Progress ShareFile

Beyond “Just an E-Signature”

A Practical Guide to eIDAS-Compliant Signature Levels for Every Agreement

EBOOK

Choosing the Right Signature Levels Matters Under eIDAS

At the turn of the century, the European Union set new expectations for member states regarding electronic document signing. As society's reliance on digital interactions grew, the directive evolved into the Electronic Identification, Authentication and trust Services or eIDAS regulation. Introduced in 2014, it is designed to verify electronic interactions between organizations and businesses are secure, efficient and consistent across member states.

Although digital engagement was already prevalent at the time, no one predicted the exponential reliance on technology that followed the global pandemic. The need for social distancing forced organizations worldwide to adapt quickly. As a result, the way people engaged with businesses, organizations and one another fundamentally shifted, making eIDAS Regulation all the more important.

The Regulation today provides governance for digital signatures and trusted services, which electronically create, validate and verify electronic signatures, certificates, seals and time stamps, as well as a European-wide framework for digital identity through the European Digital Identity Wallet.

As you can imagine, the Regulation is not the only thing that has evolved over the past 25 years. Today, digital signatures vary in their level of assurance and use. European Parliament and Council identify three distinct levels under eIDAS, all of which can be legally binding—Simple Electronic Signature (SES), Advanced Electronic Signature (AES) and Qualified Electronic Signature (QES)

3 Levels of Electronic Signature

- **Simple Electronic Signature (SES)**
  Basic electronic signatures, often acceptable for low risk approvals.
- **Advanced Electronic Signature (AES)**
  Stronger identity assurance and tamper evidence for most business critical agreements.
- **Qualified Electronic Signature (QES)**
  The highest level under eIDAS—treated like a handwritten signature in court.

Choosing the right one can be the difference between "probably fine" and "bullet proof."
This eBook is designed to help you better understand when and why to use each one.

This guide is provided for general information and informational purposes only and does not constitute legal, compliance or risk advice. Decisions about which signature level to use for any given workflow should be made by appropriately qualified members of your organization (such as Legal, Compliance, Risk or other designated experts) who understand the specific laws, regulations and contractual obligations that apply. Your organization remains solely responsible for assessing its requirements and for any consequences arising from how electronic signatures are implemented and used.

SES vs AES vs QES Plain-Language Definitions

You don't need to be an expert in EU Regulations to choose the right signature level, but you do need to understand how each option differs.

Simple Electronic Signature (SES)

When speed and convenience matter most.

Benefits

- Broad coverage of "everyday" electronic approvals under eIDAS, from click through consents to typed names in a document
- Ease of use and deployment, with no special hardware or identity checks required, making it ideal for high volume, low risk interactions
- Legal validity as an electronic signature when it can demonstrate who signed, their intention to sign and what they agreed to
- Minimal friction for signers, helping drive completion rates for routine forms and acknowledgments

Example SES Use Cases

- Everyday consents & acknowledgments: "An online service uses SES for newsletter opt ins and privacy policy updates, keeping proof of consent without slowing users down."
- Low risk internal approvals: "A small business uses SES for internal expense approvals and simple policy sign offs, prioritizing speed over heavy weight identity checks."

Advanced Electronic Signatures (AES)

When you need strong, scalable trust.

Benefits

- Unique linkage to the signer with ability to identify them
- Tamper detection to note if anything is changed in the document after signing
- Suitability for most commercial contracts and high volume workflows
- Strong evidentiary support in the event of disputes without adding friction

Example AES Use Cases

- Customer contracts and SOWs: "A regional services firm uses AES for thousands of client agreements each year—balancing strong proof with a smooth signing experience."
- HR and employment documents: "An HR team uses AES for employment contracts and policy acknowledgments, keeping a clear audit trail without slowing down hiring."

Qualified Electronic Signatures (QES)

When "this absolutely must stand up in court."

Benefits

- Compliance support with all AES requirements, plus stricter identity verification
- Use of qualified certificates issued by approved service providers
- High-assurance signature creation, supported by secure devices
- Strong legal presumption under eIDAS, equivalent to a handwritten signature.

Example QES Use Cases

- High value financing agreements: "A bank executes large credit facilities with QES to minimize legal uncertainty across multiple jurisdictions."
- Regulated public sector approvals: "A government agency uses QES for formal decisions that legally must be signed 'in writing' under national law."

Choosing the Right Level: Side by Side View

To determine which level is right for your needs, start by asking two things: “What happens if this signature is challenged?” and “What does the law or policy require?”

If the legal risk and transaction value are low, a simple electronic signature is usually enough and keeps things moving fast for users. As the stakes rise—whether your money is at risk, there is regulatory scrutiny or cross border enforcement—it’s wise to consider upgrading to advanced electronic signatures as your default for business contracts and HR documents. Reserve qualified electronic signatures for the small subset of use cases where either regulation explicitly calls for them or your risk team would lose sleep if the signature were ever questioned in court.

