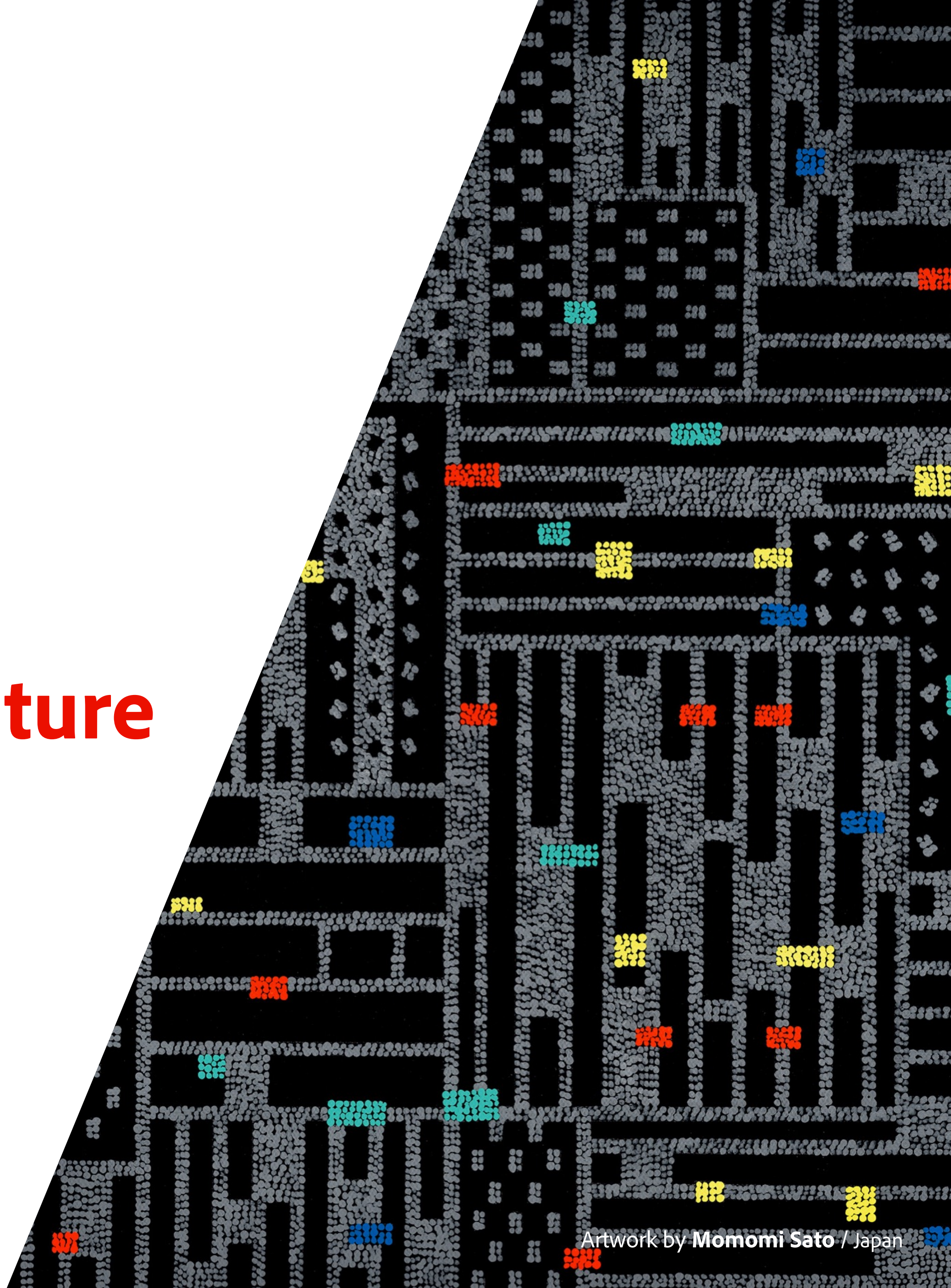
Enabling Global Trust: Digital Identity and Signatures for a Secure and Connected Future

Thailand PKI D-DAY

Bangkok, August 5, 2025

Adobe

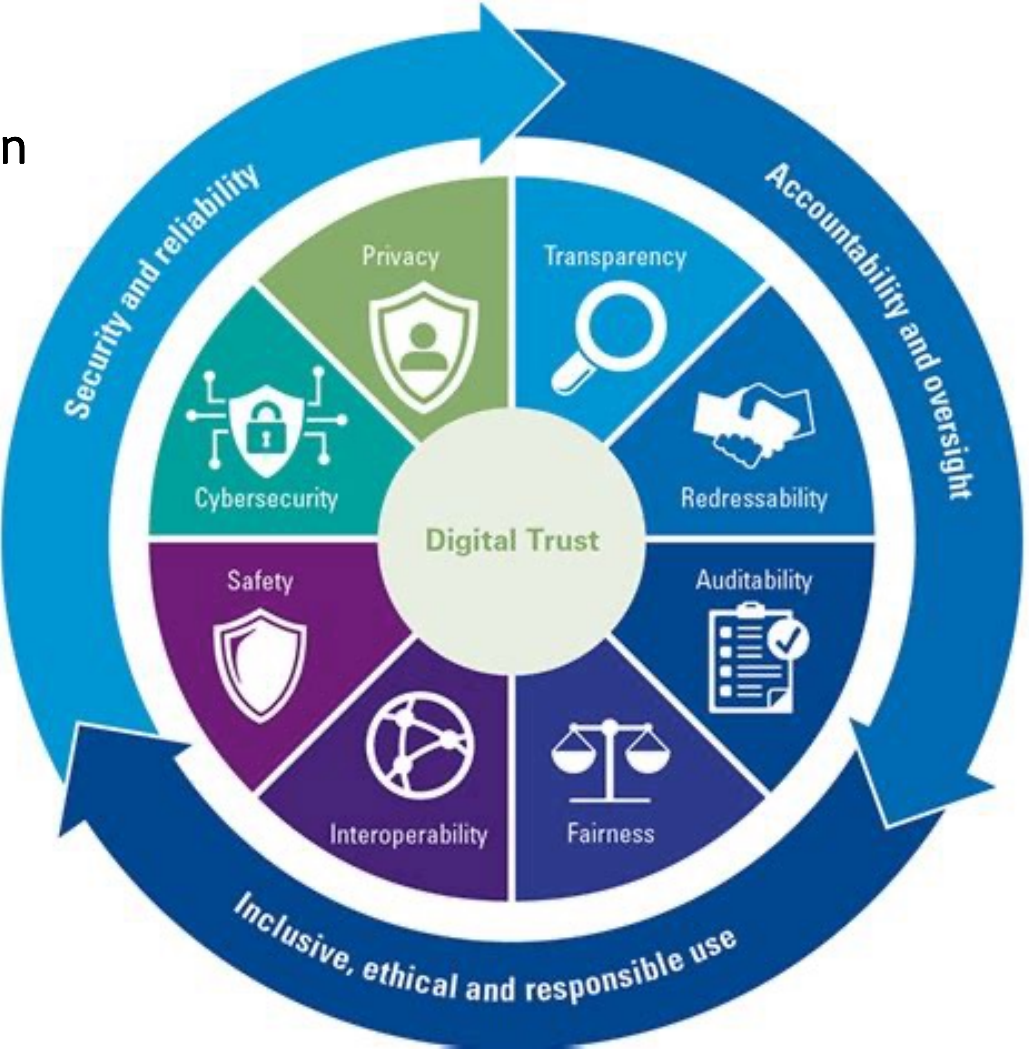
Andrea Valle | Principal Product Manager



