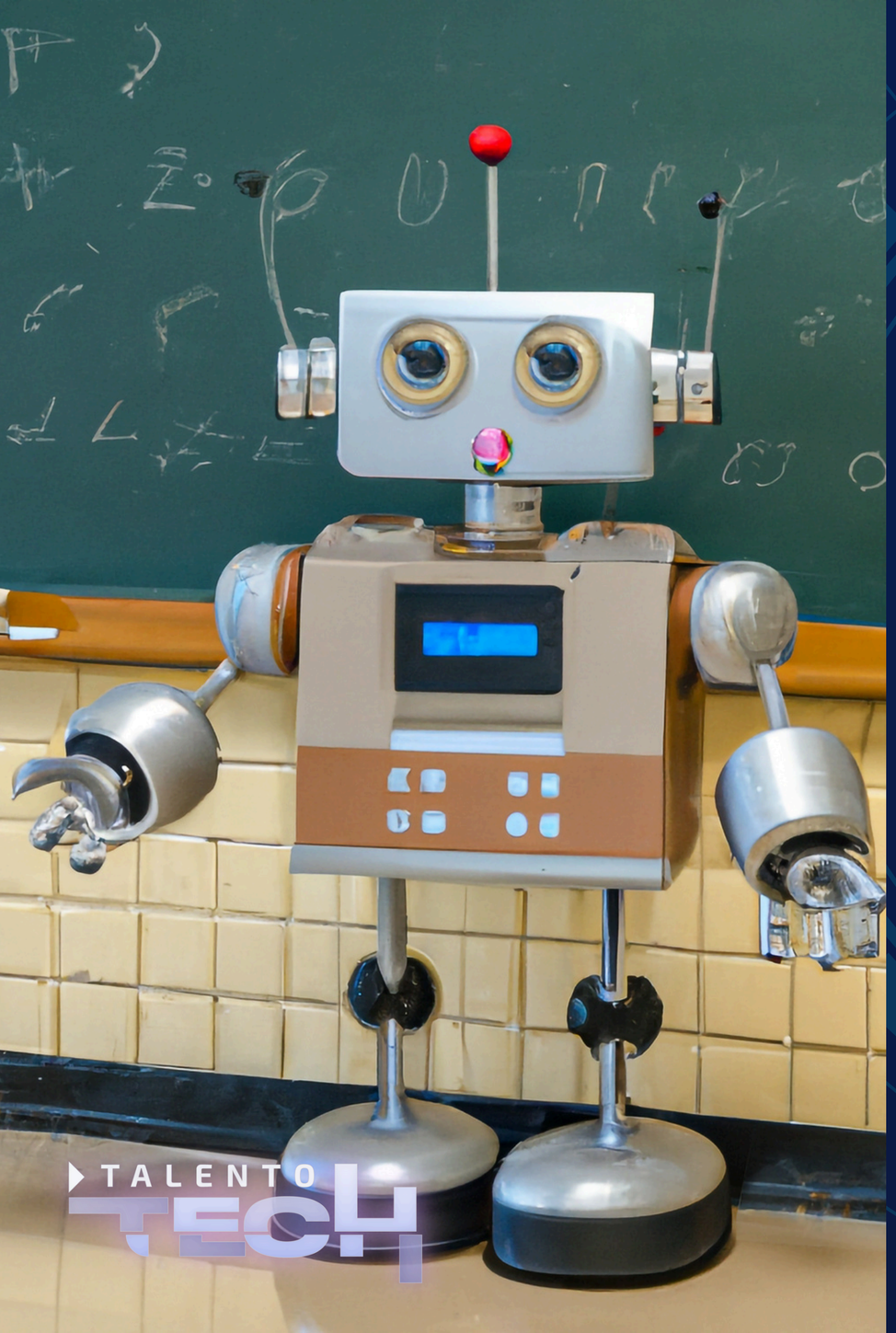
TALENTO TECH

REGIÓN 3
CAUCA – NARIÑO
LESSON 1- UNIT 2

TIC

Universidad Tecnológica de Pereira

faceIT



TIC

LESSON 1: READING

Digital signatures: What they are & why they matter

What is a digital signature?

Digital signatures are a unique type of electronic signature in which information about the signer's identity and proof of their intent to sign are cryptographically bound to a signed document in an unalterable way. Depending on how they are created, digital signatures can carry much greater legal weight than traditional electronic signatures and convey the reliability of the signature over the long term. Simply put, digital signatures allow two or more parties to trust each other. If you are certain that the signature binds a specific signer to the contents of a specific agreement and can be enforced and legally defended if challenged, you can rely on that agreement as the basis for any decision.

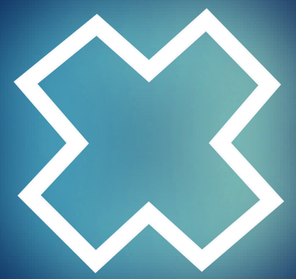
Universidad Tecnológica de Pereira | faceIT

- **Adobe Approved Trust List (AATL)**

Technical requirements define the level of identity verification required, the information that must be included in the certificate, and how it must be issued. AATL certificates must be generated using a trust system that protects the authorized holder's private key. Members are audited against the European Telecommunications Standards Institute (ETSI), WebTrust, and the International Organization for Standardization (ISO) audit programs to ensure they comply with their policies and procedures. This type of certificate can be validated in Adobe Acrobat or Reader.

- **Qualified Trust Service Providers (QTSPs)**

QTSPs must comply with standards defined by ETSI and must be audited by an accredited conformity assessment body. Users must have their identity verified with a high level of security before a qualified certificate can be issued. Only qualified signature creation devices (QSCDs) that are specially certified and validated by certification laboratories may be used to generate certificates.



TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

Signature formats

The industry chooses the PDF format as the additional content to preserve the presentation and placement on the document page, as well as all the cryptographic information associated with the signature. International standardization bodies have developed four different levels of PDF advanced electronic signature (PadES) formats to reflect the different information that can be captured. These formats determine the long-term reliability of a document:

PAdES-B-B : these base signatures are valid until the signature certificate is active (not revoked or expired).

PAdES-B-T : this level integrates a time stamp from a trusted source, proving that the document exists at a specific time.

PAdES-B-LT: This level integrates all the cryptographic elements required for signature validation and allows for offline signature validation with the help of the following integrated information:

- Signature certificate
- Certificate chain
- Hourdata server certificates
- Revocation data

PAdES-B-LTA: This level includes PAdES-B-LT and adds a cryptographic data element from a trusted source directly to the document. This proves that the validation elements exist at the time of signing, also ensuring future validity even if the signature algorithms or certificates expire.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT