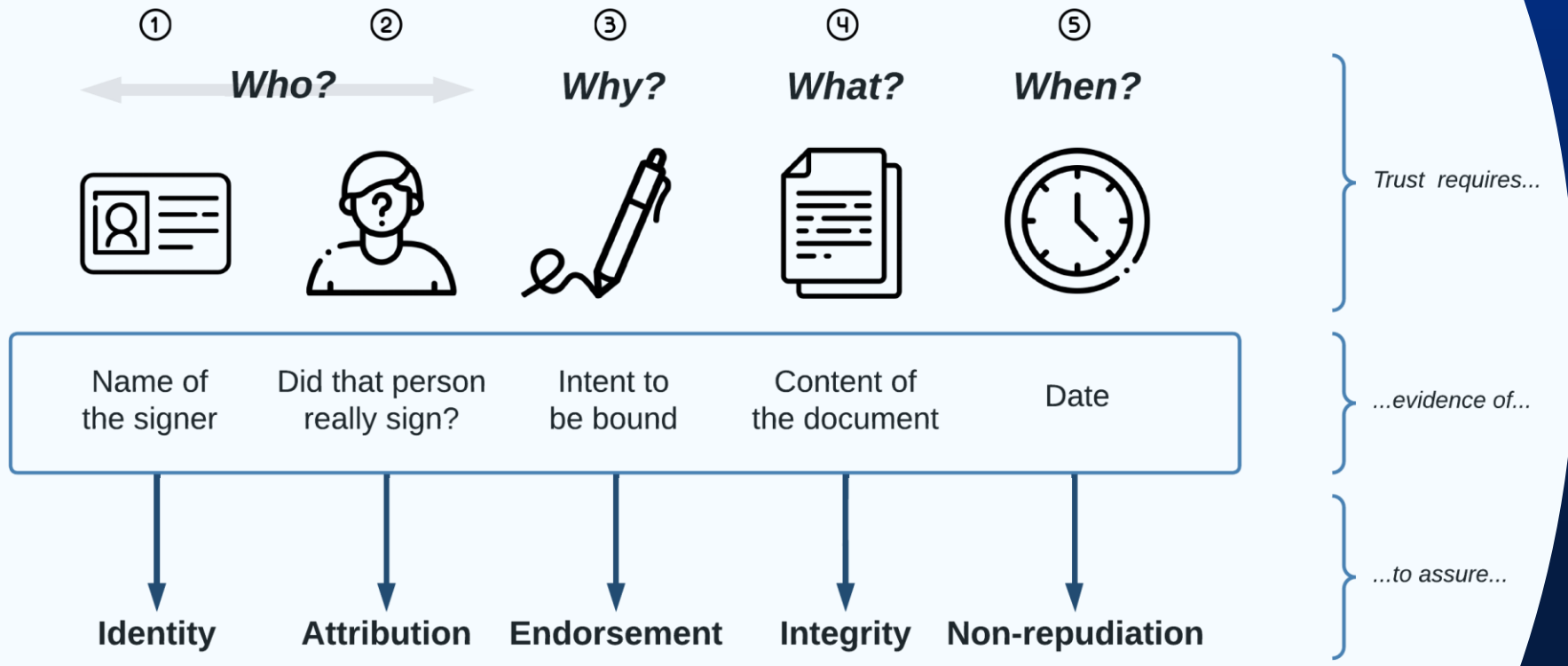
e-Signature
Deep Dive

Day 2 | 14:15 – 15:00

THE WORLD BANK

What is a signature anyway?

This functional view is equally valid for paper and electronic signatures.



What is an electronic signature?

Electronic Signature

"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."

(eIDAS Art. 3(10))

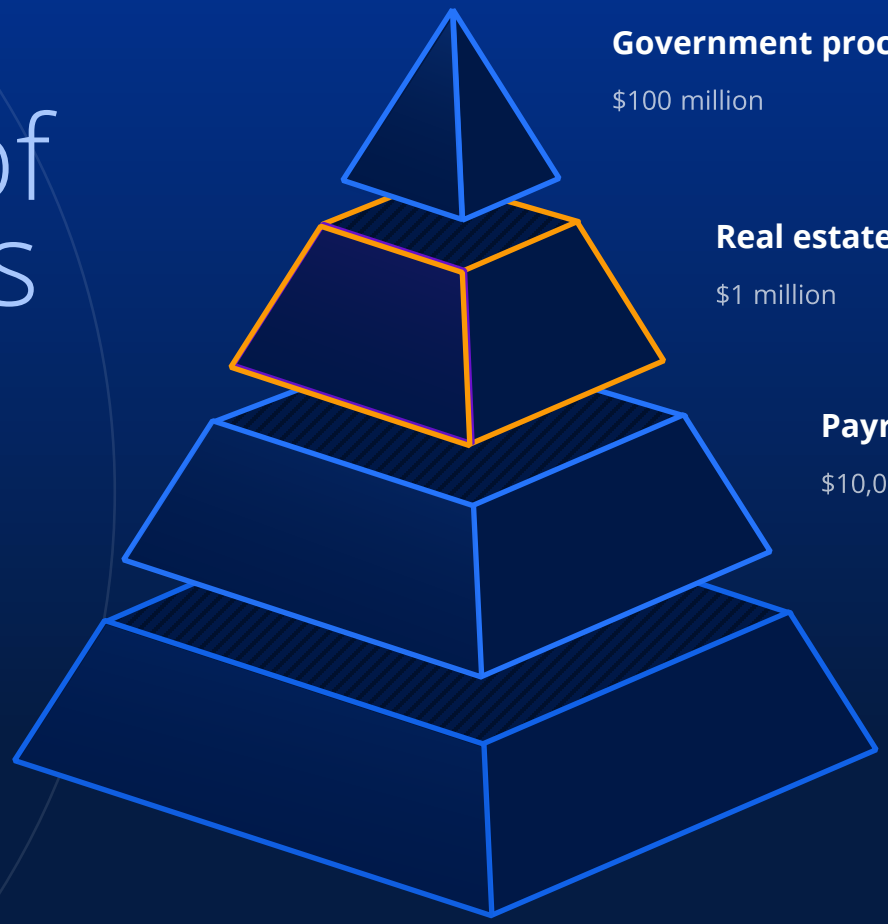
Digital Signature

"A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the public key to verify the data has not been altered since it was signed by the private key."

(NIST SP 800-63B)

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.



Government procurement

$100 million

Real estate

$1 million

Payroll

$10,000

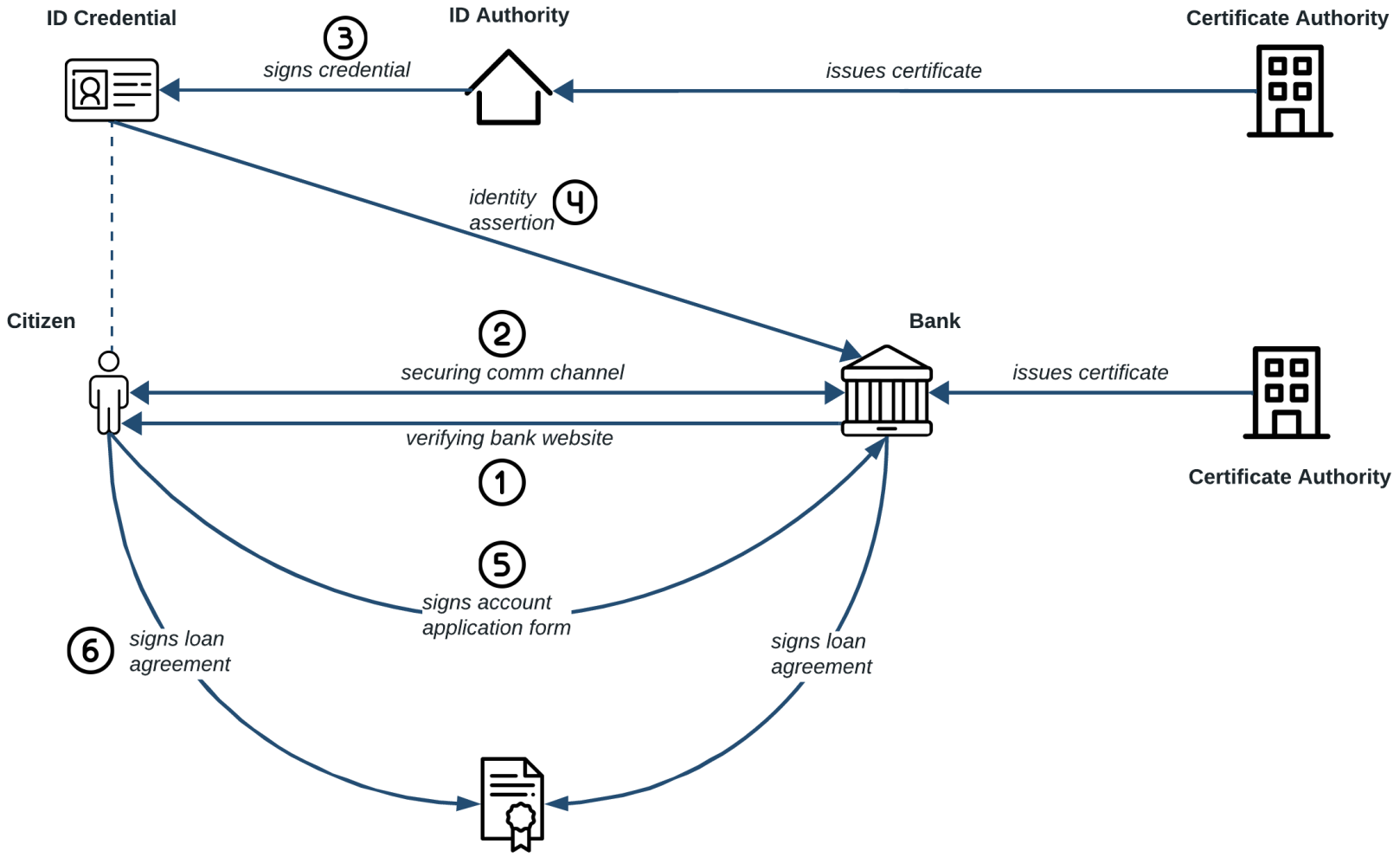
P2P payment

$10

Increasing transaction risk

Signatures are all around us

Sample use case:
Online loan application



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

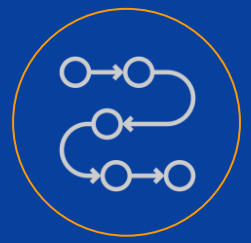
Technical measures to protect the integrity of the signed document

Trust framework

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

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

Levels of assurance in practice

The example of the European eIDAS regulation.