Artwork by **Momomi Sato** / Japan

Trust as the Foundation of Digital Transformation

- Key Risks to Address:
  - **Legal Fragmentation - Risk of disparity in law interpretation**
    - Inconsistent application of digital trust frameworks across jurisdictions undermines mutual recognition and compliance.
  - **Technical Silos - Risk of lack of interoperability**
    - Proprietary implementations and fragmented standards hinder seamless integration across platforms and services.
  - **Unequal Access - Risk of digital divide**
    - Disparities in digital infrastructure and identity access create barriers for individuals and SMEs to participate in the digital economy.
  - **Pace of Change - Risk of slow adoption**
    - Lack of incentives, unclear ROI, and complexity in implementation delay adoption of trust-enabling technologies.



Why Trust matters the most in Electronic Signatures

Verification makes a Digital Signature Meaningful

➤ *A signature is only as strong as the confidence others have in it.*

- **Signature Generation is easy. Trustworthy Verification is hard!**
- You can generate a self-signed certificate in seconds…
- But unless the **recipient can verify** who signed the document, the signature has no legal or practical value.
- Building a system that others **trust to verify** that signature requires:
  - Rigorous identity proofing
  - Secure key management
  - Certificate status validation (e.g., OCSP, CRL)
  - Transparent audit and compliance.

The Role of Sources of Trust

➤ ***Without trusted infrastructure, digital signatures are just worthless blobs of data.***

- Signature Verification depends on the **Source of Trust**
  - Trusted Certificate Authorities (CA)
  - Trusted Identity Providers (IDP)
  - Authentic Sources
- These entities vouch for the signer's identity and ensure that credentials are issued, used, and disposed properly.

Legal Recognition relies on Trust Frameworks

➤ ***Interoperability and cross-border recognition are only possible when trust is standardized and auditable.***

- eIDAS in Europe, NIST in the US, and similar regulations worldwide define trusted lists and accreditation requirements.
- Only signatures issued under these **recognized trust frameworks** carry legal weight across jurisdictions.

Only User Confidence can Drive Adoption

➤ ***Lack of trust leads to fallbacks like printing, scanning, or even rejecting signed documents.***

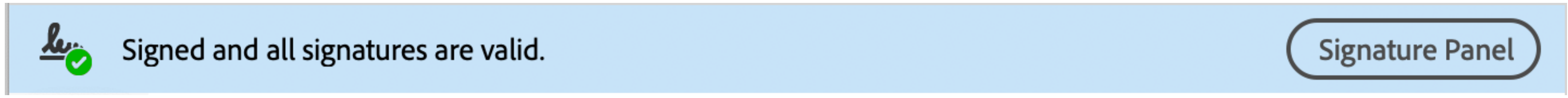
- Visual feedback and User Experience are critical success factors
- End users, businesses, and governments are more likely to adopt electronic signatures when they can **trust the outcome**:
  - Knowing who signed
  - Knowing that the signature is valid
  - Knowing that the document hasn't been altered.

The AATL Program

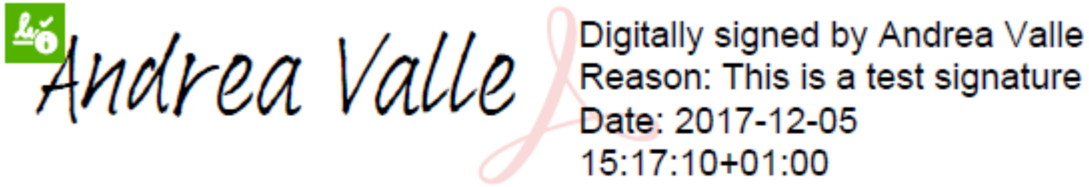
Why Digital Signature Trust is an Adobe's problem to solve

- PDF is the most widely used format for digitally signing documents.
- Estimated volume of 10+ Billion PDF digitally signed every year.
- ~1 Billion of Adobe Acrobat and Reader installed.
- 800+ Million digital signature verifications per month.
- Adobe is compelled to solve the **signature assurance** problem
  - Provide a source of trust that is natively available in the Adobe PDF viewing applications.
  - Policy management and legal assurance to provide the legitimacy and reliability of the source of trust.
  - The Electronic Signature industry has built on top of the "green check" validation in Acrobat desktop.

Characteristics and benefits of native PDF digital signatures


Signed and all signatures are valid.

- Native Visual Trust and Identity Assurance
  - Is this signature valid?
  - Has the document been tampered?
  - Can I trust the signatory?



Digitally signed by Andrea Valle
Reason: This is a test signature
Date: 2017-12-05
15:17:10+01:00

- Based on PKI industry standards
- Aligned with Regulatory Compliance requirements
- Engaging User Experience

High assurance + Standards + Reliable Source of Trust

=

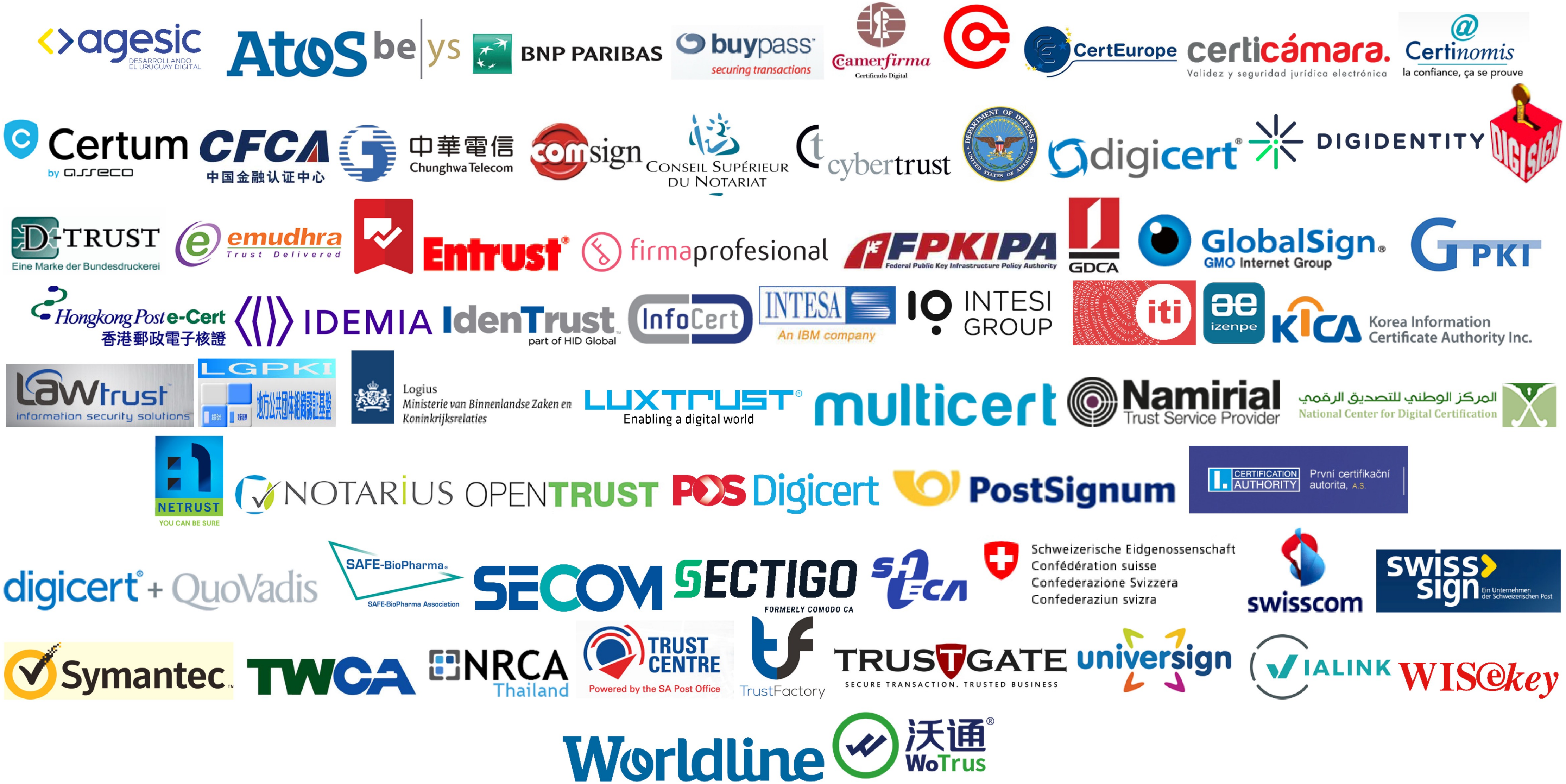
High value, trustworthy digital signatures

The AATL program

Adobe Approved
Trust List Member

- Adobe Approved Trust List
  - A Global Trust Program for Certification Authorities, established in 2008.
  - Covers digital certificates for signatures, seals and time-stamping services.
  - 90 active members, covering about 170 Trust Service Providers around the world.
  - Several Government Root CA included (US, EU, India, Brazil, Thailand, Uruguay…)
  - Annual membership fee for Commercial members.
  - Free membership for non-commercial Government members.
- https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html

The AATL Members


agesic DESARROLLANDO EL URUGUAY DIGITAL
Atos
be|ys
BNP PARIBAS
buypass securing transactions
Camerfirma Certificado Digital
CertEurope
certicámara. Validez y seguridad jurídica electrónica
Certinomis la confiance, ça se prouve
Certum by asseco
CFCA 中国金融认证中心
中華電信 Chunghwa Telecom
comsign
Conseil Supérieur du Notariat
cybertrust
Department of Defense United States of America
digicert
DIGIDENTITY
DIGISIGN
D-TRUST Eine Marke der Bundesdruckerei
emudhra Trust Delivered
Entrust
firmaprofesional
FPKIPA Federal Public Key Infrastructure Policy Authority
GDCA
GlobalSign. GMO Internet Group
GPKI
Hongkong Post e-Cert 香港郵政電子核證
IDEMIA
IdenTrust part of HID Global
InfoCert
INTESA An IBM company
INTESI GROUP
iti
izenpe
KICA Korea Information Certificate Authority Inc.
LawTrust information security solutions
LGPKI
Logius Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
LUXTRUST Enabling a digital world
multicert
Namirial Trust Service Provider
المركز الوطني للتصديق الرقمي National Center for Digital Certification
NETRUST YOU CAN BE SURE
NOTARIUS
OPENTRUST
POS Digicert
PostSignum
I.CA CERTIFICATION AUTHORITY První certifikační autorita, a.s.
digicert + QuoVadis
SAFE-BioPharma SAFE-BioPharma Association
SECOM
SECTIGO FORMERLY COMODO CA
SI-CA
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
swisscom
swiss sign Ein Unternehmen der Schweizerischen Post
Symantec.
TWCA
NRCA Thailand
TRUST CENTRE Powered by the SA Post Office
TrustFactory
TRUSTGATE SECURE TRANSACTION. TRUSTED BUSINESS
universign
VIALINK
WISeKey
Worldline
沃通 WoTrus

Key AATL Policy Requirements

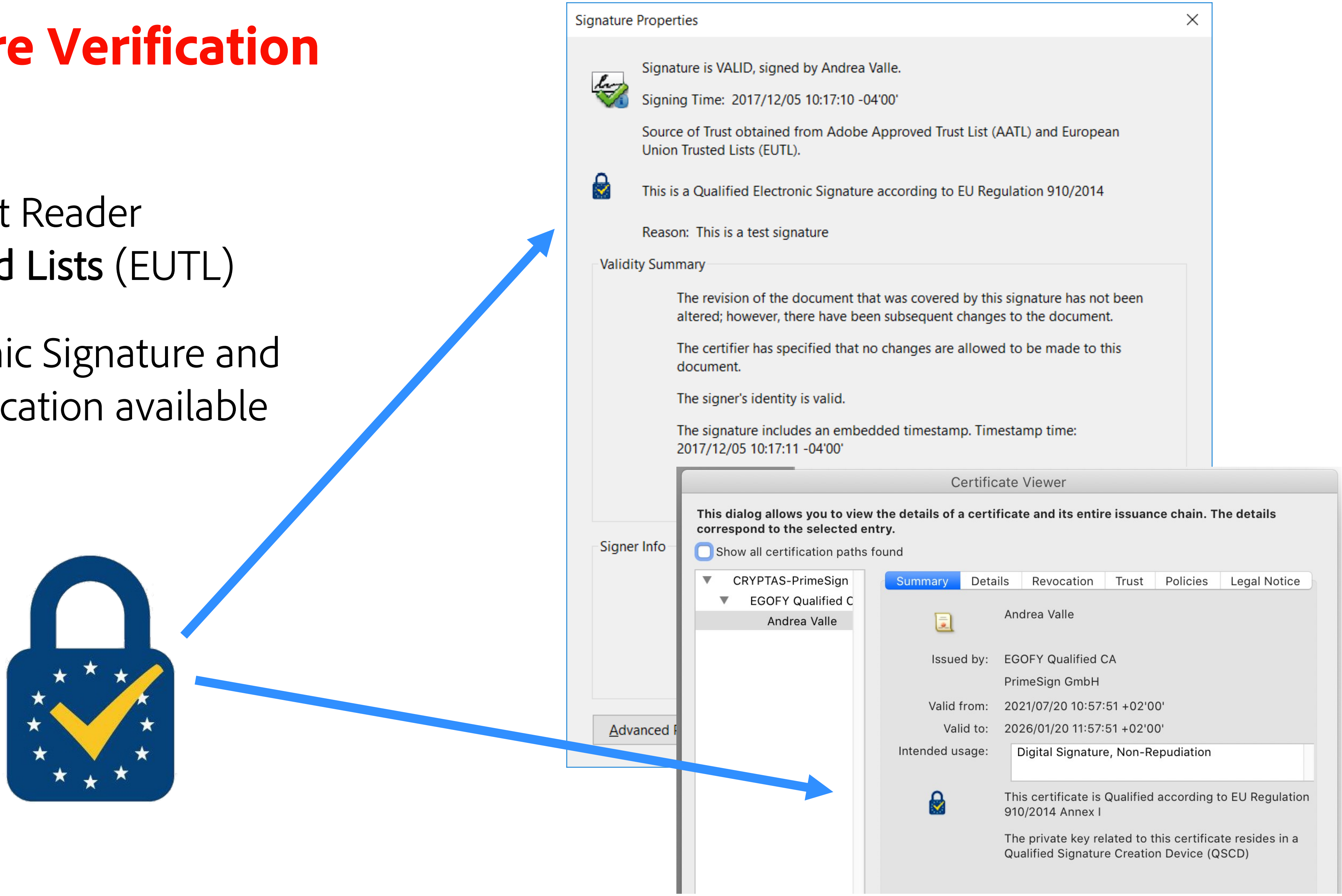
- Responsibility and Liability of the Certification Authority
- Hardware support for the Private Key (FIPS 140-2 Level 2 or superior)
- Strong Identity Verification (Face to face or equivalent)
- Pass a recognized Audit at least every 2 years (ETSI, WebTrust)
- End Entity Key size (RSA: 2048+ bit / ECDSA: 256+ bit)
- Two-factor authentication of key activation
- Revocation mechanisms
- Incident reporting

New trends demanding AATL Policy update

- The AATL program builds on its stability, consistent policy, and Adobe's reliability as trusted Vendor.
- … but the AATL has not been updated over the last 8 years…
- Technical, Market and Regulatory factors driving the need for an AATL Policy update
  - Identity verification has improved, but it's at risks of AI-based threats
  - New Electronic Identity Wallet frameworks
  - Cloud Signing is the de-facto approach for electronic signatures
  - Signing and hashing algorithm robustness, including Quantum-safe algorithms
  - Prevent.
- A major policy update is in the works.

EU Qualified Signature Verification

- Adobe Acrobat and Acrobat Reader natively support **EU Trusted Lists** (EUTL)
- Make EU Qualified Electronic Signature and Qualified Time Stamp verification available to anyone and for free



Signature Properties

Signature is VALID, signed by Andrea Valle.

Signing Time: 2017/12/05 10:17:10 -04'00'

Source of Trust obtained from Adobe Approved Trust List (AATL) and European Union Trusted Lists (EUTL).

This is a Qualified Electronic Signature according to EU Regulation 910/2014

Reason: This is a test signature

Validity Summary

The revision of the document that was covered by this signature has not been altered; however, there have been subsequent changes to the document.

The certifier has specified that no changes are allowed to be made to this document.

The signer's identity is valid.

The signature includes an embedded timestamp. Timestamp time: 2017/12/05 10:17:11 -04'00'

Signer Info

Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

- CRYPTAS-PrimeSign
  - EGOFY Qualified C
    - Andrea Valle

Andrea Valle

Issued by: EGOFY Qualified CA
PrimeSign GmbH

Valid from: 2021/07/20 10:57:51 +02'00'

Valid to: 2026/01/20 11:57:51 +02'00'

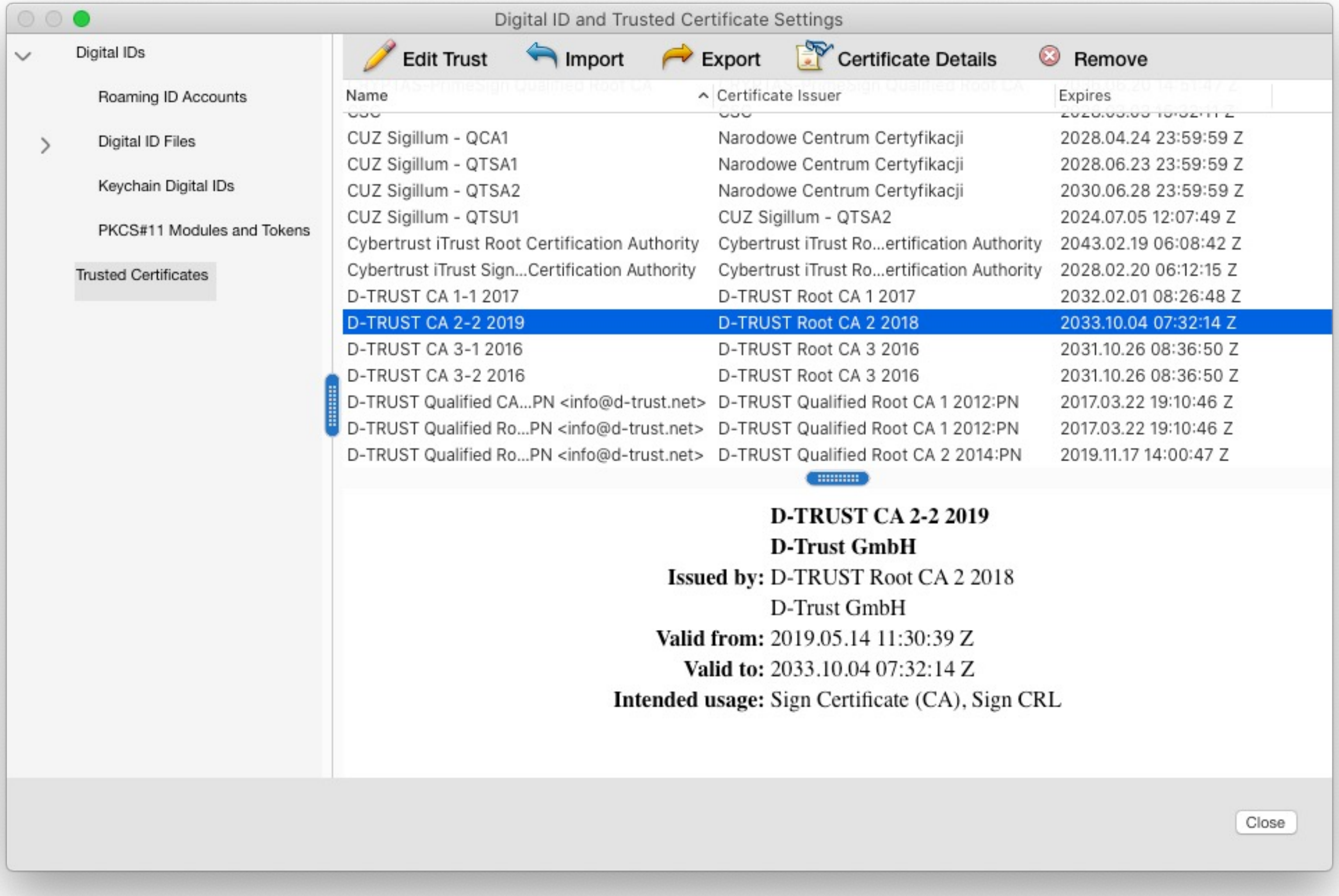
Intended usage: Digital Signature, Non-Repudiation

