The Time For A Digital Signature Is Now

by Enza Iannopollo

June 18, 2020

Why Read This Report

The COVID-19 pandemic has forced consumers, employees, and partners to dramatically change their digital habits and adopt new ones. These new behaviors are here to stay, and businesses are under pressure to digitize fully and quickly. Digital businesses around the world will add digital signatures to their toolkits, and security and risk pros (S&R) must help them evaluate, choose, and deploy the best option to support their digital transformation.

Key Takeaways

The Demand For Digital Services Will Intensify
Social distancing has forced people to use digital services as never before. They expect businesses to respond to and anticipate their new digital needs.

eIDAS-Like Rules Promote Best Practices
From its roots as a specific European regulation, eIDAS is shaping the digital signature market globally. It increases the security and legality of transactions involving customers, businesses, and even machines.

Digital Signatures Increase Trust, With Few Compliance Burdens For Companies
The adoption of digital signatures means businesses must ensure their systems are compliant; however, the right vendor can take care of most of the compliance burden.

The Time For A Digital Signature Is Now

by Enza Iannopollo
with Martin Gill, Kate Pesa, and Peggy Dostie

June 18, 2020

Table Of Contents

Related Research Documents

Decentralized Digital Identity: A Primer

Forrester Infographic: The State Of Digital Transformation In Financial Services, 2020

New Tech: Decentralized Digital Identity (DDID), Q1 2020

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

The Digital Signature Market Is On The Verge Of A Lifetime Opportunity

Electronic signature technology is not new. It underpins digital transformation of processes and operations, and firms across verticals have adopted it. With consumers and employees now forcing companies to become more digital, this market is on the verge of transformation.[1] But electronic signatures are not all the same. From simple e-signatures that typically rely on an email address for identification purposes, to robust and highly secure options, customers can choose among:

- **Electronic signatures (e-signatures).** This type of electronic signature is the most widely used. An e-signature is an electronic symbol attached to a contract or other record that a person with an intent to sign uses.[2] The definition of "symbol" is very broad, which provides a lot of flexibility.[3] If one can prove that data hasn't been tampered with, e-signatures can be legally binding in certain geographies.

- **Digital signatures.** Digital signatures offer greater assurance than simple e-signatures about the identities of the parties involved in a transaction. They embed a personal key infrastructure (PKI) into the signing process to identify both the party requesting a signature and the party providing one. This also guarantees that an electronic document is authentic. eIDAS defines advanced signatures and qualified signatures as types of digital signatures.

- **Advanced signatures.** Advanced signatures are an intermediate approach between a simple e-signature and a qualified signature. Advanced signatures are legally binding. They uniquely identify and link its signatory. They offer strong security because: 1) the private key used to create the signature is under the sole control of the signatory and 2) the signature identifies whether the data has been tampered with after the message has been signed, invalidating the signature. This last feature is essential to make the signature legally binding.

- **Qualified signatures.** This signature carries higher probative value and can't be challenged easily because the authorship is considered nonrepudiable. These signatures are stronger than advanced signatures. The difference between the two is the addition of a qualified certificate. This certificate is issued by a qualified trust services provider (TSP), and it attests to the authenticity of the electronic signature to serve as proof of the identity of the signatory. Simply put, a qualified signature further increases the level of security that an advanced electronic signature provides.

The eIDAS Regulation Defines Digital Identity And Trust Services Providers

The electronic identification and trust services (eIDAS) regulation creates a harmonized approach — including requirements and standards — across the EU for trust services supporting identity attribution, authentication, and signature.[4] An increasing number of geographies, including some countries in South America, have adopted similar standards and regulations, which means eIDAS-like requirements are going global. Countries that lack similar regulations, such as the US, must look at qualified trust services providers for best practices. eIDAS has shaped the digital signature market. It:

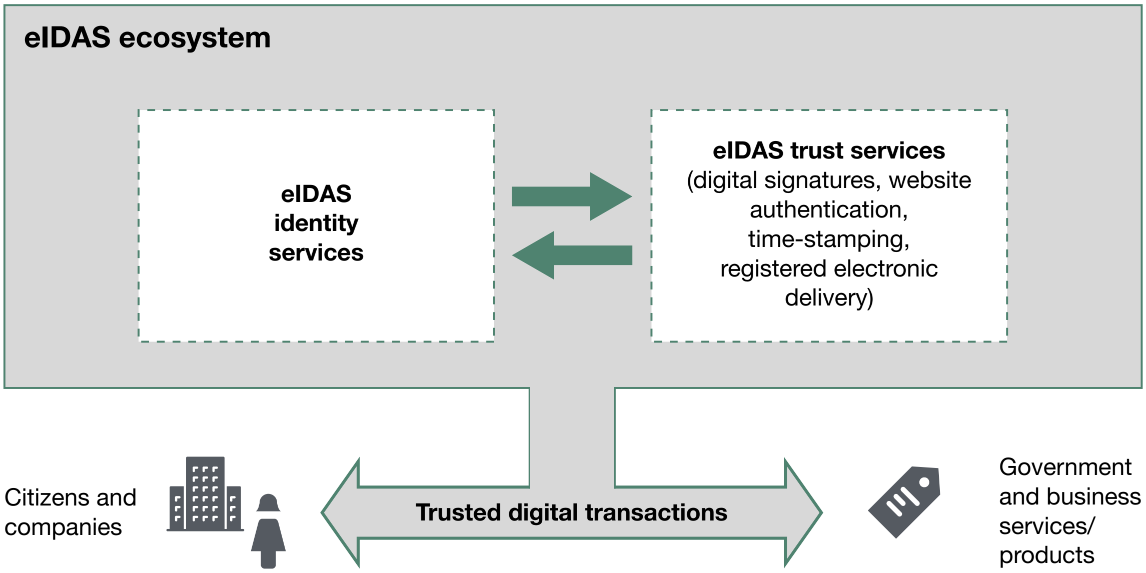
- **Defines the role of providers of digital identities.** These providers help organizations answer the “who are you” question. In other words, they certify citizens’ digital identities. This role was primarily intended for governments. They can digitally identify citizens and companies and mutually recognize them, connecting their identification and authentication infrastructures.[5] This means, for example, that electronic identities (eIDs) issued in Germany or Austria can access Dutch online public services.[6] Consumers can also use their eIDs for commercial purposes, such as opening a bank account across countries. Companies can use them, too, such as B2B electronic invoicing.

- **Recognizes trust services providers.** These providers help organizations answer the “how to prove who you are” question. They provide identity authentication and signature (non-repudiation services), which creates trust among parties: These services make parties accountable for their actions.[7] While eIDs and TSPs are covered by different parts of the regulation, TSPs often depend on the same identity verification checks required to issue an eID. TSPs that meet the highest eIDAS quality requirements are “qualified trust services providers” (QTSPs) and can act as a certification authority (CA) and issue qualified identity certificates.[8]

- **Promotes cooperation and enables business across Europe.** Every business transacting over a public network needs assurance about participants’ digital identities and their actions in binding contracts. Using qualified providers of trust services (identity attribution, authentication, and signature) means transactions will be binding and recognized across Europe without too much compliance burden, as the qualified trust services provider takes care of compliance requirements. S&R and I&O teams have to deal only with the solution’s deployment and potential residual risk.

- **Evolves digital transaction management use cases.** Classic digital transaction management — signing, sharing, and storing documents — is evolving. TSPs assist clients with services such as timestamping, website authentication, and registered electronic deliveries. Edge use cases are also emerging, including management of digital identities, electronic invoicing, attribution and management of machines’ identities, etc. Namirial offers video-based consulting on documents, DocuSign has developed a validator (software that autovalidates compliance with specific legal requirements for data sciences), and InfoCert offers identity attribution and verification for machine-to-machine (M2M) communication (see Figure 1).