Level	When to use	Typical documents	Trust & friction balance
SES	High volume, low risk agreements where convenience and speed are more important than strong identity proof	Newsletter opt ins, basic web forms, internal approvals, low value commercial agreements	Lowest assurance, lowest friction; good enough if the risk of dispute or fraud is low
AES	Commercial agreements where you need reliable signer identification and tamper evidence without over burdening users	Customer contracts, SOWs, HR documents, higher value B2B deals	Strong assurance with moderate friction; default choice for most business contracts
QES	High risk, high value or legally prescribed situations where you must maximize evidential weight	Large financing deals, regulated public sector decisions, signatures that must legally equal “wet ink”	Highest assurance with highest setup friction; use where the law or risk profile clearly demands it

Rule of Thumb

Default to AES for most business critical workflows and step up to QES when regulation or risk clearly demand maximum assurance.

A Simple Checklist for Your Next Agreement

Use this checklist as a quick triage tool, not a case by case legal opinion. Ask teams to classify each workflow by legal requirement, transaction risk and user friction—then apply the suggested default (SES, AES or QES) for that category. Legal and compliance can then focus on reviewing only the exceptions where teams want to deviate from the standard.

Checklist: Picking SES, AES or QES

Check legal or policy requirements

1. Does a law, regulator or internal policy explicitly require a qualified signature or "equivalent to handwritten?"	**Use QES**
2. Does it just say "electronic signature" with no higher requirement?	Continue

Assess transaction value and risk

1. Is the value low and impact of a dispute minor (e.g., marketing consents, basic internal approvals)?	**SES is usually enough**
2. Is there significant money, long term obligations or reputational/ regulatory risk?	Continue

Evaluate evidence needs

1. Do you need strong proof of who signed and that the document was not altered (typical for B2B contracts and HR docs)?	**Use AES as your baseline**
2. Is maximum evidential weight critical (e.g., you expect possible court scrutiny across borders)?	**Prefer QES if practical**

Consider user experience and friction

1. Are signers external customers or non-EU citizens and completion rates are crucial?	
• Low risk workflow • Medium/high risk workflow	• **SES** • **AES with user friendly identity methods**
2. Are signers internal staff or professional counterparties who can handle more steps?	
• High risk or tightly regulated workflow • Most other business/HR workflows	• **QES** • **AES**

Standardize by category

1. Define default:	
• Low-risk • Standard business contracts/HR • Exceptionally high-risk or prescribed by law	• **SES** • **AES** • **QES**
2. Document these defaults so teams can apply them consistently without re-deciding every time.	

eIDAS-Compliant Signatures in Practice

Below are a few scenarios that demonstrate how SES, AES and QES typically map to real world documents in Accounting & Tax, Legal, Financial Services and Public Sector industries.

The table is not exhaustive nor jurisdiction specific, but it gives organizations a practical starting point for deciding which signature level to use for common engagement letters, contracts, customer agreements and government workflows.

Level	Accounting & Tax	Legal	Financial Services	Public Sector
SES	Basic engagement confirmations, low value quotes, routine internal approvals	Low risk NDAs, event T&Cs, simple consent forms, internal sign offs	Everyday customer consents, low value account changes, standard disclosures	Staff acknowledgments, low value grants, routine citizen consents and forms
AES	Engagement letters, recurring service agreements	Commercial contracts, NDAs, routine settlements	Standard product terms, mid risk customer agreements	Supplier contracts, smaller grants, internal approvals
QES	POA mandates, high value representation agreements, certain regulatory filings	High stakes settlements, cross border agreements where enforceability is critical, documents with written form requirements	Loan contracts, mortgage documents, account openings with strict KYC/written form rules	Formal administrative decisions, high value grants, public tenders that require handwritten equivalent signatures

Decisions about which signature level to use for any given workflow should be made by appropriately qualified members of your organization (such as Legal, Compliance, Risk or other designated experts) who understand the specific laws, regulations and contractual obligations that apply.

eIDAS-Compliant eSignatures Built Directly into ShareFile Workflows

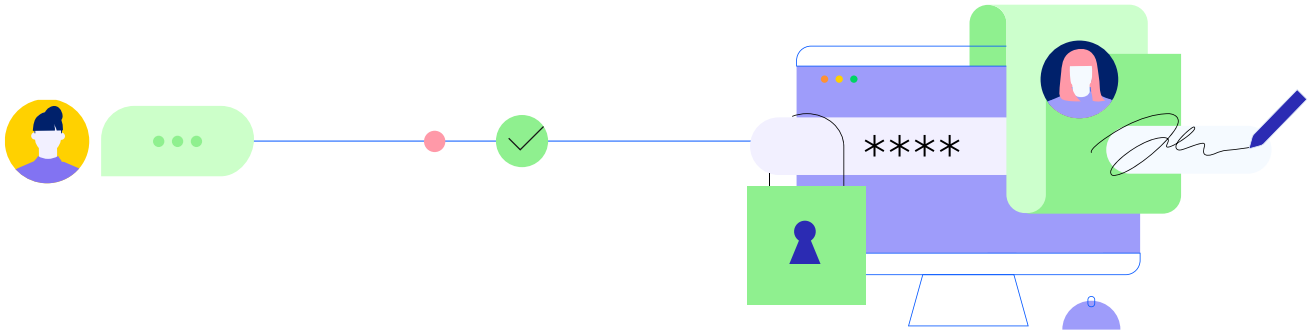
With Progress® ShareFile® software, you don't have to choose between effective collaboration and compliant signing. SES, AES and QES are built into the same secure platform you already use for file sharing and document workflows, so teams can pick the right level of trust without jumping between tools.

One Platform, Three Levels of Trust

- **Start in the ShareFile platform:** collaborate on the document, collect inputs and finalize the version to sign.
  - Admins can enable eIDAS Signatures feature for the entire account from: Account Settings => Signature
- **Choose the signature level:** select AES for most business agreements, QES for higher risk and regulated workflows. SES should be selected when the burden of proof is low—it should not be used for sensitive or legally complex agreements.
- **Route for e signing:** send documents to internal and external signers with clear instructions built into the system.
- **Enable eIDAS authentication:** access the eIDAS Authentication section in the Signature Request Details page when configured
- **Review completed signatures:** view authentication details and results once signing is finalized.
  - Signature level (AES or QES)
  - Authentication provider used
  - These details are also recorded in the audit history & Signature certificate. This provides a complete compliance record.

How it Works in Practice

Accounting firm onboarding a new EU client	Bank approving a high value loan	Public sector agency awarding a major grant
Scenario: A mid sized accounting firm signs a new client for annual audit and advisory services	**Scenario:** A bank issues a multi year, high value credit facility to a corporate customer	**Scenario:** A government agency signs grant agreements with organizations across multiple Member States
Recommended level: AES for the engagement letter; QES only for specific POAs or mandates when required by regulation	**Recommended level:** QES for the loan contract and associated security agreements to maximize enforceability	**Recommended level:** QES for final grant agreements; AES for supporting documentation and acknowledgments
How it works in ShareFile software: Partners review and finalize the engagement letter in a shared folder, send it for AES signing via ShareFile e-signature and store the fully executed agreement alongside all client workpapers	**How it works in ShareFile software:** Credit and Legal teams collaborate on the documentation in the ShareFile platform, initiate a QES signing process from the same workspace and retain all signed contracts and evidence together	**How it works in ShareFile software:** Program staff manage application documents in ShareFile, then send final grant agreements for QES signing from within their existing folders and workflows



Ready to Right Size Trust in Your Agreements?

Talk with us about designing SES, AES and QES into your most important workflows in ShareFile software or start with our pilot for one critical process.

The ShareFile integrated eIDAS-compliant e-signature tool is feature-rich, allowing you to get files signed in record time, all within a single secure tool.

Document Packager
Merge multiple documents into a single file for faster signatures.

Bulk Send
Share the same document for multiple signatures in one send

Multi and Sequenced Signing
Ask multiple people to sign the same document in a specific, set order

Enhance Security
Add extra layers of security with included Knowledge-Based Authentication (KBA), passcodes and expiration dates

Add Your Logo
Use branding options to customize the experience with your company logo

Reusable Templates
Save frequently-used documents as templates to quickly send for signature

Upload Your Signature
Add a personal touch by uploading an image of your handwritten signature

DocGen Templates
Create and customize reusable documents in MS Word—no more starting from scratch

Signature Certificates
Get a downloadable PDF that records every action taken, from send to sign

About Progress ShareFile Software

Secure, All-in-One Collaboration for Outstanding Client Experience

Today's clients expect more than just good service. They want a modern, easy and secure experience. As the world becomes more digital-first, both accounting and legal firms need tools that help them work smarter while delivering the high-quality interactions clients now demand.

ShareFile software is built to do exactly that with an all-in-one platform that brings file sharing, client collaboration and workflow automation together in one place without adding complexity or compromising security.

Client processes like onboarding are faster and easier, so teams can deliver work more efficiently and spend more time on higher-value tasks. Automated document requests, approvals and e-signatures help streamline processes and improve turnaround times.

ShareFile features also fit right with the tools you already use, like Microsoft 365 and other business applications, making it easy to adopt without disrupting how you work.

The result? Better experiences for clients, smoother workflows for teams and the confidence that your data stays protected every step of the way.

To learn more about how to modernize your client experience with ShareFile software, visit our site.

About Progress Software

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and personalized digital experiences with agility and ease. Businesses of all sizes get a trusted provider in Progress, with the products, expertise and vision they need to turn AI disruption into a competitive advantage. Millions of developers and technologists at hundreds of thousands of organizations depend on Progress every day. Learn more at www.progress.com

/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress