

Public Disclosure Authorized



Public Disclosure Authorized

ELECTRONIC SIGNATURES

ENABLING TRUSTED DIGITAL TRANSFORMATION

Public Disclosure Authorized

Public Disclosure Authorized

DIGITAL TRANSFORMATION
POLICY NOTE SERIES
SEPTEMBER 2024





© 2024 The World Bank
1818 H Street NW, Washington DC 20433
Telephone: +1-202-473-1000; Internet: www.worldbank.org

Some rights reserved.

This work is a product of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.





Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given. Cover photo: © Shutterstock, Inc. Used with the permission of Shutterstock, Inc. Further permission required for reuse. Cover Design: [add name here]


Attribution - Please cite the work as follows: "Tullis, Christopher; Constantine, Nay; Cooper, Adam. 2024. Electronic Signatures: Enabling Trusted Digital Transformation. © Washington, DC: World Bank."

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: +1-202-522-2625; e-mail: pubrights@worldbank.org.

TABLE OF CONTENTS

	Disclaimer	6
	About ID4D	7
	About KWPF	7
	Acknowledgements	7
	Executive summary	8
	1. Introduction	10
	2. Electronic signature basics	13
	2.1 Enabling trust in the digital economy	13
	2.2 Digital versus electronic signatures	13
	2.3 Authenticating electronic transactions	15
	2.4 Electronic signature use cases	16
	2.5 Common myths	18
	3. Trusted (electronic) transactions	21
	3.1 What is a signature anyway?	21
	3.2 Sources of trust	23
	4. Trust framework	24
	4.1 The role of a trust framework	24
	4.2 Tiered trust: Levels of assurance	25
	5. Legal framework	27
	5.1 The role of the legal framework	27
	5.2 Mutual recognition	30



	6. Technical implementation	32
	6.1 A variety of possible technologies	32
	6.2 The role of public key cryptography	33
	6.3 The role of digital identity	35
	7. Conclusions	37
	7.1 Strategic	37
	7.2 Legal and regulatory	37
	7.3 Technical	38
	8. Appendices	39
	Appendix 1: Glossary of key terms	39
	Appendix 2: Electronic signature use cases	41
	Appendix 3: Good practice legal frameworks	43
	Appendix 4: From analog to digital trust	46



Figures

Figure 1: Layered model of digital trust	12
Figure 2: How electronic and digital signatures support authentication of electronic transactions	15
Figure 3: Use cases of electronic signatures	18
Figure 4: How signatures increase trust in transactions	22
Figure 5: Functional equivalence of electronic signatures	29
Figure 6: Digital and electronic signatures	35



Tables

Table 1. Electronic signature versus digital signature	14
Table 2: Risk-based approach to analyzing electronic signature use cases	17
Table 3: eIDAS levels of assurance: Summary of key features	26
Table 4: Examples of advanced electronic signature implementation	33
Table 5: Examples of qualified electronic signature implementation	33
Table 6: Relevance of cryptography to electronic signature functionalities	34
Table 7: Illustrative example of the roles of providers of digital identity and trust services	36
Table 8. Common electronic transactions across sectors grouped by risk level	41
Table 9. UNCITRAL texts and key milestones	44



DISCLAIMER

This Policy Note is a reference document to be consulted by governments, development partners, academics and others when considering, designing, implementing, or managing national electronic signature ecosystems. It is not intended to be a comprehensive guide for planning World Bank operations. This Note is based on evolving international good practice, as understood by the World Bank's Digital Development practice. It reflects experiences in a range of countries from different regions, with different legal systems, and at different stages of economic development. It also takes into account existing literature, laws, model laws, and norms and principles. There is no guarantee that addressing all the issues raised in this Note will result in successful design, installation, or management of a national electronic signature ecosystem—as doing so will depend on the consideration of many factors, which may be different from country to country. While every attempt has been made to be complete, there may be issues affecting the design, establishment, and operation of a national electronic signature ecosystems that are not addressed in this Note, or that are addressed in the context of certain assumptions, facts, and circumstances that do not apply equally to every situation. This Note is a reference tool only.

ABOUT ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from the World Bank Group, Bill & Melinda Gates Foundation, the UK Government, the French Government, the Australian Government, the Norwegian Agency for Development Cooperation, and the Omidyar Network.

To find out more about ID4D, visit id4d.worldbank.org.

ABOUT KWPF

This work is supported through the Korea-World Bank Partnership Facility (KWPF), a single-donor trust fund sponsored by the government of South Korea and administered by the KWPF Program Management Team within the World Bank Group. KWPF supports projects that identify, implement, and scale sustainable development solutions in developing countries around the globe, drawing on the significant experience and expertise gained by South Korea across its own development journey.

ACKNOWLEDGMENTS

This policy note was authored by Christopher Tullis, Nay Constantine, and Adam Cooper. Excellent feedback and input were provided throughout the development of this guide. The authors thank the following individuals for their various contributions: Audrey Ariss, David Black, Victoria Esquivel-Korsiak, Issam Khayat, Daria Lavrentieva, Viky Manaila, Jonathan Marskell, Slavina Pancheva, David Porteous, Lara Wanna, Gillan Ward, and Matthew Zoller. The authors are also indebted to invaluable comments from our expert peer reviewers Harish Natarajan, David Satola, and Vijay Vujjini.



EXECUTIVE SUMMARY

Trust lies at the foundation of all commercial and administrative transactions, which for centuries have relied upon the handwritten signature for authentication. As transactions are digitalized, the signatures that provide trust in them must also become electronic. The lack of trusted and legally-recognized means of authenticating electronic transactions has forced a continued reliance on in-person handwritten signatures, undermining digitalization efforts by necessitating recourse to in-person interaction to complete a transaction.

In-person handwritten signatures in the analogue world are not a particularly secure means of authentication. When transactions are digitalized, new security issues arise, as the ease with which digital data can be duplicated or altered introduces additional vulnerabilities that never existed with paper. To address these concerns, electronic signature frameworks provide a means of authenticating the various electronic transactions in a way that facilitates the emergence of a trusted digital economy.

This policy note presents electronic signatures in terms of their four main functions: (1) identifying the signer, (2) attributing the signature to the signer, (3) recording the signer's intent to sign, and (4) assuring the integrity of the signed data and protecting against tampering. Not all transactions require a high degree of assurance of all four of these functions. Indeed, for lower-risk transactions, attempting to assure a high level of trust in all four functions may be counterproductive, for example, if doing so leads to excessive cost or frictions for users that dissuade them from transacting in the first place. Therefore, policy makers should balance priorities between security and usability to ensure widespread adoption of electronic signature solutions.

Because different types of transactions have very different requirements, electronic signature frameworks should be designed around a risk-based approach that allows different approaches according to the needs of the use case. Low risk use cases may have very basic requirements. Whenever we click an "I agree" button to consent to terms and conditions, enter a PIN code to authorize a payment, or type our name at the end of an email or text message—all of these gestures

may represent a form of electronic signature. Attempting to regulate such techniques out of existence in an attempt to replace them with more sophisticated mechanisms can be counterproductive. However, as transactions become riskier—for example, due to a high monetary value or a risk of legal liability—more sophisticated electronic signature solutions may be necessary to enable digitalization. Cryptographic techniques, in particular, can be used to protect the integrity of signed documents and prevent subsequent tampering. Such sophisticated electronic signature techniques can provide a very high level of trust, enabling even the highest-value and riskiest transactions to be safely digitalized. Full digital transformation cannot occur unless all transactions, regardless of risk, can be brought online.

The element of "trust" in electronic signatures is composed of a set of complementary and mutually reinforcing layers. Each layer builds on the lower layers to extend trust beyond what can be achieved without it. The foundational layer is rooted in existing "analog" sources of trust. The role of a trust framework should not be to crowd out these existing sources of trust but instead to build on them. Trust frameworks accomplish this by formalizing a set of minimum requirements for electronic signatures, providing transparency in their reliability. Trust frameworks should not only focus on the technology components, but also the people and process elements, which are as—if not more—important for providing trust. Finally, the legal framework gives legal weight to the rules in the trust framework and clarifies when and how signatures can be legally recognized, both domestically and across borders. A key function of the legal framework is to give electronic signatures the same legal weight as handwritten signatures. Many legal frameworks accomplish this by enshrining the legal equivalence of electronic and paper signatures into law, ensuring that signatures provided online are not disqualified from having a legally binding nature.

The policy note concludes with suggestions at the strategy, legal, and technical levels. Governments should design electronic signature frameworks according to demand, aligning with the needs of users and verifiers. They should seek to promote adoption across the digital economy by addressing barriers and balancing security and usability, while

promoting interoperability. Taking a risk-based approach that defines outcome-based levels of assurance can provide for an electronic signature scheme that supports both low- and high-risk transactions. Trust frameworks should ensure strong linkages with legal identity systems for digital verification and authentication, enhancing trust in electronic signatures.

Maintaining technology neutrality can promote innovation and product differentiation, allowing systems to evolve and scale with changing requirements. Implementations

requiring sophisticated cryptographic technologies, such as public key infrastructure, should be limited to high-risk use cases where the additional cost and complexity of such approaches is justified. Aligning trust frameworks with international standards can facilitate cross-border recognition, ensuring trust and facilitating cross-border trade. Governments should support sustainable business models for the actors implementing electronic signatures and facilitate private sector participation to maintain long-term financial viability.



1 INTRODUCTION

As the world becomes increasingly digital, the need for secure, efficient, usable, and legally-recognized methods of transacting online becomes ever more important. Electronic signatures are a key enabler of digital transactions, allowing parties to interact online while being able to trust that they are protected from the various types of fraud that can otherwise plague digital interactions.¹ Electronic signatures can provide assurance of the identity of the parties to a transaction as well as protect the integrity of a transaction by preventing *ex post* modification of important details, such as contract² terms or transaction amounts. Alongside other techniques for authenticating electronic transactions,³ electronic signatures are a vital component in the move towards paperless environments, as they reduce costs and streamline processes in both private and public sectors, enhance customer experience in electronic commerce, and facilitate the expansion of the digital economy.

Although the legal frameworks explicitly regulating electronic signatures tend to be more developed in higher-income countries, widespread use of electronic signatures is a common occurrence in countries of all income levels. For example, when a poor, smallholder farmer uses a mobile money account to cash out a social assistance benefit or pay his children's school fees, the PIN code he types into his phone to authenticate his identity and authorize the transaction is a simple form of electronic signature.

So, if electronic signatures are already having a transformational effect worldwide without necessarily requiring any specific attention or regulation, what is the purpose of this policy note? The answer lies in the need

to move past the limitations of current, often-rudimentary electronic signature frameworks to avoid bottlenecking the continuous development of the digital economy. Why, for example, can the PIN code on the farmer's mobile phone not be used to authorize other types of transactions apart from those on his mobile money account? Why are such electronic signatures seemingly confined to specific sectors of the economy, and often not available for interactions with government? Why is it typically only low-value aspects of service delivery that are digitalized today, with higher-value transactions still requiring an in-person visit to sign a paper form? This note will explore the ways that regulations can improve trust in electronic signatures, allowing them to be used to authenticate higher-risk transactions.

In low-income contexts, electronic signatures can support financial inclusion by enabling digital banking as well as e-commerce, extending the reach of these sectors to remote populations that are often difficult to access. Similarly, in public services, electronic signatures can make government services more accessible and efficient by reducing bureaucratic hurdles and improving transparency. However, implementing electronic signatures in such contexts does come with unique challenges, such as mitigating adoption barriers like poor connectivity, limited digital skills, and trust issues among users. Despite these challenges, the potential benefits of using electronic signatures to facilitate digital transformation makes them an essential tool in the digital age across all regions of the world.

1 OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, 2007, accessible at: <https://www.oecd.org/digital/ieconomy/38921342.pdf>

2 For the sake of simplicity and ease of understanding, this note uses the term "contract" to refer to various types of legal acts, not necessarily limited to contracts in the strict legal sense. For example, a signature may also be considered in the context of a will, which legally is not considered a contract between parties but rather a unilateral act. This note elides such distinctions for the sake of simplicity.

3 The nomenclature of the techniques used for authentication of electronic transactions can vary according to jurisdiction. Some legal frameworks reserve the term "signature" for cases where signatories are natural persons, distinguishing them from cases where transactions carried out by legal persons, such as firms or government entities, with a related term such as "stamp" or "seal." Other techniques, such as securing a communication channel, may also provide additional trust and contribute to the transaction being considered authentic. For additional discussion, see also, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, accessible at: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf>

To this end, the purpose of this note is to guide policy makers through the implementation of effective trust and legal frameworks to enable the use of robust and fit-for-purpose electronic signatures throughout the digital economy. The note is relevant for policy makers working on such electronic signatures frameworks at national, regional, or sectoral levels. Following a brief presentation of electronic signatures and their role in enabling the digital economy, the bulk of the note focuses on how to create the policy environment needed to provide for trust in, and adoption of, electronic signatures by users and relying parties.⁴

A premise of this note is that “trust” in digital interactions is not solely, or even primarily, a function of technology choices, but is rather a product of various people, process, and contextual factors. These multi-dimensional sources of trust complement, and in many cases pre-exist, the application of digital technologies. The note examines how the enabling environment can be calibrated to further two parallel objectives: (1) capitalizing on existing sources of trust in the analog world and bringing them into the digital economy, and (2) leveraging digital technologies to extend this trust to new types of transactions as well as to interactions with actors who would not otherwise be trusted. Achieving both goals simultaneously has the potential to multiply the number of electronic transactions while also increasing confidence in them, thereby enabling the growth of the digital economy. Conversely, failure to achieve either of these objectives would pose a significant bottleneck to the growth of online transactions.

The note analyzes “trust” in electronic signatures as a set of complementary and mutually-reinforcing layers. Each layer builds on the lower to extend trust beyond what can be achieved without it.

Layer 1: Sources of trust

- *Pre-existing trust.* Trust can stem from existing sources, such as parties who already know each other, in addition to contextual sources of trust, such as a secure communication channel.
- *Evidence of reliability.* Existing sources of trust can be extended using various techniques—with people, process, and technology elements—to provide evidence of a signature’s reliability beyond what would be possible relying only on pre-existing trust.

Layer 2: Trust framework

- *Requirements for evidence and assurance.* The sources of trust are then formalized and extended through a trust framework, which lays out minimum requirements for the people, process, and technology elements of a signature that provide evidence of its reliability. The trust framework extends trust through standardization and transparency.
- *Levels of assurance.* The trust framework may also include multiple levels of assurance or levels of trust. Such tiered requirements can better support the needs of transactions of varying risk levels, allowing a signature of appropriate strength to be matched with a transaction of corresponding risk.

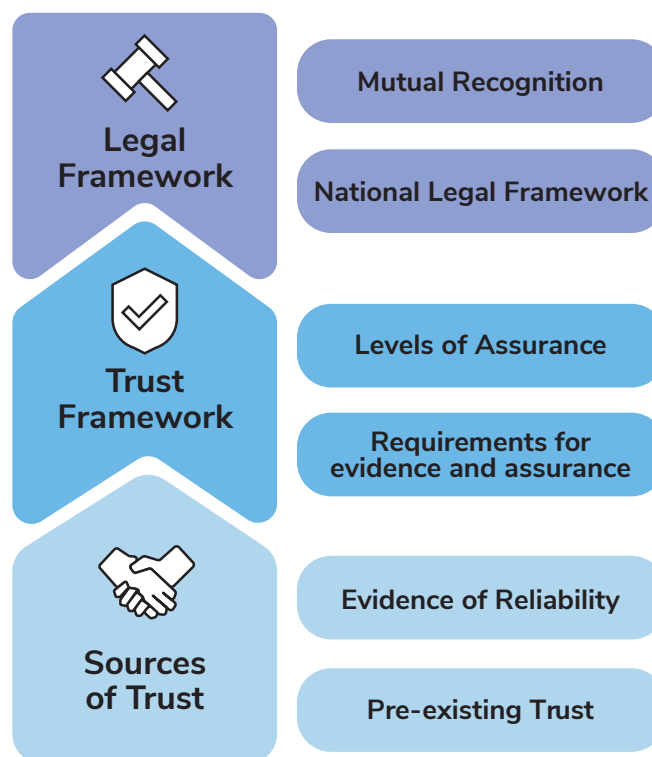
Layer 3: Legal framework

- *National legal framework.* The legal framework is the set of laws and regulations governing electronic transactions and signatures. It establishes the legal validity and enforceability of the trust framework and clarifies the legal implications, in particular the conditions under which electronic signatures are considered equivalent handwritten signatures.
- *Mutual recognition framework.* To ensure a common basis for trust and cross-border recognition and interoperability of electronic signatures, legal and trust frameworks can be harmonized internationally, extending trust across borders.

Exact details of how electronic signatures can be implemented using any specific technology is outside the scope of this note. References to specific technologies—whether paper-based or digital—are made only for illustrative purposes, and thus should not be interpreted as comprehensive or as endorsements of the technologies cited. In particular, the details of how high-trust electronic signatures (sometimes referred to as “qualified electronic signatures”) can be implemented using cryptographic techniques and accompanying public key infrastructure (PKI) is outside the scope of this note; readers interested in learning more about PKI implementation models should refer to the companion note in this series entitled, *Public Key Infrastructure: Implementing High-Trust Electronic Signatures*. Additionally, the scope of this note does not cover in detail all the various related techniques that exist

⁴ A relying party is an entity (person or organization) that relies on an electronic signature by verifying it.

Figure 1: Layered model of digital trust



for authenticating electronic transactions (e.g., stamps and seals), but instead focuses on the particular case of electronic signature. Although all electronic authentication techniques are covered comprehensively, it should be noted that the technical, legal, and operational underpinnings of methods such as electronic seals are very similar to those used for electronic signature, and due to this, much of the discussion in the present policy note may apply to those authentication methods as well.

enable trusted electronic transactions and scale the digital economy. It builds on previous analytical and normative work, in particular work done by the World Bank,⁵ the United Nations Commission on International Trade Law (UNCITRAL),⁶ the International Telecommunications Union,⁷ the United Nations Conference on Trade and Development (UNCTAD),⁸ the Organization for Economic Cooperation and Development (OECD),⁹ and others.

This note is intended to give practical guidance to practitioners on implementation of electronic signatures to

⁵ Examples of relevant work include:

World Bank. 2016. *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank.

World Bank. 2021. *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank.

⁶ UNCITRAL. 1996. *Model Law on Electronic Commerce*. Vienna: UNCITRAL.

UNCITRAL. 2001. *Model Law on Electronic Signatures*. Vienna: UNCITRAL.

⁷ International Telecommunication Union (ITU). 2019. ITU-T X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Geneva, Switzerland: ITU.

⁸ UNCTAD has engaged extensively in work related to e-commerce, including facilitating electronic transactions and fostering trust in the digital economy. Their work includes research, policy analysis, and technical assistance to developing countries, aiming to create an enabling environment for e-commerce and digital trade.

⁹ Examples of relevant work include:

OECD. 2015. *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*. Paris: OECD Publishing. <https://oe.cd/dsrm>

OECD. 2019. *Recommendation of the Council on Digital Security of Critical Activities*. OECD/LEGAL/0479. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456>



2 ELECTRONIC SIGNATURE BASICS

2.1 ENABLING TRUST IN THE DIGITAL ECONOMY

For the digital economy to develop, many face-to-face interactions will need to move online, and paper-based transactions will need to be conducted using digital means. The inherent security vulnerabilities of electronic communications systems raise the following question:

1. *How can we ensure that electronic transactions are at least as trusted as paper ones?*

The current state of digital transformation in many countries is uneven and incomplete, with certain transactions being digitalized while others remain paper based. Some transactions can be initiated online, but at some point, an in-person interaction is required to sign a registration form, transaction order, or consent form. The reverse may also be true, with initial onboarding for a service requiring an in-person signature before the door opens to future online interactions. End-to-end digital transactions and administrative processes remain the exception, especially in lower-income countries. More often than not, incomplete digitalization is due to transaction risk. Lower-risk aspects of a transaction can be carried out digitally or online, while higher-risk aspects require paper processing due to a lack of digital solutions to prevent fraud. Digitalization of business processes cannot lead to full digital transformation if high-risk transactions cannot also be brought online. This raises an additional question:

2. *How can we make electronic transactions even more trusted than paper ones?*

Although a primary concern with electronic signatures is security and fraud prevention, the development impact of the digital economy will be limited if these signatures are not usable, accessible, and adopted by users. The premium on usability and accessibility is particularly high

for use cases related to digitalization of basic services for the population. Ensuring relevance to use cases with high development impact and avoiding deepening of digital divides will require attention to accessibility and adoption. Thus, another question arises:

3. *How can we reduce the friction of carrying out electronic transactions?*

Reducing friction will increase transaction efficiency and reduce barriers for end users, however, successfully implementing electronic signature usage across the digital economy ultimately depends on lowering cost. Without cost-efficiency, the development impact of trusted electronic transactions will be mitigated by low adoption. Thus, the final question is:

4. *How can we reduce the cost of carrying out trusted electronic transactions?*

This question and the ones leading up to it will be addressed in the following sections.

