I'm not a robot

Validate the signatures on your digitally signed documentClick to upload or drag and dropUpload Doc or PDF (MAX 100 MB)Upload from zDrive How to Validate a Digital Signature in a PDF: A Step-by-Step GuideIn todays digital world, ensuring that the documents we receive and send are genuine is crucial. One of the most secure ways to verify the authenticity and integrity of a document is through a digital signature. A digital signature not only confirms the identity of the person who signed the document but also ensures that the document has not been tampered with after being signed. But how do you validate a digital signature, especially in a PDF file? In this guide, well walk you through the process in simple terms. What is a Digital Signature?Before diving into how to validate a digital signature in a PDF, its essential to understand what a digital signature is. A digital signature is a mathematical scheme that verifies the authenticity and integrity of a digital message or document. Unlike traditional handwritten signatures, digital signatures are cryptographically secure and uniquely tied to both the document and the signer.Think of it like a virtual fingerprint: just as each persons fingerprint is unique, so is their digital signature. It ensures two key things:Authenticity: The person who signed the document is who they claim to be.Integrity: The document has not been altered after it was signed. Why Do We Need to Validate Digital Signatures?Validating a digital signature means confirming that:The signature is genuine.The document has not been altered since it was signed.Imagine receiving a contract that has been tampered with after being signedthis could lead to serious consequences! Thats why its so important to verify that the document is intact and the signer is legitimate. Tools for Validating Digital SignaturesBefore we move forward, lets go over some common tools and software that help in validating digital signatures in a PDF:Adobe Acrobat Reader DC: One of the most popular tools for viewing and validating PDFs. It has built-in features that make digital signature validation easy.Foxit Reader: Another lightweight and widely used PDF reader that supports digital signature validation.Online PDF Validation Tools: If you dont want to install any software, some online tools can validate signatures, but make sure they are trustworthy before uploading sensitive documents.PDF Studio: A commercial tool that is also great for managing and verifying digital signatures.Now, lets walk through the process of validating a digital signature using one of the most common tools: Adobe Acrobat Reader. Step-by-Step Guide to Validating a Digital Signature in a PDF (Using Adobe Acrobat Reader)Step 1: Open the PDF DocumentFirst, open the PDF file that contains the digital signature using Adobe Acrobat Reader DC. If you dont have the software installed, you can download it for free from Adobes official website.Step 2: Look for the Signature FieldOnce the document is open, scroll through the pages and look for the digital signature field. A digital signature in a PDF usually appears as a box or a section indicating that the document has been signed.Step 3: Click on the SignatureWhen you find the signature, click on it. This will open a pop-up or a new window that provides details about the signature.Step 4: Review the Signature PropertiesThe pop-up will show various details about the signature, including:The name of the signer.The date and time when the document was signed.The certificate authority (CA) that issued the digital certificate.Step 5: Check the Validity of the SignatureIn the signature properties window, youll see whether the signature is valid or not. Adobe Acrobat will display a message like Signature is valid if everything checks out.Step 6: Verify the CertificateA key part of validating the signature is ensuring that the digital certificate used to sign the document is trusted. Heres how to do it:Click on Signature Properties within the signature box.Under Signature Properties, click on Show Signers Certificate.A new window will appear showing details of the digital certificate. Check whether the certificate is issued by a trusted certificate authority (CA).If the certificate is not trusted or valid, Adobe Acrobat will alert you with a warning message. In that case, you should contact the sender of the document for verification.Step 7: Check for Any Document ChangesOnce the signature is validated, Adobe will also check if the document has been altered since it was signed. If the document has been modified, a warning message like Document has been changed since it was signed will appear. If no changes have been made, the validation message will confirm that the document is intact. What if the Signature is Not Valid?If the digital signature is invalid, or the certificate is not trusted, youll need to take a few extra steps:Contact the Signer: Its possible that the signers certificate has expired or their signature is corrupted. Ask them to re-sign the document with a valid certificate.Check Your Certificate Authorities (CAs): Ensure that the CA issuing the signers certificate is recognized by your system. You might need to update your list of trusted CAs. Digital Signatures vs. Electronic Signatures: Whats the Difference?Its easy to confuse digital signatures with electronic signatures, but they are not the same. Heres a quick breakdown:Electronic Signature: This can be as simple as typing your name into a document or using an image of your handwritten