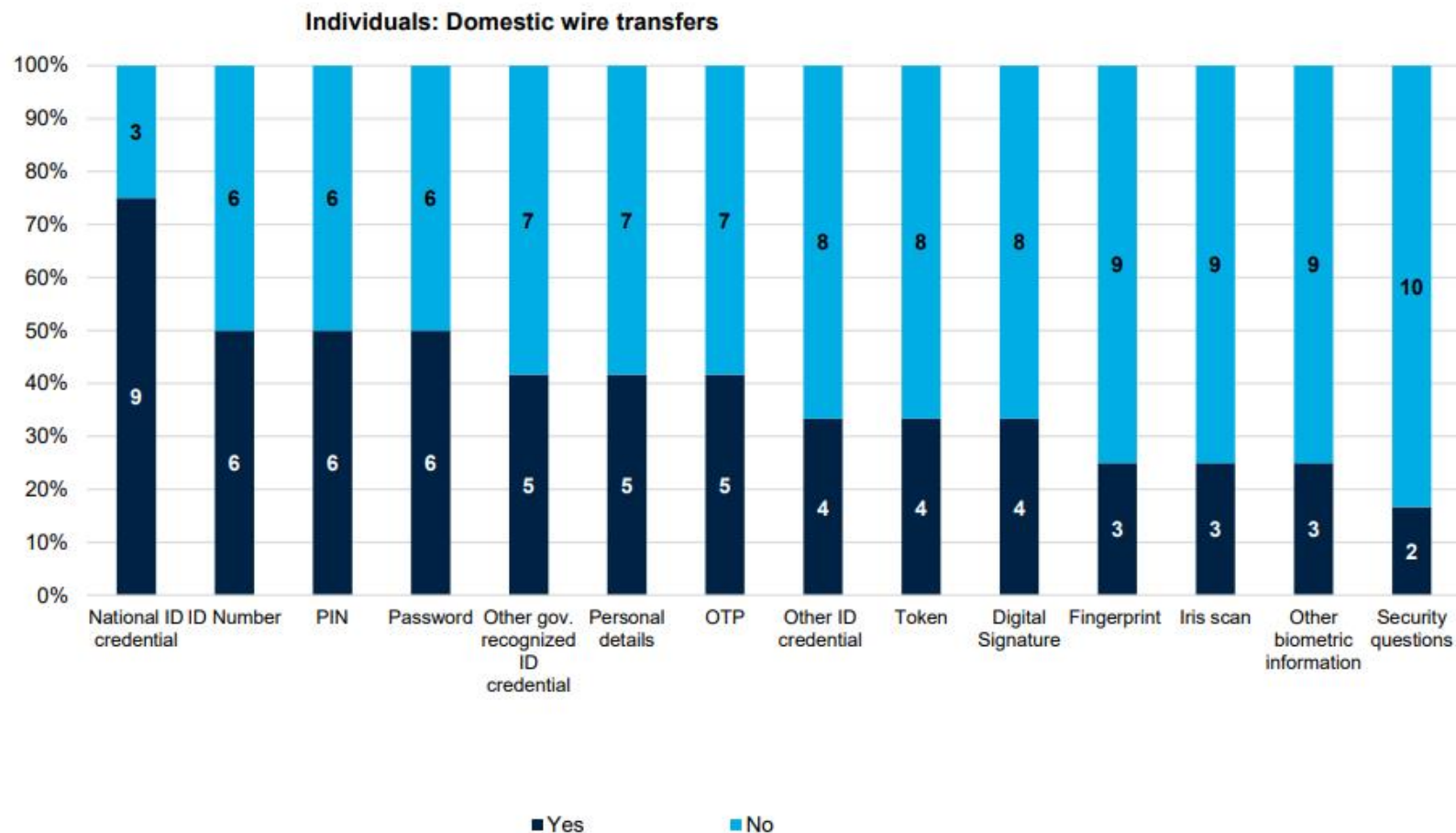
Assurance that the individual asserting identity for account authorization controls an authenticator(s) bound to the subscriber's account