FIGURE 1 eIDAS Defines Identity Services/Trust Services Providers As Key Enablers Of Trusted Digital Processes


eIDAS ecosystem
eIDAS identity services
eIDAS trust services (digital signatures, website authentication, time-stamping, registered electronic delivery)
Citizens and companies
Trusted digital transactions
Government and business services/ products

The Adoption Of Digital Signatures Is A Business Priority

Growth expectations for the digital signature market were high even before the pandemic. In fact, the value of this market is expected to reach $5.5 billion by 2023.[9] A number of factors will push growth even further: 1) The pandemic will force governments to accelerate digitization of services; 2) growing consumer demand for environmental sustainability will boost the adoption of greener solutions such as digital signatures; and 3) consumers' new digital habits will force companies to intensify efforts to digitally transform.[10] These new digital habits mean that customers are willing to engage in higher risk transactions, which requires S&R pros and their organizations to strengthen the underlying security of these services and seek more assurance about users' identities. S&R pros must move quickly to enable their firms to securely meet the digital demands of their employees, customers, and business leaders.

Post-Pandemic Engagement Requires Companies To Strengthen Their Signature Toolkit

Companies that so far relied only on simple e-signatures must rethink that strategy. While national legislation should indicate which transaction requires which signatures, each company should decide which risk mitigation strategy it prefers to adopt for simplest, higher-value, and higher-risk transactions. Once the pandemic is over:

› **Hybrid workplaces will require appropriate tooling.** Most companies had to embrace work from home overnight out of necessity when COVID-19 struck. There is no way back. Companies are pushing for some of their workforce to embrace work from home as the new normal, beyond the pandemic. Twitter aims for 100% of its employees to work from home. Other companies' objectives range from 20% to 50% or more. This means that a greater volume of transactions that traditionally relied on signing documents must be carried out digitally. Companies must equip themselves now to ensure that their employees can tackle whatever level of assurance a transaction requires.

- **Consumers that embraced new digital habits will stay digital.** Our data shows that consumers are embracing new digital habits during the pandemic: 22% of Italian, 19% of French, and 15% of UK online adults have purchased groceries online for the first time as a result. And for the first time, 18% of Italian online adults paid bills online, 17% banked online, and 15% used a digital payment method.[11] Consumers in France and in the UK followed a similar path. Next time consumers need to open a bank account, they will do so digitally. Remote identification and digital signatures will become basic, daily business requirements. And with increasing concerns over identity fraud, S&R pros will welcome a more secure approach to identity verification and management.

Digital Signatures Deliver Even More Value In The Post-Pandemic World

The original goal behind the creation of eIDAS was to harmonize standards and requirements for electronic identities, authentication, and signatures across European countries. The creation of a trust services infrastructure not only delivers on that objective, but it also allows providers to deliver tangible business benefits — and even more so in a post-pandemic world. QTSPs:

- **Make onboarding new customers more secure.** QTSPs deliver on both security and customer experience through flexible onboarding platforms. From the initial data collection to the activation of the account, for example, onboarding platforms help banks take care of all necessary steps, including remote identification, signature, compliance with requirements such as anti-money laundering (AML), and long-term archiving. Digital onboarding offers stronger governance, too. A digital native bank reduced fraud by 80% through a digital onboarding platform.[12]

- **Deliver on CX and business outcomes.** Companies want to create digital experiences that customers like and come back for. InfoCert's Trusted Onboarding Platform enables banks to approve instant lending for their customers, including real-time scoring and with a fully digital process.[13] Namirial's DTM platform goes to market with fully flexible deployment options to support digital engagement with a wide range of services and a white-labelled solution.[14] GlobalSign works with the US' top preemployment screening service provider, USAFact, to provide a secure, streamlined contract signing process for its end customers' 600 field sales reps.[15]

- **Support customers' decentralized digital identity management.** As the boundary between physical and digital interactions becomes indistinguishable, decentralized digital identity (DDID) frameworks are emerging to provide trusted, portable, verifiable, use-centric digital identities.[16] In a DDID ecosystem, claim/proof issuance is recorded on a blockchain-based ledger without storing any PII on it. This means no central identity provider owns the identity. Instead, individuals and businesses can securely share their trusted digital identity with entities that request it. It's not a small change. The potential for disruption is high. QTSPs such as Signicat are positioning themselves as DDID implementation providers, offering specialized turnkey solutions for DDID in specific verticals.[17]

- **Can assure the security of M2M communications.** Automation is changing the workplace as we know it. Machines dealing with increasingly sensitive tasks and decisions need trusted identities, and companies need assurance that M2M communications are secure and have not tampered with. QTSPs such as InfoCert and GlobalSign developed offerings that target this specific use case. They offer clear audit, traceability, certainty, and trust about machine identities and their communication channels.
- **Support compliance across a number of regulatory requirements.** Banks and financial services providers must comply with an array of requirements about their customers' identities and their transactions. Banks leverage QTSPs qualified digital identities and services to comply with know your customer and anti-money-laundering regulations. But new use cases are emerging. The European Payment Service Directive 2 (PSD2) and connected standards require strong customer authentication (SCA). SCA is improved authentication where customers initiate online payments or access an account. QTSPs can support this use case.[18] Namirial, for example, launched a new PSD2-compliant Strong Customer Authentication Platform.

Recommendations

Choose Your QTSPs Based On Risk Appetite And Legislation

The digital signature market has witnessed tremendous growth through partnerships, agreements, and acquisitions among IT companies. DocuSign acquired SpringCM, Entrust Datacard acquired Barcelona-based Safelayer Secur, and InfoCert acquired Camerfirma and LuxTrust.[19] To respond to businesses' digital needs during and after the pandemic, vendors are partnering even more. This is the right time to choose your QTSPs. S&R pros and their business partners must:

- **Focus on the use cases you want to tackle first.** There is a plethora of vendors out there and the market moves quickly. S&R pros and their business partners must focus on specific use cases they want to tackle first. Support for digitizing workflow and empowering employees working from home has been a priority for many organizations in recent weeks.
- **Look at transactions' risk profiles and legislation to choose your level of assurance.** Across European countries, national legislation defines whether a digital signature is required for certain transactions. But this is only the first element S&R pros should consider when choosing their signature providers. They must also consider: 1) the risk profile of the specific transaction; 2) the risk appetite of the organization; and 3) local market practices. For example, companies in Germany have traditionally relied more on qualified signatures than other countries in Europe, regardless of specific legal requirements.

- **Mind privacy and residency requirements when you deploy the solution.** eIDAS compliance doesn't lift any GDPR requirements. Privacy rules still apply to personal data of employees and customers, including rules for physical location of data. Most solutions offer long-term archiving, too. Make sure that data collection, processing, sharing, and storage comply with relevant privacy requirements.
- **Cocreate solutions for evolving digital use cases.** It's not unusual for QTSPs to work with their clients to ensure that they address emerging needs. When you choose a provider and its services, think broadly about how the digital strategy of your company might evolve and how QTSPs can help you make it more secure and trustworthy. Challenge your provider to leverage their technical capabilities to meet your evolving use cases.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Airslate

DocuSign

GlobalSign

HelloSign

InfoCert

Namirial

Nuvola Group

Signix

Endnotes

[1] Source: “Digital Signature Market by Solution (Software and Hardware), Service, Deployment Mode, Application (BFSI, Government & Defense, Legal, Real Estate, HR, Manufacturing & Engineering, Healthcare & Life Sciences), and Region - Global Forecast to 2023,” Markets and Markets, September 2019 (https://www.marketsandmarkets.com/Market-Reports/digital-signature-market-177504698.html).

[2] As defined by the US ESIGN law of 2000. Source: “Electronic Signatures In Global And National Commerce Act,” GovInfo, June 30, 2000 (https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf).

[3] It can be a keystroke, the swipe of a stylus, or even a selected checkbox.

[4] Source: “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing,” EUR-Lex, July 23, 2014 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG).

[5] Source: “First cross border, eIDAS compliant connections achieved!” e-SENS, February 3, 2017 (https://www.esens.eu/content/first-cross-border-eidas-compliant-connections-achieved).

[6] However, eIDAS does not provide for an EU-wide database of citizens. Each member-state and organization maintains its own database. The eIDAS-mandated identity services component simply provides cross-border recognition on an as-requested basis.

[7] Under Regulation (EU) No 910/2014 (eIDAS), a Trust Service Provider (TSP) is defined as “a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.”

[8] A list of qualified trust services providers (QTSPs) can be found in the following websites. Source: “EU Trusted Lists,” European Commission (https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers) and “QTSPs and eIDAS,” Open Banking Europe (https://www.openbankingeurope.eu/qtsps-and-eidas/).

[9] Source: “Digital Signature Market by Solution (Software and Hardware), Service, Deployment Mode, Application (BFSI, Government & Defense, Legal, Real Estate, HR, Manufacturing & Engineering, Healthcare & Life Sciences), and Region - Global Forecast to 2023,” Markets and Markets, September 2019 (https://www.marketsandmarkets.com/Market-Reports/digital-signature-market-177504698.html).

[10] Source: “Europe’s COVID-19 Outlook: eGovernment Services Accelerate,” Forrester (https://www.forrester.com/fn/5dBXvIlG3X4xc6z4Juqt6A).

Source: “Europe’s COVID-19 Outlook: Environmental Sustainability Will Take Center Stage As Digital Legislation Slows,” Forrester (https://www.forrester.com/fn/6p9MjLEIBkfOKgelq6BK8d).

[11] We surveyed 1,118 UK online adults, 1,116 French online adults, and 1,137 Italian online adults between April 10 and April 15. Source: Forrester Analytics Consumer Technographics® COVID-19 Survey (Wave 1).

[12] Source: “Top,” InfoCert, May 27, 2019 (https://docs.infocert.digital/top/files/top-overview.pdf).

[13] Source: “Customer Onboarding,” InfoCert (https://infocert.digital/solutions/customer-onboarding/).

[14] Source: “Namirial Digital Transaction Management,” NamirialGmbh, July 25, 2016 (https://www.xyzmo.com/Downloads/Documents/en/Namirial_DTM_Solution.pdf).

[15] Source: “GlobalSign’s Digital Signing Service Provides USAFact with Ability to Secure and Streamline the Contract Signing Process for End Customer’s 600 Field Sales Reps,” GlobalSign press release, March 10, 2020 (https://www.globalsign.com/en/company/news-events/news/globalsigns-digital-signing-service-provides-usafact-ability-secure-and-streamline-contract-signing-process-end-customers-600-fi).

[16] For more information, see the Forrester report “New Tech: Decentralized Digital Identity (DDID), Q1 2020.”

[17] For more information, see the Forrester report “Decentralized Digital Identity: A Primer.”

[18] For more information, see the Forrester report “Retailers, Use PSD2 To Drive Differentiation For Your Customers.”

[19] Source: “DocuSign Completes Acquisition of SpringCM,” DocuSign press release, September 4, 2018 (https://www.docusign.com/press-releases/docusign-completes-acquisition-of-springcm).

Source: “Entrust Datacard Acquires Barcelona-Based Safelayer,” Entrust Datacard press release, November 8, 2018 (https://www.entrustdatacard.com/about/newsroom/press-releases/2018/entrust-datacard-acquires-barcelona-based-safelayer).

Source: “The joint venture between InfoCert, LuxTrust, and Camerfirma goes pragmatic on February 26th in Luxembourg,” InfoCert (https://infocert.digital/the-joint-venture-between-infocert-luxtrust-and-camerfirma-goes-pragmatic-on-february-26th-in-luxembourg/).

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

› Research and tools
› Analyst engagement
› Data and analytics
› Peer collaboration
› Consulting
› Events
› Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
› Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.