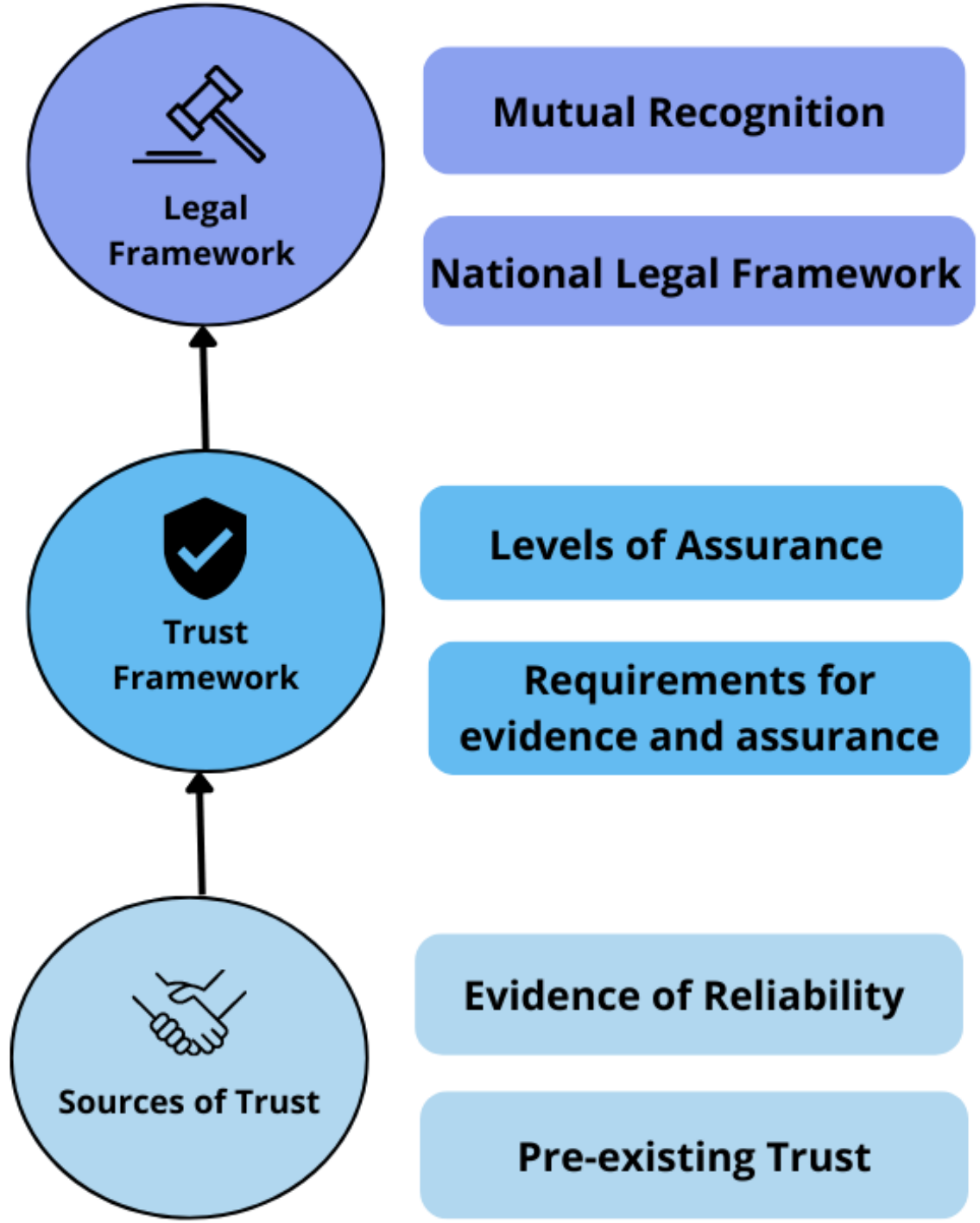
		Level of Assurance	
Requirement	Low	Medium	High
Signer identity	*none*	Signer can be identified	Signer can be identified
Data integrity	*none*	Modifications after signing detectable	Modifications after signing detectable
User onboarding	*none*	*none*	Identity verification done face to face
Technology	*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