2.2 DIGITAL VERSUS ELECTRONIC SIGNATURES

Electronic signatures are a legal concept. The term is relevant in cases where there is a need for a transaction carried out electronically to be considered legally equivalent to its analogue equivalent. Such transactions could be commercial (e.g., signing a contract), administrative (e.g., issuing an official document), or involve individual signers (e.g., consenting to a medical procedure).

At the simplest level, an electronic signature is any data in electronic form, associated with other data, used by a signatory to sign. Electronic signatures are technology neutral and concerned with enabling trust in electronic transactions along with legal recognition. Technical

sophistication and trust can vary widely, from a simple name typed at the bottom of an email to a trusted implementation of a PKI-based digital signature. Electronic (and indeed all) signatures presume that the signer is an individual person.¹⁰

Not to be confused with the legal concept of electronic signatures, digital signatures are a technological concept. The term digital signature refers to a specific way of assuring the authenticity of a document or communication using techniques based on public key cryptography. In contrast to the technology-neutral concept of electronic signature, digital signatures are a technology-specific technique, allowing for robust cryptographic verification of the association between the signature and the digital certificate

used to generate it. It should be noted that digital signatures also have myriad uses outside of implementing high-trust electronic signatures—such as securing everyday internet browsing—which are outside the scope of this paper.¹¹

While digital signatures refer to the technical process of assuring trust through cryptographic verifiability, the term electronic signature introduces a socio-legal dimension of trust.¹² Digital signatures are often used to implement electronic signatures, which include any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. The two related but distinct notions are compared in the below table:

Table 1. Electronic signature versus digital signature

Term	Definition	Implementation	Scope
Electronic Signature	Legal concept denoting a signature generated using electronic means for the purposes of authenticating an electronic transaction. ¹³	Technology-neutral	A technique for authenticating legally binding electronic transactions.
Digital Signature	Technology concept denoting a signature generated using the private key embedded in a PKI-based digital certificate.	Technology-specific (PKI)	Applications both within and outside the sphere of legally binding electronic transactions.

¹⁰ Legal entities and juridical persons cannot “sign” per se but may use equivalent techniques referred to as electronic seals or stamps. For further discussion, see for example, UNCITRAL. 2009. “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods.” Vienna: UNCITRAL.

¹¹ Readers interested in a detailed discussion of digital signature use cases are referred to the companion paper, Christopher Tullis and David Black (2024), *Public Key Infrastructure: Implementing High-Trust Electronic Signatures*, Washington D.C: World Bank.

¹² This note follows the convention of associating the term “electronic signature” to contexts where the focus is on signatures to enable legally recognized electronic transactions and reserving the term “digital signature” to refer to specific technology implementations using cryptographic techniques for assuring integrity and authenticity based on public key infrastructure. Although this terminological distinction is fundamentally arbitrary, making it allows for a convenient way to distinguish between two very different phenomenon, which is why the distinction is maintained here. Readers should note that several jurisdictions use these terms differently; in the United States and India, for example, the term “digital signature” is used to refer to the highest-trust electronic signatures provided for in national regulations.

¹³ Examples of more technical definitions can be found in relevant electronic signature legislations. For example, according to the EU eIDAS Regulation (2014), electronic signature means “Data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign.” Alternatively, in UNCITRAL Model Law on Electronic Signatures (2001), “data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message.”

2.3 AUTHENTICATING ELECTRONIC TRANSACTIONS

Legally, a transaction or document is generally regarded as “authentic” if there is sufficient evidence that it is what it—or its proponent—claims it to be.¹⁴ In the context of an electronic transaction carried out online, this means that the results of the transaction accurately reflect the intentions and understanding of the parties that carried it out. The parties could be natural persons, legal entities (juridical persons), or a combination of the two.

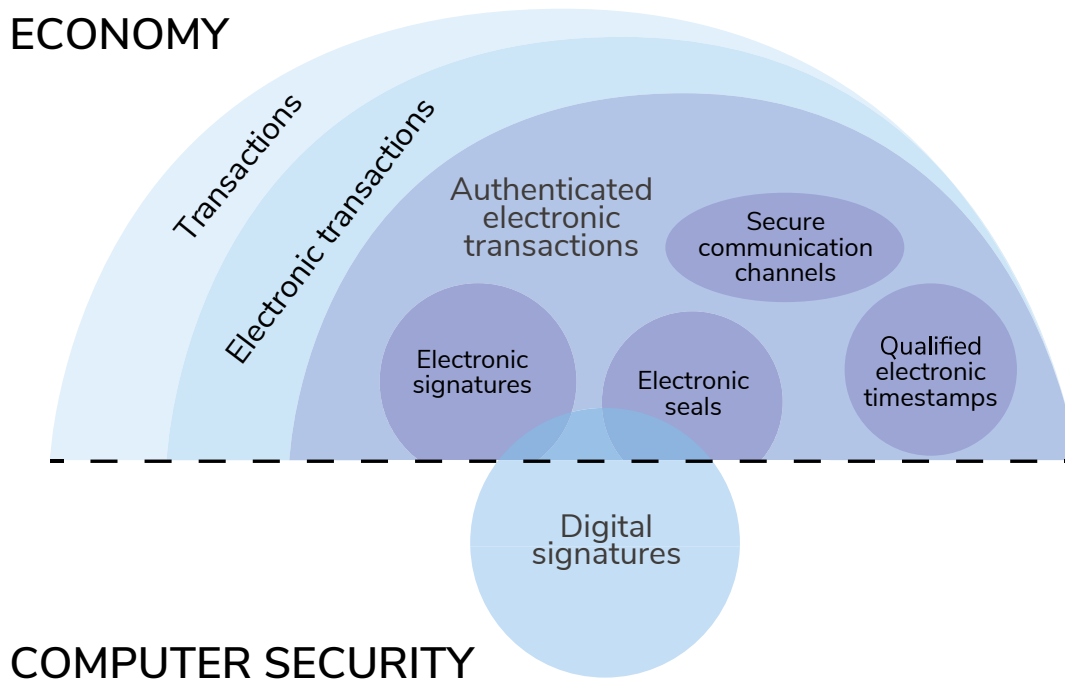
Electronic signatures are a central technique for authenticating electronic transactions because they allow to identify and capture the intent of the people involved in the transaction, as well as offer some assurance of the integrity of any documents or other data exchanged as part of the

transaction. For many electronic transactions involving individuals, an electronic signature is sufficient.

There are, however, cases where additional evidence may be required. For example, since electronic signatures are generated by individual signers, transactions that require a person to sign on behalf of a legal entity may also require an additional authentication technique, such as an electronic stamp or seal. In such cases, the combination of the electronic signature (of the representative of the legal entity), the electronic seal (of the legal entity itself), as well as other potential authentication techniques, such as the use of a secure communication channel, would be considered together when evaluating the authenticity of the transaction.

The relationship between electronic transactions, electronic signatures, digital signatures, and other authentication mechanisms such as stamps and seals is illustrated in Figure 2.

Figure 2: How electronic and digital signatures support authentication of electronic transactions



14 UNCITRAL. 2009. “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods.” Vienna: UNCITRAL.

2.4 ELECTRONIC SIGNATURE USE CASES

Electronic signatures are relevant to a variety of use cases across the economy. In general, any transaction – whether high or low value, commercial or administrative—that can be digitalized, can be an electronic signature use case. Drivers for making signatures electronic include allowing transactions to be carried out online, as well as reducing the number of digitalized processes that need to be interrupted and continued offline due to a digital trust deficit.

More specifically, there are transactions across sectors for which the absence of a trusted electronic signature is a key barrier to digitalization. Some examples are given below; a more comprehensive list can be found in Annex 2: Electronic Signature Use Cases.

General

- *Authenticating electronic transactions.* Signing a contract, issuing an official document, verifying their integrity.
- *Providing consent.* Recording user consent, e.g., to share personal data or for a medical procedure.
- *Trusted data sharing.* Sharing data and documents between entities in a way that preserves data integrity and machine readability.

Specific

- *Banking.* Opening accounts, online banking, authorizing payments.
- *Credit and insurance.* Submitting applications, signing agreements, submitting claims.
- *Health.* Consenting to procedures, issuing prescriptions, managing medical records.
- *Education.* Course registration, online exams, issuing diplomas and certificates.
- *Electronic commerce.* Ordering from suppliers, signing contracts, real estate transactions.
- *Public services.* Initiating administrative procedures, tax declarations, e-procurement, online voting.

- *Judiciary.* Submitting affidavits or declarations, signing court orders or judgements.

For many services and administrative procedures, only part of a process can be digitalized without an electronic signature, but the overall transaction cannot be completed without an in-person paper signature. The absence of suitable electronic signatures solutions for riskier transactions impedes the resilience and competitiveness of the digital economy, effectively leading to a “glass ceiling” effect, potentially limiting legal recognition and therefore putting limits on what can be safely digitalized. While the Covid-19 pandemic prompted a swift move towards remote online services for which in-person interaction was previously needed (such as notary services),¹⁵ the requirement for a handwritten signature is still prominent in many countries for sensitive transactions. The lack of trusted means for conducting digital transactions poses a significant barrier to achieving end-to-end digitalization of services and administrative processes, a pre-requisite for bringing them fully online.

In the financial sector, for example, governments worldwide are trying to improve access to and portability of financial services through financial inclusion and open banking strategies. These efforts can be hampered if electronic signature mechanisms are not in place to facilitate secure online transactions. Financial institutions may allow customers to start the process of opening a new account or applying for a loan online, but the customer may still be required to visit a branch in person to sign the necessary documents to complete the process. Electronic signatures would provide a secure and legally binding way for customers to sign the account form or loan agreement digitally without needing to visit a branch.

An important dimension that needs to be analyzed for each use case is the risk level of the transactions as well as the usability requirements. Some transactions are highly risky, for example, if they have a high monetary value or process highly sensitive data, while other transactions may be relatively low risk. For lower-risk transactions—where the premium is on promoting transaction volumes and accessibility while lowering costs—the most sophisticated electronic-signature trust measures may not be appropriate as they might be too expensive or too cumbersome to use. These high-security measures should be reserved for higher-risk transactions where the trust benefits outweigh the cost.

15 See for instance: “e-Signatures and remote notarization in the time of COVID-19,” Jones Day, March 2020 accessible at: <https://www.jonesday.com/en/insights/2020/03/esignatures-and-remote-notarization>

Consider the following three illustrative examples:

- **Low risk: P2P Payments.** A person-to-person (P2P) remittance payment made using mobile money, generally done in small monetary amounts, is a relatively low risk transaction. This is reflected by the very simple mechanisms used to process payment orders, which can be signed using a four-digit personal identification number (PIN) code. This technology choice may be appropriate given the typically low transaction amounts as well as the low digital skills of the target population, which include low-income and illiterate populations, and accompanying need to actively promote service adoption through service design.
- **Medium risk: MSME Payroll.** A micro, small- or medium-sized enterprise (MSME) may wish to process payroll digitally into employee accounts using electronic bank transfers without having to go to a bank branch to sign a payment order. Since such transfers may be of higher value and subject to more disputes than P2P payments, which are often sent within trusted networks, additional

security features—over the mobile money case - may be justified to ensure trust.

- **High risk: Government Procurement.** Digitalizing government procurement systems is crucial to enhance efficiency, increase transparency, reduce corruption, and facilitate access to government contracts for a wider range of suppliers.¹⁶ However, procurement digitalization can also heighten the risk of fraud and manipulation of procurement processes if robust security measures to safeguard the integrity of the procurement process are not in place. The high value of many government procurement contracts gives fraudulent actors a high incentive to try to break the system. Relatively low transaction volumes combined with the relatively high digital skills of the target population (bidders on government contracts) puts less of a premium on usability.

These three indicative use cases, and the risk-based methodology used to analyze them, are illustrated in Table 2, in addition to a real estate use case.

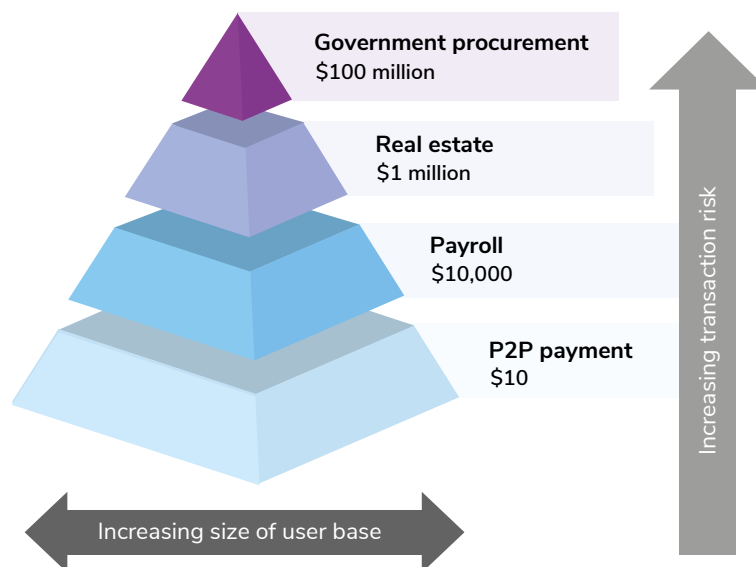
Table 2: Risk-based approach to analyzing electronic signature use cases

Use case	Transaction value (indicative)	Transaction risk level	Usability requirement	Signature Assurance Level	Signing method (indicative)
P2P payment ¹⁷	\$10	Low	High	Low	User enters PIN code using standard mobile money interface.
MSME payroll	\$10,000	Medium	Medium	Medium	Mobile banking app used. User may authenticate with a biometric; other security features may be employed.
Real estate	\$1,000,000	High	Medium to Low	High	High-trust electronic signature generated using a digital certificate issued by a trusted party in conformity with applicable standards.
Government procurement	\$100,000,000	Very High	Low	High	

¹⁶ Electronic government procurement can also help open government contracts to international competition by eliminating the need to submit physical bidding documents, which can be costly, time-consuming, and may disincentivize bidding.

¹⁷ The amount of individual person-to-person (P2P) transactions can vary widely. The amount represented here should be taken as indicative, for comparison purposes only, as it is based on general trends observed in Global Findex surveys for typical P2P transfers made using mobile money or other digital financial services in emerging markets. Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar. 2022. *The Global Findex Database 2021*:

Figure 3: Use cases of electronic signatures



A list of additional potential use cases of electronic signatures, broken down by risk level, can be found in Annex 2: Electronic Signature Use Cases.

2.5 COMMON MYTHS

A number of common myths about electronic signatures can lead to the design of sub-optimal electronic signature frameworks. This section examines and dispels six common myths regarding electronic signature application and implementation, motivating a more detailed discussion later in the paper, which will further substantiate this analysis.

Myth #1: Electronic signatures require a PKI for implementation.

In certain cases, it's assumed that electronic signature implementation must be centered around PKI technology. Although the cryptographic technologies underlying PKI do offer some of the most secure techniques for verifying the integrity of signed documents and preventing the subsequent repudiation of electronic signatures, it is

important to recognize that the PKI itself gives no assurance of one of the most crucial components of the signature: the signer's identity.

For many common use cases, the identity functions of a signature—knowing who signed or confirming that someone intended to sign—may be more important than the sophisticated assurance of integrity and non-repudiation offered by a PKI-based signature. For this reason, the many electronic signatures for low- to medium-risk transactions are designed around the identity component rather than a PKI.

For example, many financial-sector transactions allow a wire or P2P transfer to be initiated based on the authentication of the identity of a user using a feature phone interface or a bank or payment provider's mobile application—using a PIN code or biometric, for instance.¹⁸ In such cases, the electronic signature authorizing these transactions is implemented based on digital ID authentication technology without any PKI-based digital certificate or other cryptographic methods. Introducing sophisticated functionality to such simple transactions would be counterproductive, as doing so could pose a barrier to the increasing adoption of digital money transfers without adding meaningful additional security to

Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. <https://doi.org/10.1596/978-1-4648-1897-4>

¹⁸ In this particular use case, both the authentication of the user's identity and the electronic signature of the transfer order are implemented using the same technological means. This is possible when assurance of the identity function of an electronic signature is determined to be sufficient to the risk level of the use case.

these generally low-value transactions. Cryptographic technologies such as PKI can be reserved for higher-risk use cases where it is necessary to be able to verify the integrity of the precise text of the wire transfer order, or its

Myth #2: A digital signature is just a specific, highly secure type of electronic signature.

precise timestamp, in order to ensure trust in the transaction.

The term “digital signature” usually refers exclusively to signatures based on digital certificates issued and managed by a PKI. Such PKI-based digital signatures can be—and are—used to create legally valid signatures to support electronic transactions. Digital signatures have the potential to provide very high levels of trust when they are used as a technology to implement electronic signatures.

However, digital signatures are also used in a variety of other applications outside the digital economy where legal equivalence to handwritten signatures is not the goal. The most common of these transactions is securing everyday electronic communications, such as internet browsing and email. Indeed, modern web browsers require PKI-based signatures to be verified for every website a user visits.¹⁹ The type of PKI required to support such secure electronic communications is significantly less complex to implement than the type of PKI that would support high-trust electronic signatures implemented at country scale. These technical use cases for digital signatures are not electronic signatures, since the legal dimension is lacking. While such purely technology-focused implementations of digital signatures may provide a high level of assurance of data integrity, without being coupled with additional non-technology measures, they would not offer assurance of the identity of a signer, which is a key requirement of electronic signatures

Myth #3: The highest-security electronic signature available is always preferred.

and most electronic transactions. Designers of national-level electronic signature frameworks should avoid the temptation to prioritize security above

all else—especially if additional levels of security would degrade usability, accessibility, cost-efficiency, or adoption. The most ideal way to provide an adequate balance of security is through a multi-tiered trust framework based on a risk-based approach that creates space for different types of electronic signature solutions for different needs, according to specific use cases. Standardizing levels of assurance in an outcome-based way can facilitate transparency and trust in

Myth #4: Low- and medium-assurance electronic signatures are not legally valid.

such a variegated electronic signature framework. While low-trust electronic signature may not benefit from a presumption of reliability in court, it still can be legally valid as functionally equivalent to a handwritten signature. The nuance is that courts have the final authority to determine the validity and legal effect of lower-trust electronic signatures. While laws and regulations provide general guidance, courts interpret and apply these laws based on the specific circumstances of each case. Factors such as the intent of the parties and the reliability of the signature process are considered. Observed jurisprudential trends in both civil and common law systems highlight a liberal approach in which courts have recognized even the simplest forms of electronic signatures (such as a name typed at the bottom

Myth #5: Electronic signatures are not relevant to lower-income countries.

of an e-mail) as legally valid for many common transactions.

When a mobile money account user in a low-income country makes a transfer and enters his or her PIN code to authorize the transaction, this simple gesture is an electronic signature. Despite any shortcomings from a functional or security perspective, such simple electronic signature technologies have been largely successful because they are fit-for-purpose for the types of transactions for which they are used in terms of risk-appropriateness, usability, and adoption. Such pragmatic and innovative solutions to securing transactions are continuously emerging as the digital economy develops. Further digital transformation

¹⁹ It is incorrect to assume that it would be straightforward to implement PKI-based digital signatures in the digital economy simply because they are mainstream for internet transactions. The way that digital signatures are implemented on the internet does not require individual users to generate electronic signatures (this burden falls on the website publishers). For individuals and businesses, this method removes many adoption barriers to PKI-based digital signatures, particularly constraints related to registration/identification and usability/adoption.

will require additional innovations to extend the reach and relevance of electronic signatures to enable additional electronic transactions. Demand for additional use cases will increase as the volume of digital transactions continues to grow. Consenting to having personal data shared with third parties, signing loan and microcredit agreements, and using digital health services all require a way to reliably record a user's intent to make a transaction. Services that would use this functionality cannot be digitalized without a reliable method to record intent, as they could not be deployed securely and with trust. Therefore, innovations in this area should be embraced and competition that includes the private sector should be encouraged to yield a new generation of ever more usable and secure electronic signature technologies in less-developed countries. Building a trust framework that creates space for new innovative solutions, while simultaneously extending trust in existing solutions, is a goal relevant to countries of all income levels.

One key reason for this myth's persistence may lie in the confusion between electronic and digital signatures. Specifically, the misled assumption that electronic signature implementation requires the operationalization of a national level PKI (see Myth #1), or that public provision or monopoly on PKI is required (see Myth #6), may make electronic signature implementation seem unnecessarily daunting. At the national level, good reasons not to prioritize implementation of PKI-based electronic signatures include: (a) high cost and complexity of implementation; (b) low relevance of high trust level, especially if priority use cases are lower risk; and (c) prioritization of adoption and transaction volumes and accompanying concerns about usability and accessibility. In such cases, governments can consider phased approaches,

implementing lower-assurance electronic signatures first to begin harnessing their benefits while PKI implementation issues are sorted out.

Myth #6: To implement national PKI, government must build and operate the infrastructure.

To implement high-trust electronic signatures, there needs to be a legally recognized way for signatories to obtain digital certificates and relying parties to verify the signatures created using them—in other words, a PKI. Operationalizing a PKI on a national scale system is a complex undertaking, usually requiring the intervention of multiple actors in complementary roles—for certification, registration, etc.

There is no one best practice institutional or architectural model for PKI implementation. While vertically integrated models are possible, where one public sector entity performs all the PKI's functions, it is more common for a PKI to be implemented in a partnership of multiple actors in the public or private sector, or a combination of the two. There are strengths and weaknesses to each model, and the most appropriate model for a country to choose depends on a variety of contextual factors, including institutional capacity, private sector market maturity, and financial and budgetary considerations, among other concerns.

For a more complete discussion on this topic and more concrete guidance on how to choose the best implementation model for a national PKI, the reader is referred to the companion note to this document.²⁰

20 Christopher Tullis and David Black. 2024. *Public Key Infrastructure: Implementing High-Trust Electronic Signatures*. Washington D.C: World Bank.



3 TRUSTED (ELECTRONIC) TRANSACTIONS

3.1 WHAT IS A SIGNATURE ANYWAY?

"If you say to the most illiterate person 'Sign this paper,' if he cannot write, he will put a cross to it, and if he do not know how to do this the most experienced man of business cannot tell him to do more."²¹

Although signatures have been used for centuries to provide trust in commercial and administrative transactions, the term "signature" has no strict formal definition. Definitions can vary between contexts and jurisdictions,²² stemming from the fact that a signature may be many things and can take many forms.²³ A signature is, ultimately, whatever mark or sign that allows transacting individuals to trust a written transaction.²⁴ This reasoning has prompted scholars (and courts) to shy away from defining signatures in terms of the form they take and focus rather on the functions they fulfill.

This "functional" approach to the definition of a signature is important to understand how the concept can be best adapted for use in the digital world.²⁵ This note considers

signatures - whether electronic or handwritten - in terms of a set of distinct but overlapping functionalities that help ensure trust in transactions of various types.²⁶ Specifically, when attached to some data or a document,²⁷ signatures provide evidence of one or more of the following:

1. **Identification.** The real-world *identity* of the signer should be known.
2. **Attribution.** It should be possible to *reliably link* the signature to the signer, demonstrating their personal involvement in signing.
3. **Endorsement.** A signer signals an *intent* to be bound by the contents of the signed data or document.
4. **Integrity.** It should not be possible to *alter* the contents of the signed data or document after it has been signed.

Not all types of signatures perform each of the above functions equally well. For example, traditional handwritten signatures can be said to fulfill the first three functions, as a handwritten name both identifies the signer and attributes the signature to him/her (with some degree of confidence),

21 Opinion from the 1855 South African case *Van Vuuren v. Van Vuuren*, cited by S. Mason in *Electronic Signatures in Law*, Chapter 1, p.3, published by University of London Press; Institute of Advanced Legal Studies, available at: <http://www.jstor.com/stable/j.ctv5137w8.7>

22 Different sources and jurisdictions use terms such as "signature," "verification," "authentication," as well as related and/or complementary terms such as "seals," "legalization," "apostille," among others, in similar and sometimes overlapping ways. Readers interested in a discussion of these terminological nuances are referred to UNCITRAL. 2009. "Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods." Vienna: UNCITRAL

23 Common dictionary definitions include "a special mark of a person written with his or her own hand as an authentication of some document or writing" or "a sign or mark impressed upon anything; a stamp; a mark; the name of a person written by himself either in full or by initials." Oxford English Dictionary, accessed in 2023, available at: <https://www.oed.com/view/Entry/179546?rskey=ixiPb1&result=1&isAdvanced=false#eid>. Jowitt's Dictionary of English Law (4th edn., London: Sweet & Maxwell, 2015).

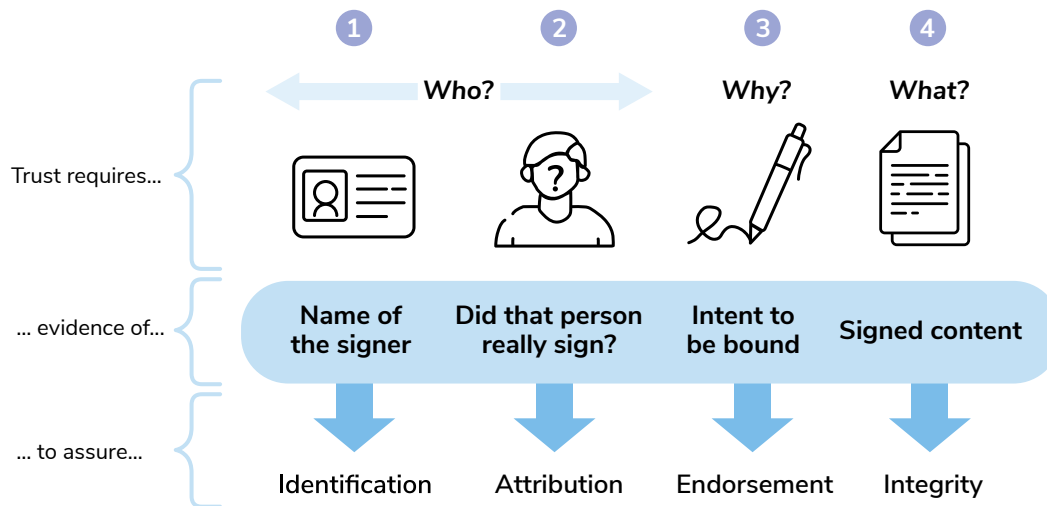
24 A signature can be affixed to any type of writing, document, data, or message of which the authenticity might be called into question.

25 This "functional equivalent approach," established in 1996 by the UNCITRAL "Model Law on Electronic Commerce," is based on an analysis of the functions of the various requirements for authenticating paper-based documents in order to determine how those same functions could be fulfilled in the digital world.

26 In the UK, courts have, for example, held that the many non-electronic forms amount to valid signatures. And including "a description of the signatory if sufficiently unambiguous, such as 'Your loving mother' or 'Servant to Mr Sperlring' - Law Commission. 2022. *Electronic Execution of Documents*. Industry Working Group Interim Report.

27 The notion of a "document" used in this note is broad and covers not only documents in the traditional sense, but also other types of writings, information, instructions, data, messages, and records destined for transmission, or of which the source or authenticity might be called into question. In principle, any piece of data can be signed. This note generally refers to all of the above as "documents" for convenience.

Figure 4: How signatures increase trust in transactions



Source: Authors' elaboration

as well as signals the signer's intent to endorse the signed document. Traditionally, handwritten signatures are defined²⁸ primarily in terms of these three main functions: identity, attribution, and endorsement (or intent to be bound).²⁹ Fulfilling the integrity function and providing strong assurance of attribution, however, requires additional measures beyond simply writing a name.

In cases where signatures provide a high level of assurance of attribution, this function is sometimes referred to as "non-repudiation" to indicate that the assurance of attribution is strong enough to make it very difficult for the signer to subsequently repudiate their signature. The need for non-repudiation is why signers of paper documents are typically required to do additional things such as use an ink pen, include the date, and sign two copies of the document, among other authentication measures.³⁰ Ensuring integrity requires even more measures still, such as notarization, for example.³¹

The similarities between electronic signatures and digital identity are worth highlighting. Indeed, the first three

functions of electronic signatures (identity, attribution, and endorsement) directly relate to the signer, establishing their identity and intentions. Unsurprisingly, the means used in electronic signature solutions to assure these functions may be the same as the means applied by digital identity systems for identification and authentication assurance.³² Likewise, since the last function (integrity) relates to the document to be signed and not the signer, assurance of this function does not overlap with digital identity.

Many simple electronic signature implementations limit themselves to assuring the identity-related dimensions of a signature; such solutions may be technically identical to digital identity or authentication implementations. A basic requirement for any signature involves some basic ability to authenticate the identity of the signer, thus, the simplest electronic signature implementations usually focus on this aspect. One example is the case of mobile money, discussed above, where a PIN code (authentication factor) is relied on to initiate and authorize a payment and make it difficult for the user to subsequently repudiate the transaction.

28 UNCITRAL. 1996. *Model Law on Electronic Commerce*. Vienna: UNCITRAL. UNCITRAL. 2001. *Model Law on Electronic Signatures*. Vienna: UNCITRAL.

29 Additional measures beyond the signature itself may be required in some contexts to authenticate a transaction by providing additional assurance of the intent to be bound. For example, in some francophone jurisdictions it is common to require the signer to handwrite the phrase "lu et approuvé," meaning "read and approved," prior to signing.

30 The ink pen prevents erasure of the signature; the date prevents time-based repudiation; while the additional copy allows the other party to produce evidence of the signature if the signer attempts to disavow it.

31 In addition to notarization, in some jurisdictions it is common practice to initial each page of a multi-page document to assure integrity by preventing later tampering. Imprinting each page with a raised seal can serve a similar purpose.