This certificate is Qualified according to EU Regulation 910/2014 Annex I

The private key related to this certificate resides in a Qualified Signature Creation Device (QSCD)

EUTL: Digital Trust for Europe

- Adobe Acrobat natively validates EU Qualified Certificates
- The EUTL contains ~1700 QTSP Trust Anchors
- Sourced from 300+ QTSP services:
  - Qualified Signatures
  - Qualified Seals
  - Qualified Time Stamps
- Downloaded globally from Adobe Acrobat desktop software 800+ million times every month

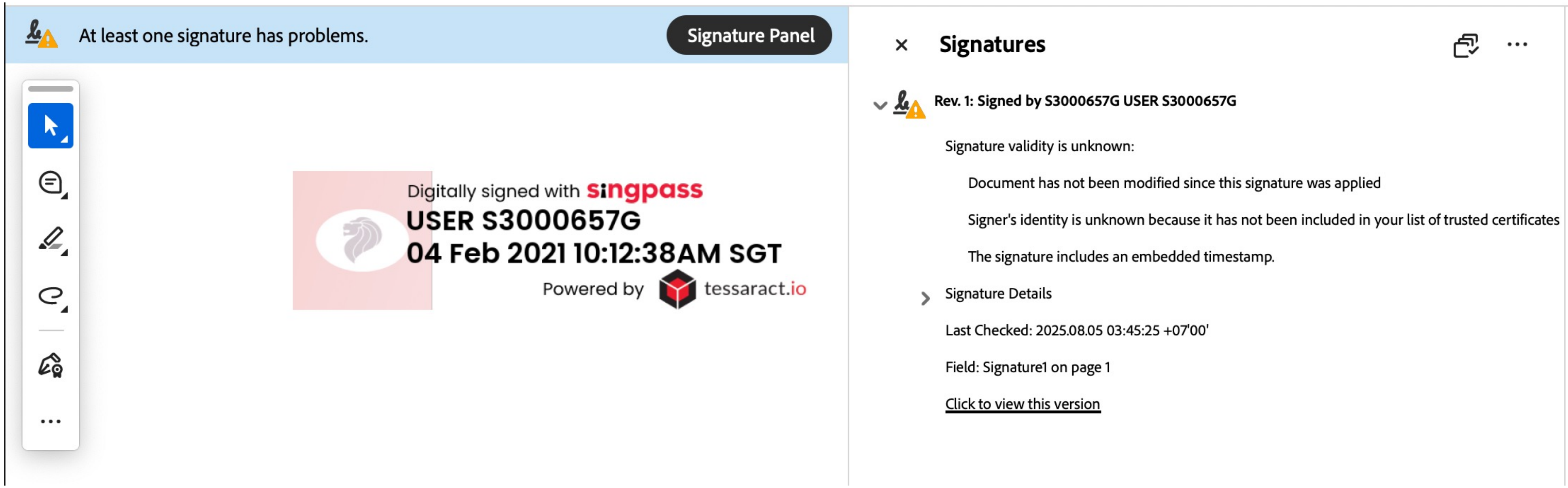


Name	Certificate Issuer	Expires
CUZ Sigillum - QCA1	Narodowe Centrum Certyfikacji	2028.04.24 23:59:59 Z
CUZ Sigillum - QTSA1	Narodowe Centrum Certyfikacji	2028.06.23 23:59:59 Z
CUZ Sigillum - QTSA2	Narodowe Centrum Certyfikacji	2030.06.28 23:59:59 Z
CUZ Sigillum - QTSU1	CUZ Sigillum - QTSA2	2024.07.05 12:07:49 Z
Cybertrust iTrust Root Certification Authority	Cybertrust iTrust Ro...ertification Authority	2043.02.19 06:08:42 Z
Cybertrust iTrust Sign...Certification Authority	Cybertrust iTrust Ro...ertification Authority	2028.02.20 06:12:15 Z
D-TRUST CA 1-1 2017	D-TRUST Root CA 1 2017	2032.02.01 08:26:48 Z
D-TRUST CA 2-2 2019	D-TRUST Root CA 2 2018	2033.10.04 07:32:14 Z
D-TRUST CA 3-1 2016	D-TRUST Root CA 3 2016	2031.10.26 08:36:50 Z
D-TRUST CA 3-2 2016	D-TRUST Root CA 3 2016	2031.10.26 08:36:50 Z
D-TRUST Qualified CA...PN <info@d-trust.net>	D-TRUST Qualified Root CA 1 2012:PN	2017.03.22 19:10:46 Z
D-TRUST Qualified Ro...PN <info@d-trust.net>	D-TRUST Qualified Root CA 1 2012:PN	2017.03.22 19:10:46 Z
D-TRUST Qualified Ro...PN <info@d-trust.net>	D-TRUST Qualified Root CA 2 2014:PN	2019.11.17 14:00:47 Z

D-TRUST CA 2-2 2019
D-Trust GmbH
Issued by: D-TRUST Root CA 2 2018
D-Trust GmbH
Valid from: 2019.05.14 11:30:39 Z
Valid to: 2033.10.04 07:32:14 Z
Intended usage: Sign Certificate (CA), Sign CRL

Adobe

Does your electronic signature look good?



Digitally signed with singpass
USER S3000657G
04 Feb 2021 10:12:38AM SGT
Powered by tessaract.io

Rev. 1: Signed by S3000657G USER S3000657G

Signature validity is unknown:

Document has not been modified since this signature was applied

Signer's identity is unknown because it has not been included in your list of trusted certificates

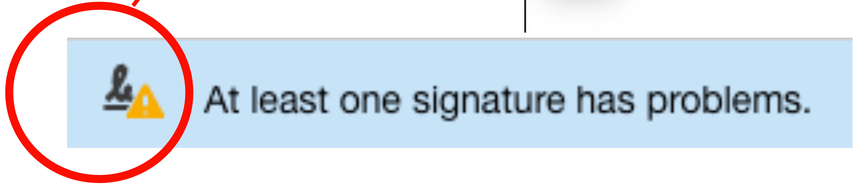
The signature includes an embedded timestamp.

Signature Details

Last Checked: 2025.08.05 03:45:25 +07'00'

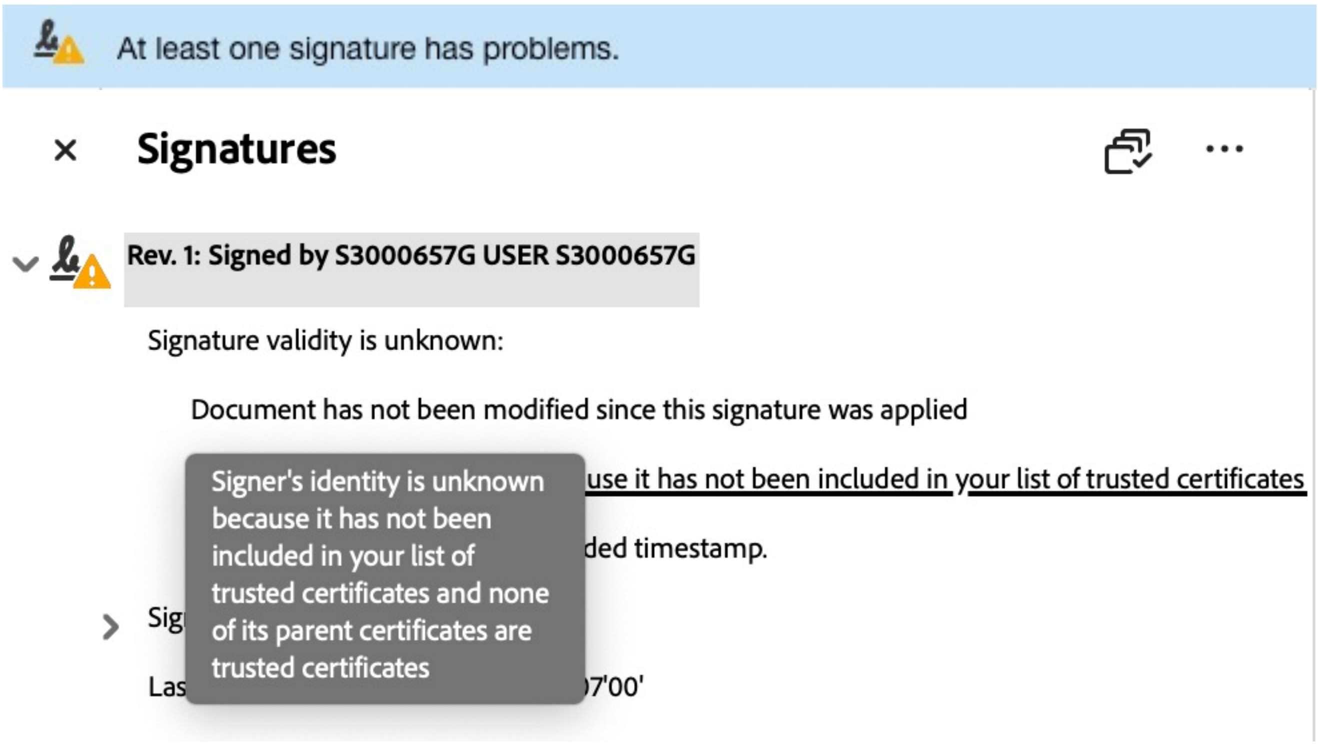
Field: Signature1 on page 1

Click to view this version



At least one signature has problems.

It’s about Digital Trust!



At least one signature has problems.

Signatures

Rev. 1: Signed by S3000657G USER S3000657G

Signature validity is unknown:

Document has not been modified since this signature was applied

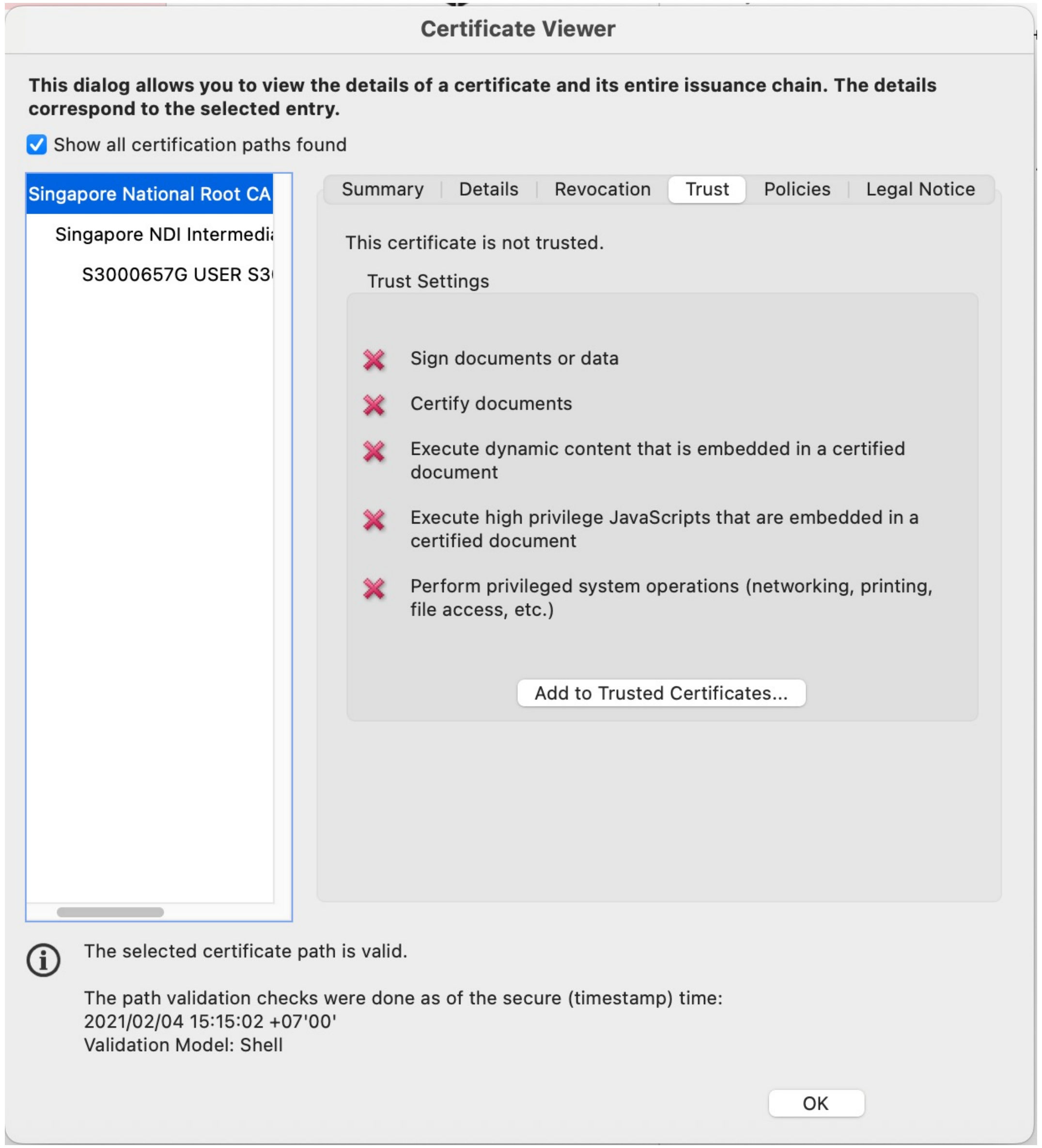
use it has not been included in your list of trusted certificates

ded timestamp.