Legal effect

- Enforceability
- Admissibility as evidence
- Presumption of validity

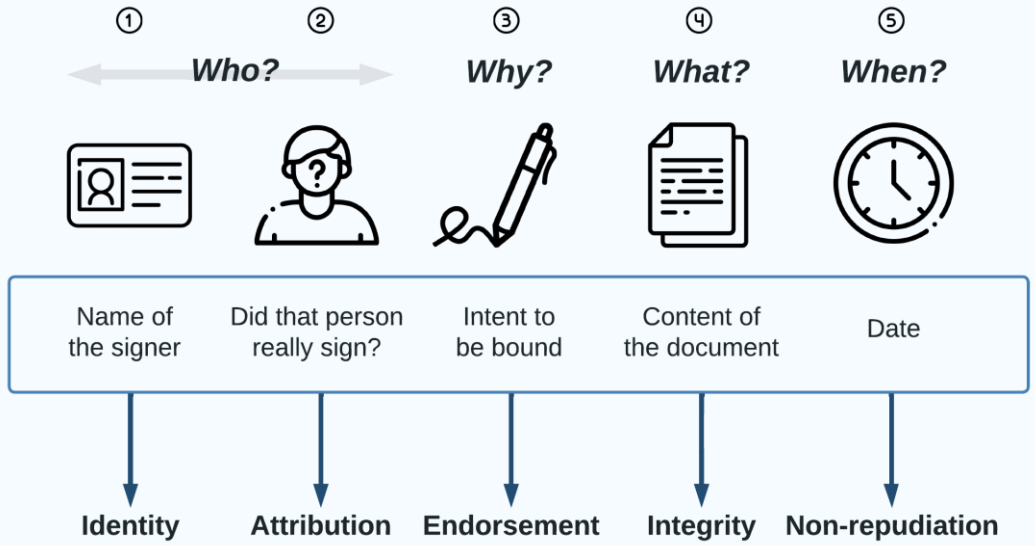
Mutual recognition

- Scaling trust across borders

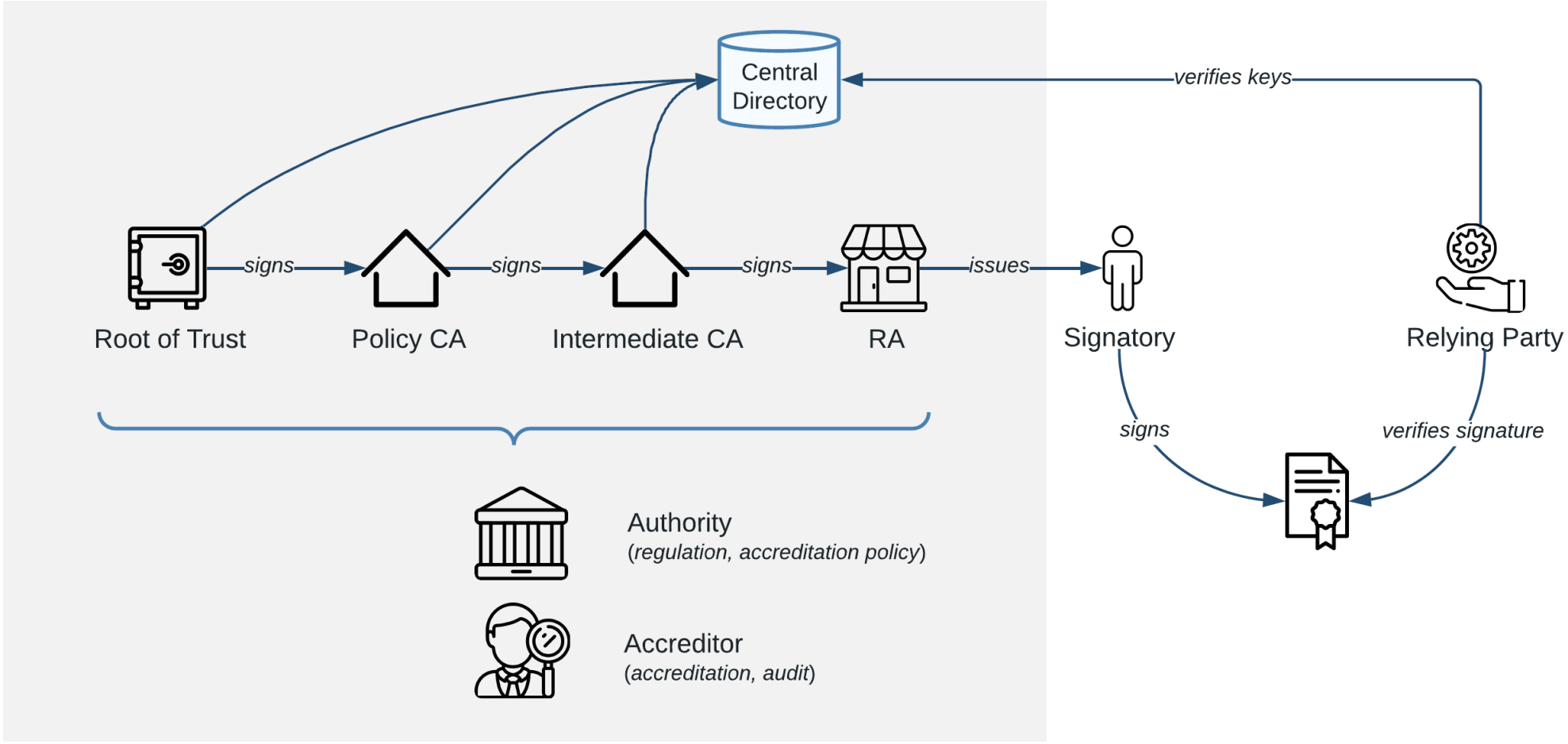

Legal Framework
Mutual Recognition
National Legal Framework
Trust Framework
Levels of Assurance
Requirements for evidence and assurance
Sources of Trust
Evidence of Reliability
Pre-existing Trust

The role of PKI

Functionality	Role PKI
Identity	*none*
Attribution	*none*
Endorsement	*none*