32 Identification and authentication assurance are discussed and defined in various standards for digital identity, such as the US National Institute for Standards and Technology (NIST) special publication 800-63 providing Digital Identity Guidelines. <https://doi.org/10.6028/NIST.SP.800-63-3>

However, as electronic signatures are extended to higher-risk use cases and potentially exposed to more sophisticated attackers, stronger identity or authentication assurance may be required. This may lead to the use of multifactor authentication, or to a decision to rely on trusted digital ID credentials outside of the electronic signature software solution. High-risk use cases also make assurance of the function of integrity increasingly important. In such implementations, electronic signature solutions diverge from digital identity and integrate other complementary assurance measures, such as implementation using a cryptographically-based digital signature.

For use cases where strong assurance of integrity is not required, a digital ID system alone could be leveraged to provide the authentication functionality required to implement an electronic signature. The legal value of such an implementation would then depend on the legal and trust frameworks in that jurisdiction.

3.2 SOURCES OF TRUST

Although trust lies at the foundation of commercial and administrative transactions, in most cases, the handwritten signatures used to authenticate these transactions are quite insecure. For a handwritten signature to function securely, the persons relying on the signature should ideally have access to both the names of the persons authorized to sign as well as specimen signatures for comparison—both of which are rarely available. Even when specimens are available, expertise is required to detect forgery. Moreover, such expertise may only be available in rare cases when a signature’s authenticity is challenged in court.

Despite these deficiencies, the analog economy has functioned effectively for centuries relying upon handwritten signatures to establish trust. Indeed, the use of additional authentication measures that could improve transaction security (such as stamps, seals, attestation, and notarization) are quite rare in practice, as are legal challenges to signatures’ authenticity. It is also worth noting that handwritten signatures have functioned to support these transactions without any particularly designed legislative trust framework.³³ Prior to the emergence of digital media, law on signature was focused on questions related to the identity of the signer.³⁴

One reason why handwritten signatures are able to keep the analog economy functioning so smoothly, particularly for everyday transactions, is because of existing sources of trust between the transacting parties that can serve to supplement and reinforce the technical trust offered by the signature itself. Depending on the transaction, technical trust may be supplemented by existing sources of trust in cases where parties:

- Know each other or otherwise have a pre-existing trust relationship;
- Have transacted with each other successfully over a period of time;
- Have a pre-existing contractual relationship, such as a service provider and its client;
- Belong to the same group, such as a professional body or trade association.
- Transact in person, on closed systems, through other trusted communication channels.³⁵

When moving from paper to electronic transactions, the aim should be to use technology to supplement and extend existing sources of trust, not to replace existing sources of trust with technologically-derived sources of trust on the grounds that they are superior.

Importantly, governments should take these considerations into account when regulating electronic signatures to avoid requirements of excessive technological sophistication that may have a chilling effect on electronic transactions. Just as it is important to supplement and extend the sources of trust underpinning paper transactions to ensure trust in the digital world, it is also equally important not to assume the deterioration of such pre-existing trust relationships. Efforts to overly formalize electronic trust or make it excessively reliant on technology-based sources of trust could “crowd out” pre-existing non-technology sources of trust. Efforts to arrogate the notion of trust to a purely technology realm could lead to overly technological sophistication of electronic transactions, which adds a barrier to the continuity of currently well-functioning commercial relationships and administrative transactions.

33 UNCITRAL. 2009. “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods.” Vienna: UNCITRAL.

34 Historically, law on paper signatures was primarily concerned with a signature’s reliability in terms of (a) identifying the signer; (b) attributing the signature to the signer; and (c) demonstrating the signer’s intent to be bound by the terms of the document.

35 UNCITRAL. 2009. “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods.” Vienna: UNCITRAL.



4 TRUST FRAMEWORK

4.1 THE ROLE OF A TRUST FRAMEWORK

If the vast majority of electronic transactions can be carried out without issue, free of any particular regulatory attention, then what is the role of an electronic signature trust framework?

A trust framework for electronic signatures is a set of requirements and standards that governs their use, recognition, and interoperability. It establishes the roles and responsibilities of parties involved, including the issuers of electronic signatures, users, and relying parties. This framework often includes standards for identity proofing, authentication, consent, and the use of technologies, among other elements. It outlines the processes and security requirements necessary for ensuring that electronic signatures are trustworthy and reliable. Trust frameworks extend trust by providing standardization, rigor, and transparency around the elements that determine the reliability of electronic signatures. Trust frameworks may be comprehensive from the outset, or they may be organic outgrowths or progressive formalizations of existing implicit or de facto relationships. Trust frameworks include requirements related to:

- **People**, such as a requirement to link a signature to the identity of a real person;
- **Process**, such as minimum standards for the identity checks carried out by the signature provider when onboarding a signer;
- **Technology**, such as technical measures to protect the integrity of the signed document.

The role of a trust framework is not to provide all the elements of trust or to assume that parties don't trust each other. Trust frameworks for electronic signatures should not be overengineered in an effort to supplant contextual trust with technologically-derived trust on the basis that the latter is assumed to be superior. Instead, the emphasis should be

on the substance and adequateness of the trust framework, and not its legal form or (initial) comprehensiveness. Regulators should see their role as extending existing sources of trust—through standards and transparency - to scale the digital economy beyond what can be based on existing trust relationships. This extension could include scaling to new sectors, new untrusted parties, and new risk levels, where electronic transactions would not be possible without the transparency and trust supplied by regulation.

A well-designed trust framework for electronic signatures should adhere to the following principles:

1. **Ensure security of electronic transactions.** Given the inherent fungibility and velocity of electronic communications, additional measures are needed to ensure trusted online interactions.
2. **Capitalize on existing sources of trust.** Improving trust in technology should not "crowd out" existing sources of trust, including sources that are not technology-derived.
3. **Extend the frontiers of trust.** One role of a trust framework can be to extend existing sources of trust to new types of transactions. This could include extension to higher-risk use cases or to parties without pre-existing trust relationships who would not otherwise transact online.
4. **Promote usability and adoption.** Risk-based approaches can help ensure that the most sophisticated technologies are reserved for cases where the transaction risk justifies them.
5. **Promote innovation and technology neutrality.** Avoiding technology-specific requirements can allow for innovative approaches and avoid obsolescence and technology lock-in over time.
6. **Clarify roles and responsibilities.** In addition to defining the roles and responsibilities of the various actors in operationalizing the trust ecosystem, the trust framework can clarify liability, establish penalties, and provide the opportunity for redress by any party, all of which serve to build confidence in electronic transactions.

4.2 TIERED TRUST: LEVELS OF ASSURANCE

Increasingly, countries around the world are adopting a multi-tiered or hybrid approach to electronic signature regulation, where the regulation defines levels of assurance, remaining agnostic to implementation strategies or technology specifics.³⁶ Levels of assurance describe the degree of confidence in the identity of the signer and the integrity of the signed document. The higher the level of assurance, the more rigorous the requirements.

Generally, the lower trust levels are formulated with minimal requirements, if any, and contracting parties and market players are left to determine what technologies they consider adequate. At low assurance levels, courts may weigh the assurances provided by these technologies as evidence if the signature is challenged.

Higher levels of trust introduce more requirements to increase trust by providing additional assurance of identity, endorsement, integrity, and/or non-repudiation. They do this by establishing standards for the people, process, and technology elements of a signature, such as how a user's identity is verified during onboarding, or how the trust ecosystem is monitored and supervised. These requirements and their surrounding transparency provide evidence of electronic signature reliability.

A concrete example of a multi-tiered approach can be found in the European Union Electronic Identification, Authentication and Trust Services (eIDAS) regulation,³⁷ which gives an indicative illustration of how levels of assurance for electronic signatures can be structured. Although the eIDAS is regulated at the EU-level, the framework has also been emulated outside the EU³⁸ and also served as a key source of inspiration for the recent UNCITRAL model law on cross-border recognition of trust services.³⁹ However, the specifics of the eIDAS assurance framework—such as the number of assurance levels or the detailed requirements for each – are not set in stone and can vary between frameworks and jurisdictions.⁴⁰

The following table summarizes some key features of the eIDAS assurance levels.⁴¹

In summary, a trust framework performs the following functions:

- Defines **requirements** around the people, process, and technology components used to create an electronic signature and provide evidence of its reliability.
- Enables multiple levels of standards to coexist through different **levels of assurance**, allowing for multiple levels of trust to improve relevance to electronic signature use cases of varying risk levels.
- Provides **transparency** around the requirements, standards, and compliance with these measures during implementation, in turn, fostering trust in electronic signature reliability.

Taken together, these requirements and their surrounding transparency provide the foundation of trust in the people, process, and technology elements that are used to create a signature. This, in turn, provides evidence of the signature's reliability, underpinning trust in the authenticity of the signed document.

In addition to encouraging transparency, trust frameworks should also promote certainty about the allocation of liability among parties to the framework when things go wrong. The consideration of liability is an important component of risk and return attached to the business model of parties to the framework and to the operator of the trust framework. Effective trust frameworks allocate liability to those best able to bear it. As an example, credit card schemes are sector-specific trust frameworks which are very specific about how liability is allocated based on evidence that parties have followed set standards for different processes, especially authentication and authorization. In certain countries, such as the US, these frameworks must comply with specific laws which explicitly limit customer liability for unauthorized transactions; in relation, legal frameworks incentivize credit card schemes to manage these risks carefully.

36 While lower assurance levels may be fully technology neutral, higher assurance levels may introduce some technology-specific elements, in particular, elements related to public key infrastructure and digital certificates, although the implementation model is usually unspecified.

37 eIDAS regulation governs electronic signatures in the EU and was established in EU Regulation 910/2014 of 23 July 2014.

38 Georgia, Lebanon, Singapore, and Switzerland are examples of countries with electronic signature frameworks containing levels of assurance or other elements that mirror eIDAS.

39 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>

40 For example, some governance frameworks leave the low-trust (simple) assurance level implicit, while others may require accreditation of the certification authority for the medium-trust (advanced) assurance level.