signature. Its legally binding in many situations, but its not as secure as a digital signature.Digital Signature: This is much more secure and uses encryption to authenticate both the signer and the document. It is legally recognized in most countries and provides greater protection against fraud. Why Trust the Certificate Authority (CA)?One of the key aspects of a digital signature is the certificate that verifies the signers identity. These certificates are issued by trusted third-party organizations known as Certificate Authorities (CAs). When you validate a digital signature, part of the process involves checking whether the CA is recognized and trusted.CAs have strict standards and procedures in place to verify the identity of individuals or companies before issuing a certificate. So, when you see that a signature is verified by a trusted CA, you can be confident that the signers identity has been thoroughly checked. Other Methods to Validate a Digital Signature in PDFsWhile Adobe Acrobat is one of the most common tools, there are other methods to validate a digital signature in a PDF.Using Foxit Reader:Foxit Reader is a lightweight alternative to Adobe Acrobat. Heres a quick guide to validating a digital signature in Foxit Reader:Open the PDF with Foxit Reader.Locate the signature field in the document.Click on the signature to view its properties.Check the certificate used to sign the document, and ensure its from a trusted CA.Verify that no changes were made to the document after it was signed.Online Tools:Some websites allow you to upload your PDF and validate the digital signature. While these tools can be convenient, they come with risks. Be cautious when uploading sensitive documents, as you are trusting a third-party service with potentially private information. ConclusionValidating a digital signature in a PDF is a critical step in ensuring the authenticity and integrity of a document. By following the steps outlined in this guide, you can easily verify whether a document has been signed by the right person and if it remains unchanged.Always use trusted software, such as Adobe Acrobat Reader, and ensure that the certificate authority issuing the digital signature is recognized. By doing so, youll protect yourself and your business from potential fraud or tampering.In a world where digital transactions are becoming more common, knowing how to validate a digital signature is an essential skill Digital signatures have become a cornerstone in digital-first environmentsbe it verifying the authenticity of a PDF, ensuring software packages are uncompromised, or securing email communications. Understanding how to verify digital signature accurately is critical to maintaining data integrity, preventing fraud, and ensuring compliance with security protocols across organizations. This comprehensive guide walks you through the entire process of signature verification. Whether you are an IT administrator, business user, or software developer, this blog provides step-by-step methods, tools, and best practices tailored to both technical and non-technical audiences. We also introduce how platforms like Certinal can streamline digital verification workflows. What Is a Digital Signature? A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital message or document. Unlike handwritten signatures, digital counterparts use encryption protocols and digital certificates issued by trusted Certificate Authorities (CAs). Core Components: Hashing algorithms (e.g., SHA-256) Signers private key Public key certificate Signature metadata (timestamp, algorithm details) When a document is signed, the hash of its content is encrypted using the senders private key. The recipient verifies it by decrypting the signature using the senders public key and ensures the contents match the original hash. If they do, the document is verified as untampered and authentic. Why Verification Is Crucial? Digital signature verification is not just a technical stepits a trust-building process. It ensures: Authenticity: Confirms the senders identity. Integrity: Validates that the document or message hasnt been altered. Non-repudiation: Prevents the signer from denying their involvement Organizations rely on this for everything from onboarding new clients and sharing financial reports to submitting government filings and sealing software distributions. How to Verify Digital Signature: Methods & Tools There are multiple ways to verify a digital signature, depending on the contextPDF files, emails, software, or code. Below are the most commonly used methods, complete with tools and step-by-step instructions. Method 1: Verifying Signatures in PDF Documents PDFs are among the most common formats requiring digital signature verification. Applications like Adobe Acrobat offer built-in mechanisms to validate signatures. Steps: 1. Open your signed PDF. 2. Locate the signature ribbon or signature panel. 3. Click Signature Panel for detailed information. 4. Look for the message: Signed and all signatures are valid. Learn How to eSign PDF in 6 Simple Steps Method 2: Command Line Signature Verification with OpenSSL Most developers and system administrators prefer OpenSSL to validate digital signatures via command-line when working with server files or secure documents. Requirements: Original data file Corresponding signature file Public key or certificate Command Format: openssl dgst -sha256 -verify publickey.pem -signature signature.sig signed_data.txt This command confirms whether the provided signature file matches the content in signed_data.txt. Method 3: Using Java for Programmatic Signature Verification For developers building secure applications, Javas cryptographic APIs offer full control over the verification process. Sample Code: Import java.security.