Integrity	**Hashing** ensures that the content of a document has not been modified after signing.
Nonrepudiation	Verifiable **timestamps** ensure that the signer cannot deny having previously signed a document.

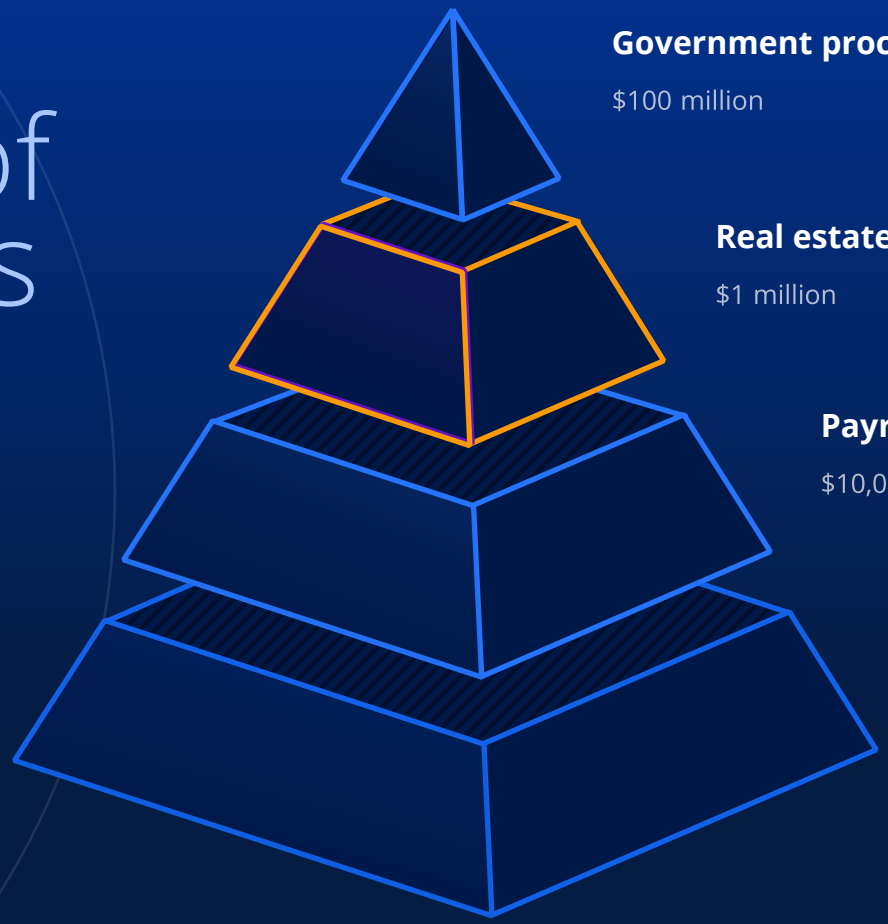


What is a PKI?


Central Directory
verifies keys
signs
signs
signs
issues
Root of Trust
Policy CA
Intermediate CA
RA
Signatory
Relying Party
signs
verifies signature
Authority
(regulation, accreditation policy)
Accreditor
(accreditation, audit)

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.



Government procurement

$100 million

Real estate

$1 million

Payroll

$10,000

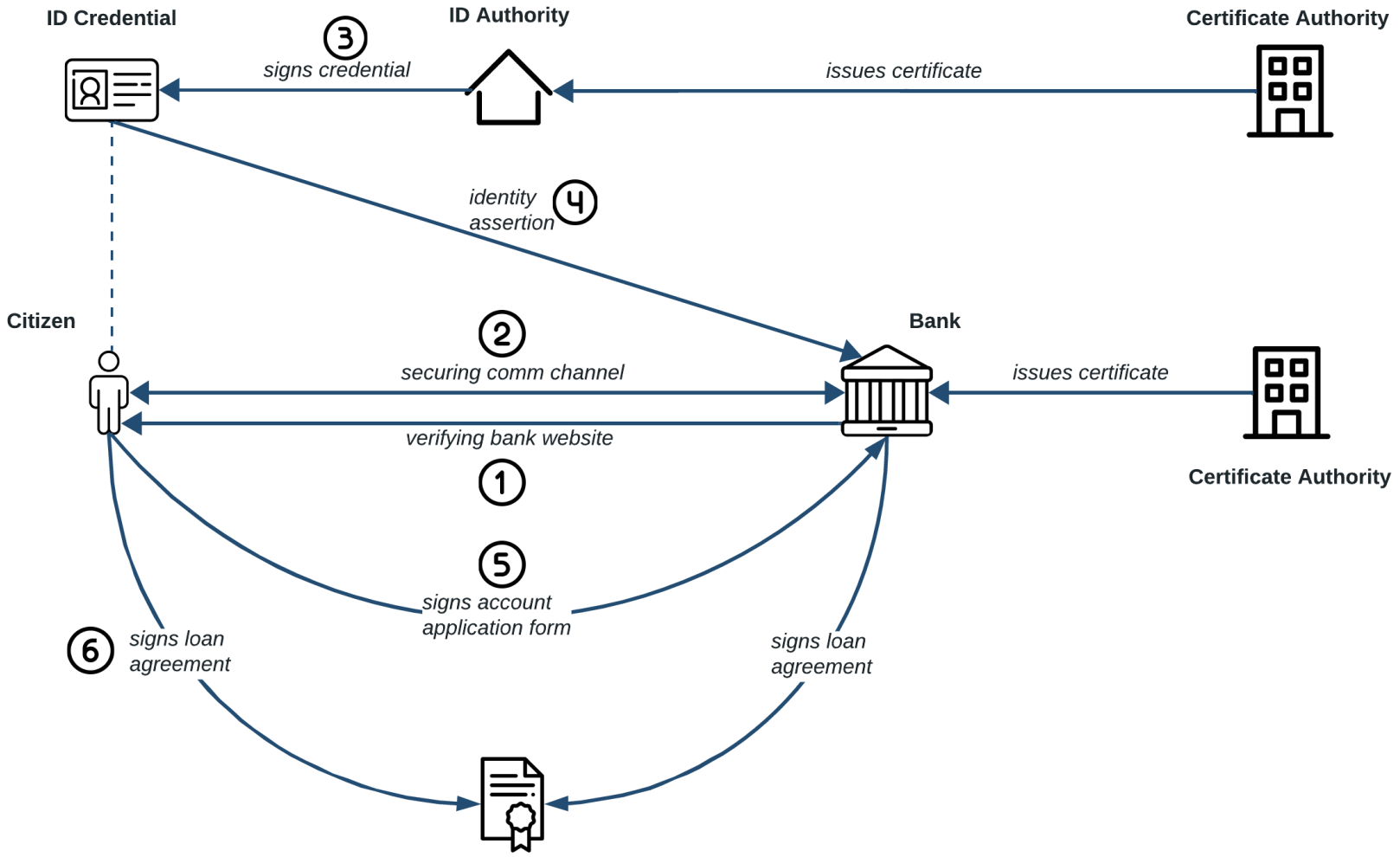
P2P payment

$10

Increasing transaction risk

Signatures are all around us

Sample use case:
Online loan application



Thank you.

Christopher Tullis
Program Officer, ID4D