	LOW	SUBSTANTIAL		HIGH	eIDAS Definition	
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 3	LEVEL 4	ISO 29115
	<p>Weak Authentication</p> <p>Legacy Password</p>	<p>Secure Authentication</p> <ul style="list-style-type: none">• Seamless• SMS+URL• USSD• SIM Applet• Smartphone App• Token or OTP	<p>Strong Authentication</p> <ul style="list-style-type: none">• USSD• SIM Applet• Smartphone App• Token OTP + pw• Biometrics	<p>Strong Authentication</p> <ul style="list-style-type: none">• SIM Applet• Smartphone App in TEE• Token OTP (PIN + certified TEE or SE)• Biometrics	<p>Very Strong Authentication</p> <ul style="list-style-type: none">• SIM Applet with PKI• Smartphone App in TEE with PKI• PKI eID (PIN)• PKI ID (PIN + SE (SIM /eSE)• Biometrics	Authentication/ electronic ID
	No Identity Proofing	Presentation of identity information	Verification of Identity information		In-person registration with verification	Identity Proofing During Registration
	EXTREMELY HIGH	MITIGATED	LOW	MINIMAL		Risk Level

Use cases

Type of Service	Low/Medium LA	High LA
Deposit	Individuals	Legal entities
Savings	Online transactions	
Payments	Basic accounts, fund transfers	Cross-border payments Wire transfers (except credit cards)
Credit and Loan Services	Loan application, credit cards	Mortgage, vehicle, Loans, commercial loans
Wealth Management		Trusts, stock account opening, retirement mutual funds
Insurance	Application, renewal, coverage changes	
	e-signatures accepted	Digital signatures required

Types of Authentication Factors Used



Annex: Translation of key technical terms from Law 81/2018

Original Arabic (in law 81)	Arabic Transliteration	Original English (in law 81)	SMEX unofficial translation ¹⁶	Standard English terminology	Standard English definition
شهادة مصادقة	shahadat moussadaqa	N/A	"Certificate of Authentication"	Digital Certificate	Digital documents (issued by CAs/TSPs) that securely associate cryptographic key pairs, which can be used for digital signing, with identities, such as individuals or organizations.
مقدم خدمات مصادقة	mouqaddem khadamat moussadaqa	"Certification Service Provider"	"Service Provider" and "Authentication Service Provider" used interchangeably	Certification Authority (CA)	A Certification (or Certificate) Authority (CA/TSP) is a trusted entity that issues digital certificates.
شهادة اعتماد	shahadat i3timad	N/A	"Accredited certificate"	Accreditation	The process through which a CA/TSP is receives accreditation as per law allowing it to issue trusted digital certificates in a given regulatory environment. Not all regulatory frameworks require an <i>ex-ante</i> accreditation process as a condition for digital certificate issuance for all levels of assurance.
مقدم خدمات مصادقة معتمد	mouqaddem khadamat moussadaqa mou3tamad	N/A	"Authorized Authentication Service Provider"	Accredited (or Authorized / Approved) Certification Authority ¹⁷	Accredited (or Authorized or (Approved) CAs (or TSP), which can issue certificates that can be used for electronic signature creation. The approval may require a formal accreditation process depending on regulation.
مقدم خدمات مصادقة غير المعتمد	mouqaddem khadamat moussadaqa ghayr al mo3tamad	N/A	"Unauthorized Authentication Service Provider"	Certification Authority (that has not undergone an accreditation process)	CAs (TSP) that have not undergone an accreditation process to issue high-trust digital certificates. Accreditation may not be a requirement to provide e-signature services in a given regulatory regime.

DEMYSTIFYING LAW 81'S TERMINOLOGY

RELEVANT ARTICLES FROM LAW 81-2018

المادة ٤٨:

تُعطى أوامر إجراء عمليات الدفع والتحويلات الإلكترونية للأموال النقدية، كتابةً، موقعة يدوياً أو إلكترونياً تحت طائلة بطلانها.
إذا تم إعطاء هذه الأوامر وتوقيعها إلكترونياً، يجب أن يكون هذا التوقيع مصادقاً عليه وفق القواعد الصادرة عن مصرف لبنان.