*; import java.nio.file.*; Signature signature = Signature.getInstance(SHA256withDSA); signature.initVerify(publicKey); signature.update(Files.readAllBytes(Paths.get(data.txt))); boolean isValid = signature.verify(Files.readAllBytes(Paths.get(data.sig))); This snippet checks if the digital signature is valid for the given data file using DSA and SHA-256. Method 4: Verifying Email Signatures with S/MIME Email platforms like Outlook and Apple Mail support email authentication through S/MIME digital signatures. Steps: 1. Open the signed email. 2. Look for a seal or signature icon in the header. 3. Click on it to view signers digital certificate. 4. Ensure it is valid and issued by a trusted CA. Such verifications prevent phishing and ensure that messages are indeed from the claimed sender. Method 5: Validating Software Packages using GPG GPG (GNU Privacy Guard) is widely used to verify open-source software packages or repositories. Command: gpg verify [signature].sig [file] A successful verification will provide the signers key details and confirm the authenticity of the file. Method 6: Checking Software Signatures on Windows To verify EXE, MSI, and DLL files digitally signed on Windows: 1. Right-click the file Properties Digital Signatures tab 2. Select the listed signer 3. Click Details to view certificate and signature status 4. You should see, This digital signature is OK. This method is essential for validating that the software hasnt been tampered with since it was signed. Best Practices for Digital Signature Verification 1. Always validate the certificate chain 2. Ensure that certificates are traceable back to a trusted root CA and are not self-signed unless in a secure internal environment. 3. Check for revocation 4. Use Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) to rule out compromised or expired certificates. 5. Use timestamping 6. Validating the signatures timestamp ensures it was made while the certificate was still valid. 7. Confirm hashing algorithm integrity 8. Stick with secure algorithms like SHA-256 or SHA-512. Obsolete algorithms like MD5 should be avoided. 9. Validate in a secure environment 10. Always verify untrusted sources in sandboxes or isolated systems to prevent malware execution. Common Tools Used in Verification Tool Purpose OpenSSL Command-line verification Adobe Acrobat PDF signature validation GPG Verifying code and software packages Java Cryptographic APIs Programmatic signature checks Outlook / Apple Mail Email signature verification signtool.exe Windows code signature checks CertUtil Windows command-line certificate tools How Certinal Helps Streamline Digital Signature Verification Manual verification, while effective, can be time-consuming, error-prone, and complex in enterprise environments. This is where Certinal eSign solutions come into play. Certinal offers a robust, enterprise-grade digital signature platform that automates and simplifies the signature lifecycle, from signing to verification and audit trails. Using Certinal, companies can: Instantly validate digital signatures on documents and workflows Ensure compliance with international and U.S.-based digital signature laws (eIDAS, ESIGN Act, UETA) Use tamper-evident technology to detect any post-signing modifications Create audit trails to track signature activities in real-time Enable secure signing and verification via mobile or desktop devices Certinal seamlessly integrates with document management systems, CRMs, and ERPs, helping businesses accelerate their digital transformation securely. Conclusion Learning how to verify digital signature is a fundamental step toward establishing secure digital trust. From validating signed PDFs to verifying software executables on Windows, each method serves to protect the authenticity and integrity of your data. However, as organizations scale and handle thousands of digitally signed documents daily, manual approaches often fall short. Thats why automated, secure, and compliant platforms like Certinal are no longer optionaltheyre essential. Why take chances with document authenticity or waste time manually verifying digital signatures? Discover how Certinal can simplify your entire signature verification process and bring enterprise-grade security to your organization. Schedule your free demo today and experience the future of secure digital signing and verification with Certinal. Frequently Asked Questions (FAQs) 1. How do I verify a digital signature in a PDF file? Use a trusted PDF reader like Adobe Acrobat. Open the document, click the signature panel, and check certificate validity, timestamp, and document integrity status. 2. What does a valid digital signature look like? A valid digital signature includes a verified identity certificate, a trusted timestamp, and a tamper-proof hash. It should pass cryptographic and compliance checks. 3. Can a digital signature be verified without internet access? Basic verification (e.g., hash check) can work offline, but full certificate status validation usually requires an internet connection to access the certificate authority (CA). 4. Why is my digital signature showing as invalid? Common reasons include an expired or revoked certificate, untrusted certificate authority, modified document post-signing, or missing timestamp. 5. Is verifying a digital signature legally required? Yes especially in regulated sectors. Validating a digital signature ensures legal enforceability, regulatory compliance, and protection against fraud. Quick to start Easy-to-use 24/7 support Collect signatures 24x faster Reduce costs by $30 per document Save up to 40h per employee / month Best ROI. Our customers achieve an average 7x ROI within the first six months. Scales with your use cases. From SMBs to mid-market, airSlate SignNow delivers results for businesses of all sizes. Intuitive UI and API. Sign and send documents from your apps in minutes. Here isalist ofthe most common customer questions. Ifyou cant find ananswer toyour question, please dont hesitate toreach out tous. Need help?Contact support To validate a PDF signature online using airSlate SignNow, simply upload your document to our platform. Our tool will verify the authenticity of the signature and provide you with a detailed report on its validity. This streamlined process ensures you can confidently manage your signed documents. airSlate SignNow offers a cost-effective solution for validating PDF signatures online. We provide various pricing plans, ensuring that businesses of all sizes can access our features without breaking the bank. You can start with a free trial to see if our service meets your needs. With airSlate SignNow, you can validate PDF signatures online while also enjoying features like document tracking, real-time notifications, and customizable templates. These tools enhance your workflow and improve the efficiency of managing your documents securely. Our platform is designed to make the entire signing experience seamless. Yes, airSlate SignNow offers integrations with various applications such as Google Drive, Dropbox, and Salesforce. This allows you to streamline your document management processes and easily validate PDF signatures online from any platform you already use. Our API is also available for custom integrations. Security is a top priority at airSlate SignNow. Our platform uses industry-standard encryption to protect your documents and signature data during the validation process. You can trust that validating PDF signatures online through us is both safe and secure. Yes, airSlate SignNow supports bulk processing, allowing you to validate multiple PDF signatures online simultaneously. This feature is especially useful for businesses dealing with a high volume of documents, saving you time and ensuring efficiency in your signature verification process. Using airSlate SignNow to validate PDF signatures online offers numerous benefits, including increased efficiency, improved document security, and enhanced compliance. By streamlining your signature validation process, you can focus on your core business tasks while ensuring your documents are valid and trustworthy. Absolutely! airSlate SignNow provides dedicated customer support to assist you with any issues or questions related to validating PDF signatures online. Our team is available via chat, email, and phone to ensure you have the help you need at any time. Validate pdf signature online free Validate signature in PDF Adobe validate signature Signature not verified in PDF Digital signature verification Signature verification person Signature verification certificate Handwritten signature verification PDF digital signatures are a type of electronic signature that uses cryptography to ensure document authenticity and integrity. When a PDF is digitally signed, a unique fingerprint (hash) of the document is created and encrypted with the signer's private key.Key aspects of PDF digital signatures:Document Integrity: Any change to the document after signing will invalidate the signatureSigner Authentication: Digital certificates verify the identity of the signerNon-repudiation: Signers cannot easily deny their signature, as it requires their private keyTimestamping: Provides proof of when the document was signedCommon Use Cases:Legal documents and contractsFinancial statements and reportsGovernment forms and applicationsMedical records and prescriptionsTechnical documentation and certificationIt's important to note that PDF signatures can be configured in different ways. Some signatures allow specific types of changes after signing (like form filling), while others lock the entire document. This tool checks if the document has been modified in ways not permitted by the signature. Key Takeaways Rise in document fraud: Validating eSignatures isnt optional for enterprises its critical to protect against tampering and ensure authenticity. eSign validation is the process of verifying that an electronic signature is authentic, untampered with, and legally valid according to regulatory standards. Up to 68% TAT Reduction with SignDesk eSign; Businesses using SignDesk eSign experience dramatic improvements in turnaround time and operational efficiency. With a 67% rise in digital fraud and document tampering, validating eSign online is no longer optional its a must-have competitive edge. From customer onboarding to vendor contracts and legal agreements, every e-signed document requires verification for authenticity, integrity, and legal compliance.Thats why over 3,000 leading enterprises trust SignDesk to power their eSign workflows. Giving compliance teams, legal heads, and CXOs the assurance they need, in just a few clicks.In this step-by-step guide, well explore how to validate eSign online quickly, accurately, and securely so your business stays compliant, protected, and ahead. eSign validation