41 See eIDAS Art. 24-28.

Table 3: eIDAS levels of assurance: Summary of key features

Level of Assurance	Low	Medium	High
eIDAS Terminology	Simple Electronic Signature (SES)	Advanced Electronic Signature (AdES)	Qualified Electronic Signature (QES)
Identity of the signer	No requirement	Electronic signature uniquely linked to a signatory identity	Electronic signature uniquely linked to a signatory identity
Data used for signing⁴²	No requirement	Must be under the sole control of the signer	Must be under the sole control of the signer Must conform to rigorous standards for digital certificates
Integrity of the signed document	No requirement	Signed document cannot be modifiable after signing	Signed document cannot be modifiable after signing
Registration process	No requirement	Requires some assurance of the identity of the signatory No requirement for in-person identity verification	Rigorous in-person (or equivalent) onboarding process with high assurance of linked signatory identity ⁴³
Accreditation of digital certificate issuer	No requirement	No requirement	Rigorous people, process, technology, and audit requirements
Supervision of the digital certificate issuer⁴⁴	None	Ex post supervision by the competent supervisory body	Ex ante supervision by the competent supervisory body
Device used for signing	No requirement	No requirement ⁴⁵	High-security, certified signature-creation device required ⁴⁶
Appropriate transaction risk level	Low	Medium	High
Legal validity	No presumption of validity; court makes evidence-based determination	No presumption of validity; court makes evidence-based determination	Presumed valid (functionally equivalent to handwritten signature)

Source: Authors' elaboration

42 In the eIDAS framework, "data used for signing" refers to the electronic data that is uniquely linked to and used by the signatory to create an electronic signature. In the case of a high-trust (qualified) electronic signature, this data is the cryptographic key stored in the digital certificate used by the signer to generate digital signatures. At lower trust levels, this description refers to other data and technical systems used to generate signatures and provide assurance of integrity.

43 In practice, live video interviews have been considered in some jurisdictions as equivalent to in-person.

44 In a public key infrastructure, the issuer of digital certificates, often called a certification authority, is a trusted organization responsible for issuing PKI-based digital certificates that binds them to a public key.

45 The concepts of "accreditation" and "qualification" of a certification authority or trust service provider are sometimes used interchangeably in the eIDAS context since only qualified electronic signatures require the certification authority to be accredited.

46 In practice, this secure "device" can be implemented on a user-managed physical device as well as in cloud implementation models.



5 LEGAL FRAMEWORK

5.1 THE ROLE OF THE LEGAL FRAMEWORK

If trust frameworks can offer transparency around the people, process, and technology elements needed to provide evidence of a signature's reliability, then what is the role of the legal framework?

The legal framework is the set of laws and regulations governing electronic signatures and trust services.⁴⁷ It provides the foundation for the trust framework, establishing its legal validity and enforceability and clarifying the legal implications on electronic transactions. More specifically, the legal framework helps clarify the circumstances under which electronic signatures may be: admissible as evidence in court; considered legally equivalent to handwritten signatures; and sufficiently reliable to have legal effect.⁴⁸ Fundamentally, the legal framework establishes the legal equivalence of electronic and handwritten signatures and ensures that an online transaction is just as legally valid as a paper-based one.

Functional equivalence

The legal framework for electronic signature should recognize functional equivalence⁴⁹ between electronic and paper-based signatures in terms of legal effects and evidentiary value.⁵⁰ Legal provisions may also prevent courts from discriminating against electronic signatures on the grounds that they are in electronic form,⁵¹ thus mandating courts to consider supporting evidence regardless of its electronic form to assess its reliability. Often introduced through primary legislation, these legal provisions would recognize the admissibility of electronic signatures as evidence in court.⁵² A legal framework recognizing the functional legal equivalence between electronic and paper signatures is a critical prerequisite for scaling electronic transactions.

Evidence of Reliability

Having an electronic signature deemed admissible as evidence in court is a first step towards establishing reliability, but this step alone is not sufficient for an electronic signature to be considered valid.

47 Specific examples include national laws, such as the Electronic Signatures in Global and National Commerce Act (ESIGN) in the United States, regional and supranational mutual-recognition frameworks, such as the eIDAS regulation in the European Union, as well as international conventions like the UN Model Law on Electronic Signatures.

48 Although contract law considers oral agreements as legally binding, contracts can only be signed inasmuch as they are written down. The law around signatures is historically an outgrowth of that governing writings. Signatures are a consequence of requiring a legal act to be drafted in writing, and the law on signatures was therefore always a function of the medium used for writing. It is natural then that the recent evolution of the law on signatures was prompted by the rise of new technologies and the emergence of electronic forms of communication. Indeed, it was the need to clarify the conditions under which an electronic writing would have the same legal value as paper writing that led to much of the recent effort to define what was meant by signature. For further information, see "L'écrit électronique : régime juridique," Aurélien Bamdé, accessible at: <https://aurelienbamde.com/2023/03/15/lecrit-electronique-regime-juridique/>

49 The "functional equivalent approach" is an approach first taken by the UNCITRAL Model Law on Electronic Commerce. This approach stems from the need for legislators to determine how the purposes and functions of the traditional paper-based requirements prescribed by laws in certain countries, such as to have "written," "signed" and "original" documents, could be fulfilled through electronic-commerce techniques, such as electronic signature. For more information, see Annex 4: Good Practice Legal Frameworks.

50 Functional equivalence means that an electronic signature will have the same legal effect as a paper-based signature, including its evidentiary value in courts, as it could be both (a) admitted and (b) potentially recognized as valid evidence in legal proceedings as fulfilling part, or all, of the functions that a signature normally serves (be it proof of identity, endorsement, integrity, or non-repudiation).

51 For example, this non-discrimination principle is explicitly stated in Article 25 of the eIDAS regulation: "An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures."

52 These provisions could naturally be part of statutes, codes, or common law pertaining to civil or criminal procedures and, more particularly, rules of evidence.

As discussed above, there is a broad range of types of electronic signatures which offer very divergent levels of assurance of their reliability. Some very simple electronic signatures offer little to no hard evidence of their reliability, while others employ very sophisticated technology and non-technological measures to marshal very strong evidence of the signature's reliability.

Legal frameworks for electronic signatures may set out (often through primary legislation) the requirements for reliability of electronic signature data as evidence in court.⁵³ Electronic signatures that provide high levels of assurance (i.e., evidence of a signature's reliability) would be more likely to be considered valid signatures in court and would thus have higher probative value.⁵⁴

Presumption of Reliability

Evaluating the reliability of an electronic signature is not a trivial task and may require specialist knowledge. Furthermore, if there is a risk that the evidence provided by the signature will not be found sufficiently reliable in court, then this also represents a commercial risk to the contracting parties.

For these reasons, some legal frameworks introduce a legal presumption of reliability.⁵⁵ Usually reserved for signatures meeting the requirements for the highest level of assurance,⁵⁶ this presumption of reliability requires the court to consider the signature as reliable, and therefore legally valid, until proven otherwise. Using this method to put the burden of proof on the party challenging the validity of the signature reduces the amount of evidence that must be evaluated in court and reduces the risk to the contracting parties of a contract being found null and void. For high-risk transactions, in particular, this quasi-guarantee that an electronic signature will be considered valid in court can

make the additional cost and effort of using a high-assurance electronic signature worthwhile.

Conversely, in cases where the legal requirements necessary to benefit from a presumption of reliability are not met, the burden of proof to demonstrate the signature's reliability is borne by the party claiming the legal effect of the electronic signature.

Electronic signature validity in practice

In practice, courts tend to take a flexible approach when it comes to the evidentiary value of electronic signatures, although the case may vary according to the jurisdiction. In general, courts aim to give effect to the initial intention of the parties rather than applying rigid rules to the reliability of an electronic signature. Factors like the nature of the transaction, the context, previous dealings between the parties,⁵⁷ industry practice, etc., are all considered. This flexibility is often found under common law jurisdictions, such as in the US and UK where, for example, a name typed at the bottom of an email is considered sufficient to authenticate the person and evidence their intent to be bound.⁵⁸ The approach taken by civil law jurisdictions is usually stricter, as courts usually rely on existing national legislation. Courts in France, for instance, have been reluctant to accept electronic signatures as equivalent to handwritten ones until the adoption of legislation expressly recognizing it. While case law remains rare, the observed trend, even under civil law systems, highlights a liberal approach taken by courts vis-à-vis electronic signature, recognizing their validity even under their simplest forms.⁵⁹

53 These provisions could be included, for example, in legislation pertaining to e-transactions/e-commerce or as part of any body of procedural laws and rules of evidence. For example, a requirement could be that the electronic signature must be issued through a reliable process for identification that guarantees its link with the document to which it is affixed.

54 Cornell Law School Legal Information Institute. "Probative Value." Wex, May 2022. https://www.law.cornell.edu/wex/probative_value
VanDerGinst Law. "E-Signature: Who Bears the Burden of Proof?" VanDerGinst Law, May 31, 2022. <https://www.vdblaw.com/e-signature-who-bears-the-burden-of-proof/>

55 Under certain circumstances, the admissible and valid electronic signature may benefit from a "presumption of reliability" allowing whoever is claiming it to presume, by law, that the electronic signature introduced before the court constitutes valid evidence of both (i) the identity of its author and (ii) the integrity of the document.

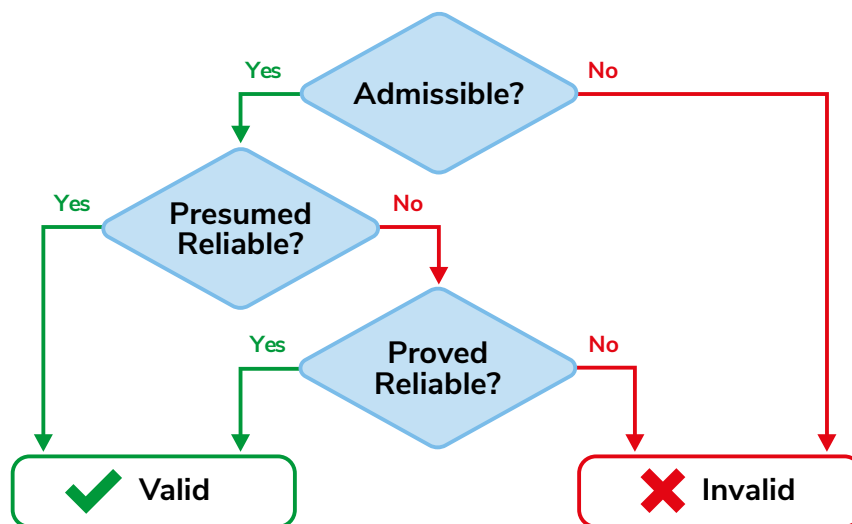
56 The primary legal framework for electronic signatures would often address the procedural aspects of functional equivalence by specifying that there are specific cases in which an electronic signature would be presumed to have satisfied the reliability requirement, i.e.: the electronic signature (i) relies on a reliable process for (ii) identification that (iii) guarantees its link with the writing to which it is attached.