Sig

Las 07'00'

Signer's identity is unknown because it has not been included in your list of trusted certificates and none of its parent certificates are trusted certificates



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

☑ Show all certification paths found

Singapore National Root CA
Singapore NDI Intermedi
S3000657G USER S3

This certificate is not trusted.

Trust Settings

- ☒ Sign documents or data
- ☒ Certify documents
- ☒ Execute dynamic content that is embedded in a certified document
- ☒ Execute high privilege JavaScripts that are embedded in a certified document
- ☒ Perform privileged system operations (networking, printing, file access, etc.)

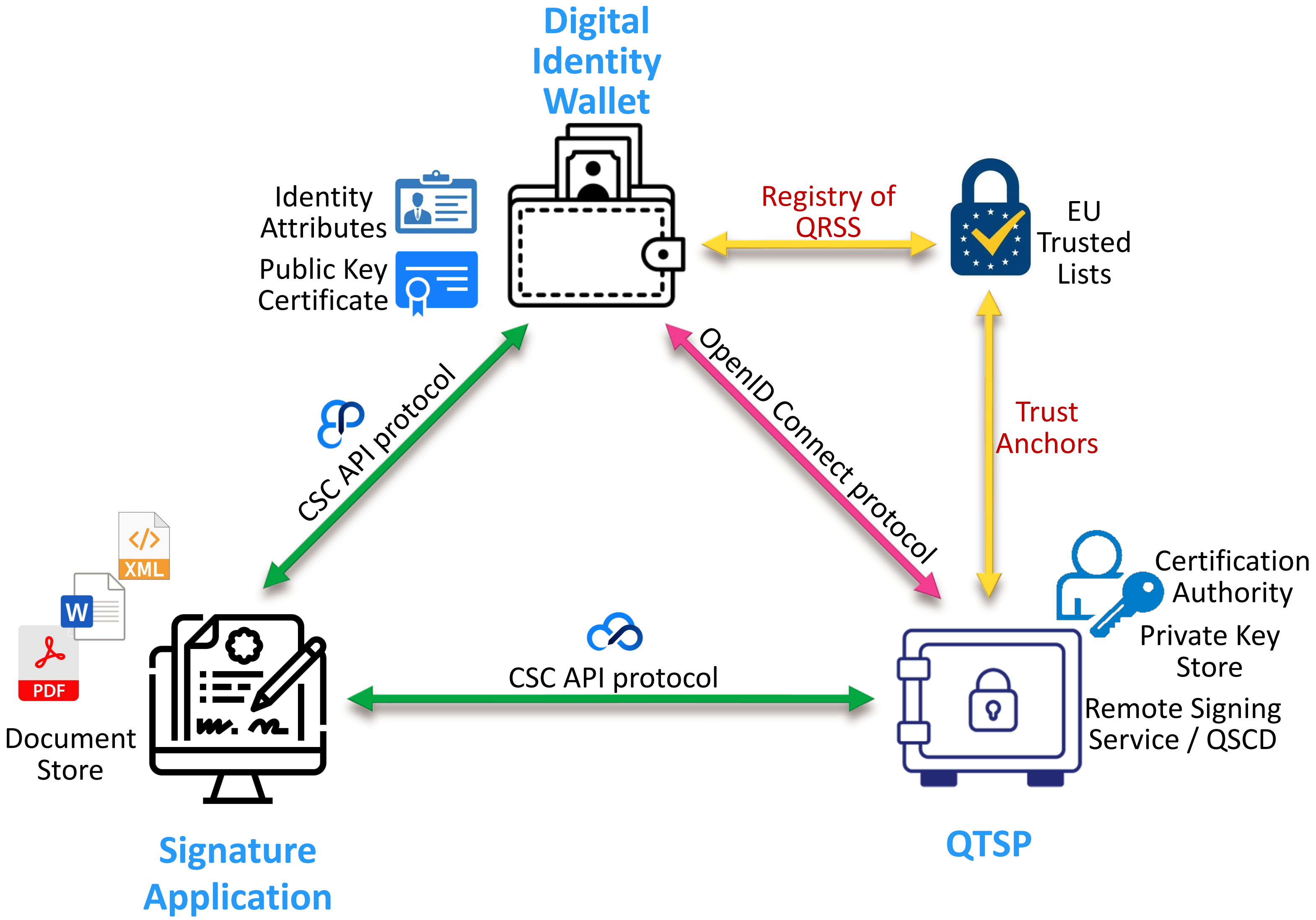
The selected certificate path is valid.

The path validation checks were done as of the secure (timestamp) time:
2021/02/04 15:15:02 +07'00'
Validation Model: Shell

New trends for Digital Signatures

DIGITAL IDENTITY
AUTHENTICATION
CYBERSPACE
DATA
INFORMATION
PRIVACY
INDIVIDUAL
PERSONALIZATION
USERNAME
UNIQUE
STORAGE
SYSTEM
SECURITY
IDENTIFIER
NETWORK
AUTHENTICATION
PERSONALIZATION
SYSTEM
PRIVACY
DATA