is the process of checking whether a digital or electronic signature on a document is:Authentic (signed by the right person),Intact (not tampered with after signing),Legally valid (compliant with the Indian IT Act 2000, and global standards).A digital audit trail, which proves the integrity and legality of your document. To validate eSign, you must follow these steps:Step 1: Open the Signed PDFUse a trusted PDF viewer, such as Adobe Acrobat Reader, to open the document containing the e-signature.Step 2: Look for Signature PanelOnce the file opens:A blue ribbon or green checkmark will typically appear at the top, indicating that Signed and all signatures are valid.Alternatively, click on Signature Panel to see more information about the signer.Step 3: Check Signature PropertiesClick on the signature and select Signature Properties:View the signers name and organization.Verify certificate details (issued by CCA in India for DSCs).In the Certificate Viewer window, click the tab named Trust.Click Add to Trusted Certificates. Click OK in the pop-up that follows.You will be redirected to the Import Contact Settings window. Check (Tick) the boxes provided before Certified documents and the three other options that follow. Then click OK to continue.Click Validate Signature in the Signature Properties window. And then click Close.Now your eSign is complete. Your eSign will have a green-colored Tick mark, which means it is validated.Step 4: Validate Certificate Trust ChainEnsure that the digital certificate is:Issued by a licensed Certifying Authority (like eMudhra, Capricorn, etc.).Valid and not expired.Not revoked or tampered with.Who Should Care About eSign Validation?If youre in any of the following roles, validating eSigns should be your daily hygiene:Legal Heads to ensure contracts hold up in court.Compliance Officers to meet the IT Act, RBI, SEBI, or GDPR standards.Finance Teams to validate NDAs, vendor agreements, or invoices.HR/Onboarding Teams to verify signed agreement, offer letters, joining forms, etc. Its 2025, and more than 83% of businesses have adopted e-signatures, considering them a more secure option. From loan approvals and NDAs to procurement deals and patient records, eSignatures are everywhere.But heres the catch when documents are sent without proper signature validation, millions of contracts are potentially at risk, not only legally, but financially. Unverified eSign open the door to forgery, manipulation, and unauthorized edits. In sectors that handle sensitive data, such as banking, insurance, and healthcare, its a serious security lapse.When contracts cant be validated:They may not hold up in courtAudit teams face compliance red flagsBusinesses expose themselves to reputational and financial damage Under the Information Technology Act, 2000, and global e-signature laws (such as eIDAS in the EU), only digitally verified signatures are legally binding. Without proper validation, even a digitally signed document may fail legal scrutiny.In regulated industries such as BFSI, legal, and healthcare, unverifiable eSignatures can lead to contract disputes, compliance penalties, and other issues, resulting in an annual revenue loss of up to 9%. For CXOs, legal heads, and compliance officers, eSignature validation is not optional its mission-critical. A validated signature ensures:The signers identity is verifiedThe document is tamper-proofAn audit trail is in placeThe contract is admissible in courtValidated eSignatures create trust not just between you and your customer, but across internal teams, regulators, and stakeholders. Yet, it is common for people to make mistakes. Below are three common eSigned document validation issues professionals encounter and how you can fix them without losing time or trust.1. Signature Not VerifiedWhat it means: This typically occurs when you open an eSigned document in an outdated or incompatible version of PDF software (like Adobe Reader). The tool fails to recognize or validate the signature algorithm.How to fix it:Update your Adobe Acrobat Reader to the latest version from the official site.Reopen the document, and click the Signature Panel to refresh validation.If needed, manually trust the signers certificate.Insight: According to a security research report, 56.46% of enterprise users running Adobe have an outdated version installed, resulting in more validation errors than necessary.2. Unknown IssuerWhat it means: The signers certificate isnt linked to a recognized Certificate Authority (CA), or your system doesnt trust the issuing authority by default. This breaks the trust chain.How to fix it:Click on the signature Signature Properties Show Signers CertificateGo to the Trust tab Click Add to Trusted CertificatesTick all boxes (certified documents, identity, and dynamic content), then hit OKPro Tip: Always ensure the certificate is issued by a valid CA licensed under Indias Controller of Certifying Authorities (CCA).3. Revoked or Expired CertificateWhat it means: The signers digital certificate was either revoked (invalidated before expiry) or has crossed its validity period. These certificates cannot be validated unless they are replaced.How to fix it: Reach out to the document issuer and request a new version signed with an active certificate. For internal workflows, revoke the old signing request and initiate a fresh eSign process.Reality Check: Digital certificates typically last between 1 and 2 years. Failure to monitor certificate validity can lead to rework, delays, and compliance penalties, particularly in regulated sectors such as BFSI and legal.By proactively managing signature validation, you protect your organizations credibility, timelines, and legal enforceability.Key Benefits of Validating eSignatures: Peace of Mind & PerformanceSpeed up deal closuresReduce legal risksEnsure clean auditsClean brand integrityDont leave your contracts to chance! Let SignDesk help you seal every deal eSign securely and quickly. Long turnaround times, rising operational costs, and mounting compliance risks are everyday hurdles thats where SignDesk eSign makes all the difference. We offer quick and secure e-signing, allowing you to validate it even more quickly.SignDesk eSign: Verified, Secure, Instant e-SigningSignDesks eSign platform empowers enterprises to sign, share, and store legally valid documents digitally. The platform is fully compliant with Indian regulations like the IT Act, UIDAI guidelines, and CCA standards.Aadhaar-based eSign: Easily authenticate signers with OTP-based or biometric Aadhaar verification. AI-Enabled Verification: Enhance signer identity assurance using geofencing, liveness detection, and AI-powered face match. Its ideal for high-value or sensitive agreements.Digital Signature Certificates (DSC): Offer high-assurance signing using DSC-based signatures, best-suited for legal, financial, and regulatory documentation. Fully API-Enabled & Scalable: Integrate seamlessly into your workflows with enterprise-grade APIs, audit trails, and multi-party signing features. Scale confidently as your operations grow.Real Impact, Real Outcomes: Fyers Success StoryTake Fyers, a leading name in Indias fintech space.They faced rising pressure from customers due to the slow and manual processing of paperwork, especially during high-volume periods. SignDesk stepped in with a customized eSign solution, designed to handle bulk signing with speed and precision.The results?Turnaround time (TAT) dropped from days to just a few hoursOver 1,000 eSigns processed daily, effortlesslyHappier customers and increased onboarding ratesFyers didnt just fix a broken process they scaled faster and delivered better experiences. SignDesk is the go-to partner for industry leaders across finance, legal, HR, and procurement. Heres how we help teams like yours:68% reduction in TAT: Get documents signed instantly, not after days of follow-ups.Process 45 M+ documents/year: Empower remote teams to operate anywhere, anytime.100% paperless = significant cost savings: No more printing, couriering, or scanning.Scalable to 48,000+ signs/month: Our platform grows with your business.What does this mean for you? Quick eSigning and faster validation = Frictionless contract closures! Most importantly, faster, more innovative customer experiences.Ready to see what SignDesk can do for your business? Join thousands of forward-thinking companies. Transform 1.6x faster with SignDesk eSign Yes, its entirely legal under the IT Act and accepted by courts and regulators across India. No, you can simply open the document in Adobe Reader and validate it; it takes just a few clicks. Check the eSign validation process. It usually means the certificate isnt trusted yet, or you may be using an older version of Adobe. You can easily resolve the issue by adjusting your trust settings. Enterprises typically use automated scripts or validation tools within PDF software to check signatures at scale. Teams also establish internal workflows to review, verify, and archive documents efficiently. Digital signature tools have been an incredible addition to our technology-rich world and help streamline decades-old PDF processes. But how do you make sure your signatures cant be forged? Or that they havent already been manipulated? Carry on reading to find out!When Do You Need To Verify a Digital Signature?If youve used an electronic signature tool that youre unfamiliar with, you probably want to make sure your signed PDF is legally binding, and your signature is considered valid before sending it to anyone, especially if its a legal document. By verifying your signature, you can relax knowing that no one can alter your signature or information without affecting the validity of the document. If the file hasnt been validated yet, you can do that in Adobe Reader.Its also important to verify that signed documents are authentic and havent been tampered with. This would come in handy to ensure that your agreements and contacts are genuine and that no forgery was involved in the creation of the signature.Note: Both electronic and digital signatures can be legally binding. Depending on where you live, an electronic signature can carry the same legal weight as an ink signature, whereas digital signatures offer a host of additional features for added security.If youre keen to learn more about the legality of digital signatures, read our article on the trustworthiness of digital signatures here.How To Verify a Digital Signature in a PDFIf youve recently received a signed document, or youve used an e-signing tool like Sign.com, you can verify that signatures are authentic by using a variety of PDF readers. Follow these easy steps to verify a signature with Adobes free PDF Reader:Open the signed document you want to verify.Select the fountain pen symbol on the left side.If needed, click on the arrow to open the drop-down menu.Check for Signature is Valid. You might see Signature not yet verified, in which case you can Validate All to start the process.

Desarrollo organizacional wendell l. french. Wendell french desarrollo organizacional pdf. French wendell.