المادة ١٣٣:

استثناء لما ورد في المادة ٢٠ وما يليها من مواد واردة في الفصل الرابع من هذا القانون، يعود لمصرف لبنان، في ما يتعلق بالعمليات المالية والمصرفية اعطاء:

- ١- شهادات المصادقة العائدة للتوقيعات الإلكترونية للمصارف وللمؤسسات الخاضعة لرقابته ولرقابة هيئة الأسواق المالية وللمؤسسات وللإدارات وللهيئات التي يتعامل معها وفقاً للقوانين التي ترقى عملياته.
 - ٢- شهادات الاعتماد للمصارف وللمؤسسات الخاضعة لرقابته ولرقابة هيئة الأسواق المالية، بصفتها مقدم خدمات مصادقة للتوقيعات الإلكترونية لزبائنهم.
- يضع مصرف لبنان المعايير والقواعد التقنية للإجراءات المنصوص عنها في هذه المادة.

ZOOM ON CDD AND EKYC

When is CDD Required - FATF

R10

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.



Business Relation

Face to Face
& remote
onboarding



Occasional Transaction

Wire Transfers
(domestic and
International)
10,000 EU/USD
Check cash in
Deposit , bill
payment
+15,000 EU or
USD (R16)



Suspicion of
ML or FT

Patterns

R16



Frequency *2
years, 5 years)

New product,
frequency
regulatory
requirements, new
NRA

When is Authentication Required - FATF

CDD Requirements	Key Components of Digital ID
<p>Identification/Verification R.10</p> <p>Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.</p>	<p>Identity Proofing- Who are you? Obtain attributes (name, DoB, ID # etc.) and evidence for those attributes; validate and verify ID evidence and resolve it to a unique identity-proofed person.</p>
	<p>Binding- Issue credentials or authenticators linking the person in possession of the credentials to the on-boarded customer/account</p>
	<p>Authentication- Are you the identified person? Who you claim to be? This applies if the regulated entity is verifying customer's possession of a pre-existing customer credentials.</p>

Risk Based Approach - Level of CDD



Simplification – In **Lower Risk** situations: identification and verification is the bottom line; other CDD measures may be subject to simplification.

Exemption - Only in proven **Low Risk** situations, on a limited basis, for certain type of institutions and activities.

RBA to Customer Due Diligence

Simplified (Low Risk of AML/CFT) (Some countries dive this into tiers see Tiered SCDD)	Standard	Enhanced (Higher Risk of AML/CFT)
NRA conducted at country level but also take into consideration Global AML risks		
No doubt of suspicious activities	All Aspects of CDD are addressed when starting a business relation with the client	Sector, country or client included in the list of high risk.
Simplified requirements are balanced with mitigating measures (thresholds in amounts and usage)	Full suite of requirements but ceilings are higher on amounts and usage	More rigorous procedures por account opening. Constant monitoring Frequent reporting to authorities
Low risk scenarios (risk, probability, consequences) G2P	Medium risk scenarios (risk, probability, consequences) Domestic wire transfers	Higher risk scenarios (risk, probability, consequences) Cross-border payments
Example of relaxed requirements; Declaration of name and address or on beneficial ownership just declaring as acting on his/her behalf. Some data is verified other not..	Data declared by the client needs to be verified. Documents provided by the client need to be validated	Same as standard plus additional monitoring of the account is necessary, observing patterns etc and reporting to financial authorities

***Note-** When applying technology such as Digital ID some scenarios classified as high could be classified as lower risk or low. Also note that there are some situations completely excepted from CDD requirements from AML but may be not from fraud.

Criteria to classify the types of accounts/clients

Type of Risks

- Some examples- Corruption, fraud, forgery

Geographical

- List of countries with preferential tax regimes, drug transit, terror financing
- Countries with bank secrecy
- High volume of international remittances
- Free trade, ability to create complex legal entities easily
- Cash intensive economies
- Non-residents

Client

- Individual (PoConcern, resident, non-resident)
- Legal entities (trusts, limited companies, licensed vs registered)
- Gatekeepers (accountants, lawyers, trustees and notaries)
- Politically Exposed Persons (PePs)

Product (High Cash deposits- , Medium –POS withdrawals Low-payrol)

- Cross border transactions, cash,
- High speed movement of funds
- Easy to trace or not

Considerations for Country Implementation

SCENARIO	IDENTIFICATION/ VERIFICATION	AUTHENTICATION
G2P	Apply Tiered approach to SCDD (Proof of ID + Proof of address could be waived) Selfies and Videoconference + ID scan	MFA but maybe no need for biometrics if not available
Internet Banking	Alternative ways and information could be used if available Verification of information through third parties (e.g. telecommunication operators)	Biometrics alone MFA but selection of factors avoid contact
Occasional Transactions	Walk in or remittances (exemptions to verification based on thresholds)	No need for authentication
E-wallets	Delayed verification of ID Allow to collect purpose and nature	Biometrics through cell phone credentials

E-KYC Examples for Account Onboarding

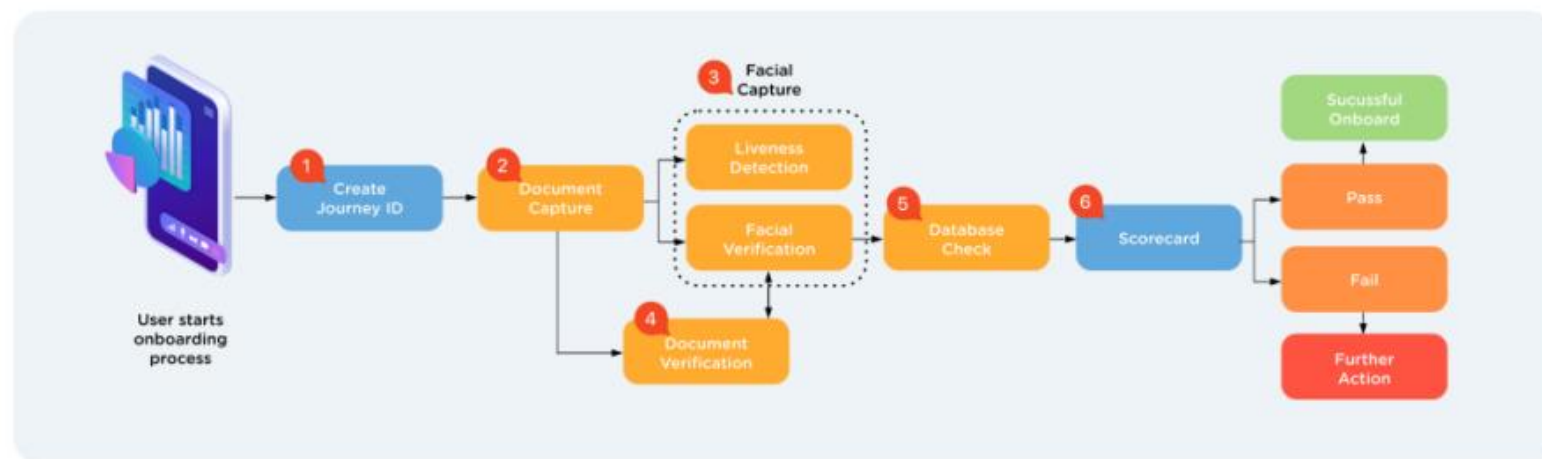
Biometrics (facial, fingerprint)

Document authentication

Liveliness detection

Digital Breadcrumbs

Trusted data sources



LOOKING AHEAD

WORKSHOP SERIES (TENTATIVE)

June

- Digital ID
- E-Signature



July

- E- Government
- Data Hosting/Cloud



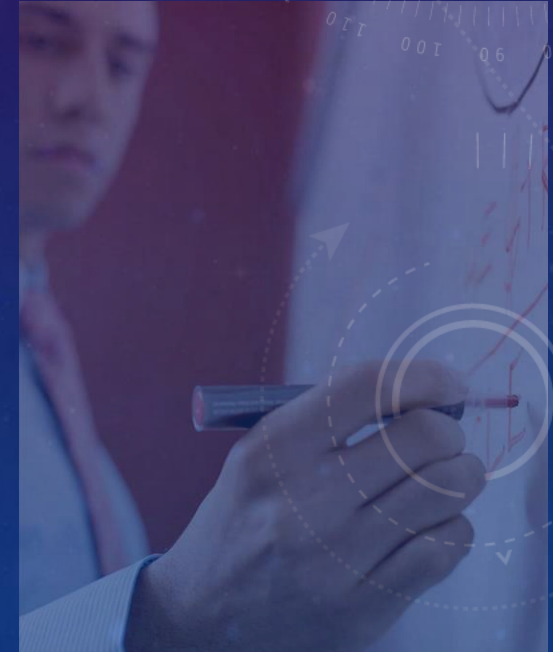
September

- Cybersecurity
- Service Digitalization



November

- Presentation of DTS Implementation Roadmap



Thank you

Lebanon Digital Transformation Strategy
2020 - 2030