The Digital Identity Wallet Revolution



Identity Validation in the AI era

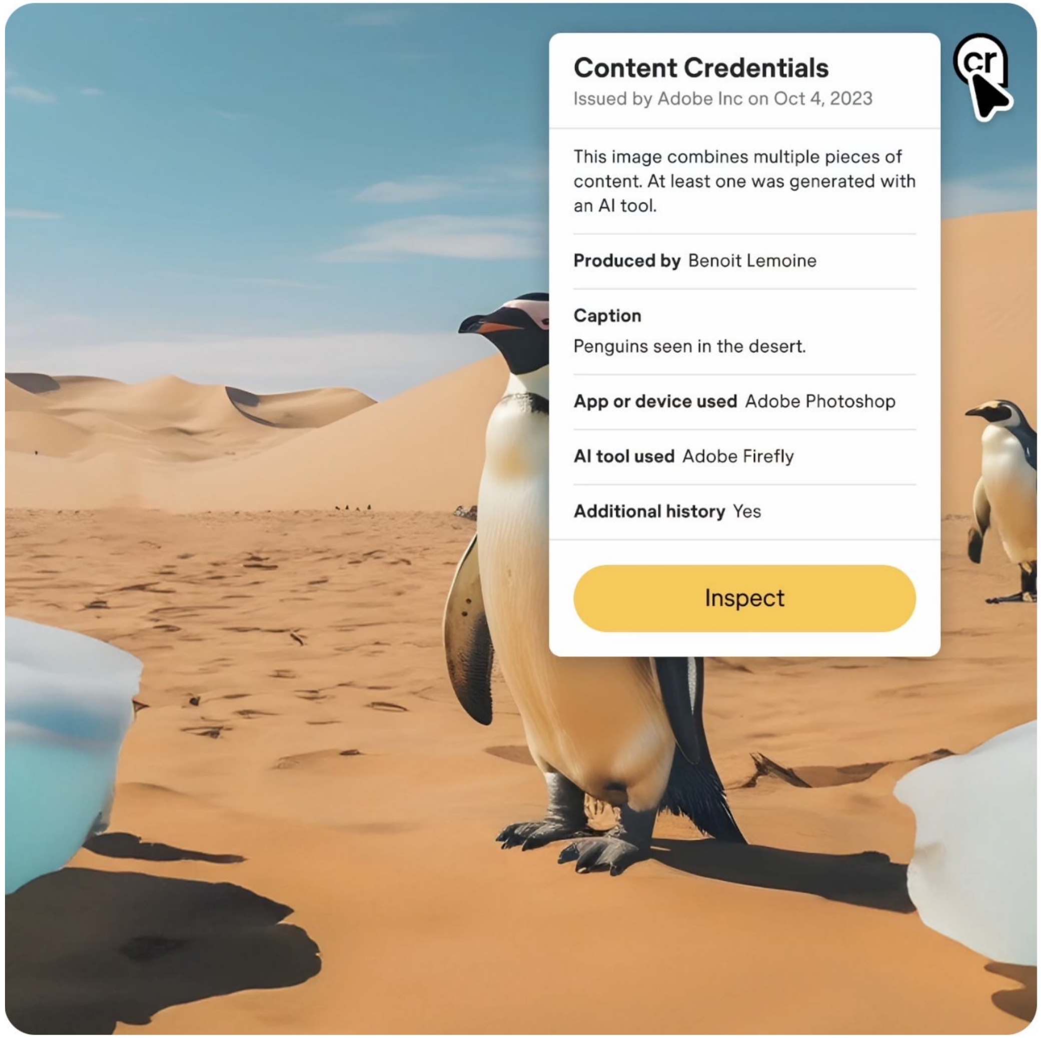
- Proof of Identity: Prove you are who you say you are.
  Proof of Humanity: Prove you are a human.
  Proof of Authenticity: Prove you originated the content.
- AI is a game-changer for Digital Identity.
- Maximize the opportunity…
  - Self-paced Identity Verification
  - Behavioral Analysis
  - Fraud Detection and Mitigation
- Minimize the risk…
  - Identity forgery and theft

Content Authenticity & Provenance

- Deepfakes. Voice cloning. Synthetic media…
  It's hard to tell if media are True and Authentic these days.
- We need a way for software, devices, and generative AI models to show the provenance of media.

cr content credentials

- A new opportunity for Certification Authorities!
- https://contentcredentials.org



Content Credentials
Issued by Adobe Inc on Oct 4, 2023

This image combines multiple pieces of content. At least one was generated with an AI tool.

Produced by Benoit Lemoine

Caption
Penguins seen in the desert.

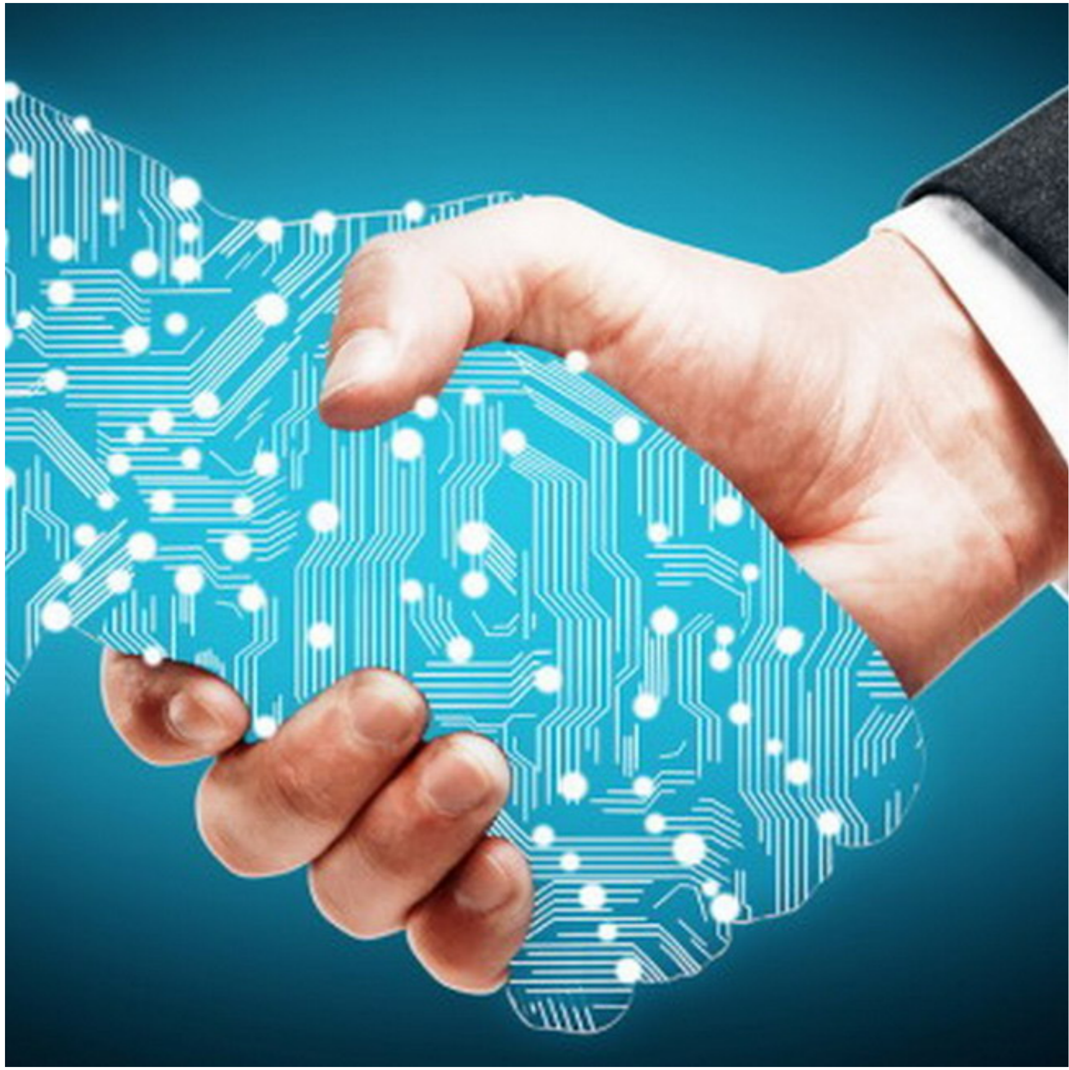
App or device used Adobe Photoshop

AI tool used Adobe Firefly

Additional history Yes

Are You Ready?

- Key Success Factors for a Global adoption of Digital Signatures:
  - Regulatory Frameworks
  - Cloud-based Certificates (Remote Signatures)
  - Global Trust recognition
  - Standardization and Interoperability
  - Great User Experience for Users



Adobe