57 For example, if the parties have been regularly using emails to communicate during negotiations.

58 A fundamental issue with respect to electronic signatures is the connection between the mental state of the person who may wish to be bound by the electronic signature and the document to which it is attached.

59 In a 2016 decision, for example, the Cour de Cassation (the highest court in France for civil law matters) acknowledged that the admissibility of electronic evidence of a written and signed document does not require a high-trust electronic signature, therefore, the judge must independently determine whether the process is reliable.

Figure 5: Functional equivalence of electronic signatures



Source: Authors' elaboration

Summary

While electronic signature legislation differs according to the relevant jurisdiction, the following three main approaches to legislating electronic signatures apply broadly:

- Prescriptive (or technology-specific) approach:** A prescriptive legislation that adopts a specific technology, such as digital signatures, as the method to replace a handwritten signature in the digital environment. This approach solely recognizes digital signatures (i.e., high-trust signatures based on a particular technology, such as PKI, that ensures its reliability) as acceptable electronic signatures while excluding other forms.⁶⁰ Although this approach prioritizes security, it risks limiting economic development by over-regulating e-commerce and relying on a specific technology which may evolve over time. Adoption of electronic signatures may be limited if high-cost or low-usability technologies are imposed for low-risk transactions, with an accompanying reduction in transaction volumes.
- Minimalist (or technology-neutral) approach:** This is the approach taken from the UNCITRAL Model law on e-commerce.⁶¹ Under this view, laws should aim to be technologically neutral in determining what constitutes an electronic signature. Countries such as Australia, for example, focus on addressing the legal effect of electronic signatures while letting the market determine non-legal aspects, such as security and reliability levels. This approach aims to give flexibility and autonomy to market participants in shaping those aspects without imposing rigid legal requirements.
- Multi-tiered (or hybrid) approach:** Under this approach, electronic signature is categorized under two or three tiers or levels of assurance, which usually range from simple or low-trust electronic signatures to higher-trust electronic signatures, sometimes referred to as “advanced” or “qualified” according to jurisdiction.⁶² Such is the approach taken by the eIDAS regulation, which is directly applicable to EU member states. It is also the approach of many countries outside the EU, such as Brazil⁶³ or

⁶⁰ Some laws, like the Indian Information Technology Act 2000, initially focused only on digital signatures but have since been amended to adopt a two-tier approach, allowing for other forms of electronic signatures. The Electronic Transactions Act 2007 of Saint Vincent and the Grenadines follows a prescriptive approach but allows parties to agree on other methods of electronic signature, with digital signatures being the only form with legal force in the absence of a specific agreement. In Malaysia, the Digital Signature Act 1997 explicitly identifies digital signatures as the equivalent of a manuscript signature in Section 62.

⁶¹ Article 7 addresses the legal recognition and validity of electronic signatures, stating that an electronic signature should not be denied legal effect solely on the grounds that it is in electronic form or does not meet the requirements for a traditional handwritten signature. It establishes a technology-neutral approach, allowing for the use of various methods to identify the person and indicate their approval of the information communicated.

⁶² Terminology varies between jurisdictions for the highest trust level, including “qualified” (EU, Japan), “advanced” (South Africa), “certified” (Switzerland), “authenticated” (South Korea), and “secure” (Canada). For further information on levels of assurance, please refer to the above section on “tiered trust.”

⁶³ Under Law No. 14.063/2020

Singapore, which recognize two levels of electronic signature assurance, with the high-trust or “secure” level providing an additional level of security and integrity.⁶⁴ While legal frameworks that adopt the multi-tiered approach usually describe lower levels of assurance in a technology-neutral manner, provisions related to higher level electronic signatures tend to require more specific standards that may be technology-specific.⁶⁵

Alternatives to challenging signatures in courts

As digital commerce has boomed, so too has the volume and complexity of disputes related to electronic transactions. These include disputes related to validating and enforcing a transaction concluded by a form of electronic signature.⁶⁶ The relatively small value of many electronic commercial transactions combined with their sheer volume means that the formal legal system is not always well positioned to address these issues, whose fair and speedy resolution is essential to building trust in the digital economy. One consequence of this is that court challenges to electronic signature reliability are relatively rare and, due to the cost involved, may generally be limited to higher value transactions that justify the cost of litigation.

Hence, Online Dispute Resolution (ODR) was created to offer an accessible, expedient method for those seeking to dispute a transaction based on the validity of an electronic signature. ODR started in the 1990s by applying existing Alternative Dispute Resolution (i.e., extrajudicial) approaches to an online environment. However, ODR had to be optimized for an entirely remote setting due to the massive volume of rich data, which warranted automatable decision making. The e-commerce platform, eBay, is recognized as an early pioneer in this area. Now, however, the application of ODR within trust systems (like online platforms) is pervasive and is even changing the functioning of court systems.⁶⁷

5.2 MUTUAL RECOGNITION

As previously mentioned, one of the most important aspects of having a legal framework for electronic signature is providing legal certainty that an electronic signature will be enforceable and recognized in court as valid evidence—meaning that an electronic signature is granted full legal equivalence to a handwritten signature on paper. As more countries move to digitization, such legal certainty is increasingly needed across borders. Hence, establishing cross-border mutual recognition frameworks for high trust electronic signatures helps create clarity on the legal effects and admissibility of these electronic signatures which, in turn, fosters trust and confidence in electronic transactions.

The EU eIDAS regulation represents the first successful attempt to establish a harmonized multilateral trust framework for electronic signatures across borders. eIDAS sets out mutual recognition as a general principle for qualified signatures stating that qualified electronic signatures and qualified certificates issued in one member state shall be recognized as qualified in all other member states.⁶⁸ By stating this principle, eIDAS ensures that the legal effects and admissibility of qualified electronic signatures are not denied solely because they were created in a different member state. Mutual recognition can reduce administrative burdens as well as barriers to cross-border electronic commerce and service delivery, enabling businesses and individuals to engage in digital transactions more efficiently.

While a country may expressly recognize in its law the legal effect of electronic signatures issued across borders (e.g., in specific countries), mutual recognition of electronic signatures can be facilitated if the national law provides for mutual recognition of electronic signatures or other trust services offered by trust service providers⁶⁹ established in third countries. Under eIDAS,

⁶⁴ See Singapore’s Electronic Transactions Act, Cap 88 (ETA) and the Electronic Transactions (Certification Authority) Regulations 2010.

⁶⁵ For example, Recitals of eIDAS regulation provides that requirements for assurance levels should be technology neutral. Yet, Article 29 of eIDAS establishes requirements for qualified signatures which reflect, indirectly, PKI. The reference to PKI was also previously included in the European Parliament’s resolution of 21 September 2010 on completing the internal market for e-commerce.

⁶⁶ Many of these disputes also relate to issues outside the scope of this paper, such as whether a good purchased online was delivered at all or in the condition advertised.

⁶⁷ See Chapter 3 of Katsch, Ethan, and Orna Rabinovich-Einy. 2017. *Digital Justice: Technology and the Internet of Disputes*. Oxford: Oxford University Press.

⁶⁸ See Article 25 (3)

⁶⁹ For more information about trust service providers and how they support the implementation of PKI, the reader is invited to consult the companion note, “Public Key Infrastructure: Implementing High-Trust Electronic Signatures.”

a special status is given to certain trust service providers recognizing them as a Qualified Trust Service Providers (QTSPs) based on compliance with specific requirements for the trust service (such as electronic signature) it intends to provide. To qualify, the entity submits an application to the designated supervisory body, which evaluates its compliance through assessments and audits. If the entity meets the requirements, it is granted the status of a QTSP. The supervisory body publishes the list of QTSPs, enabling their services to be trusted and recognized across the EU and, in some cases, beyond.

Outside the EU, each country or jurisdiction may have its own laws, regulations, and frameworks related to trust services and electronic transactions. In some cases, countries may have established bilateral or multilateral agreements with other countries to facilitate mutual recognition of trust services. These agreements outline the terms and conditions for recognizing and accepting trust services provided by entities from different jurisdictions.

Additionally, international standards and best practices developed by organizations, such as the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), can provide guidance and promote harmonization in the field of trust

services. Countries may choose to align their national frameworks with these international standards to enhance mutual recognition. Recently, in 2022, the UNCITRAL *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*⁷⁰ has provided a normative international model law for cross-border mutual recognition of electronic signatures. Heavily inspired by eIDAS, this new model law builds on previous UNCITRAL model laws on electronic commerce and electronic signatures to extend trust across borders.

Aside from mutual recognition of electronic signature and trust services more broadly, the principle is also relevant for identification (ID) frameworks that countries adopt. While recognition of an ID framework may not directly impact recognition of the electronic signature issued by a third country, in some cases, a recognized digital ID credential issued by one jurisdiction could be used as a means of authentication or identification in the context of electronic signature processes. When ID frameworks are mutually recognized, it becomes easier for individuals and organizations to use their trusted identities to sign documents across various platforms and systems. This mutual recognition, combined with cross-border interoperability, fosters seamless electronic transactions, and promotes the wider adoption of electronic signature technology.

70 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>



6 TECHNICAL IMPLEMENTATION

6.1 A VARIETY OF POSSIBLE TECHNOLOGIES

As noted above, an electronic signature is, fundamentally, any data in electronic form, associated with other data, used by a signatory to sign. The following discussion gives some examples of a few common ways that low- and medium-trust electronic signatures can be implemented in practice. The list is not exhaustive. High-trust electronic signatures are discussed in the following section in the context of public key cryptography.

Low assurance. Simple, or low-assurance, electronic signatures could fulfill this function without necessarily needing any technology specific to electronic signing. Some concrete examples of how simple electronic signatures might be implemented could include:

- Typing a name at the end of an email or document;
- Clicking on an “I accept” button on a website;
- Using a scanned image of a handwritten signature;
- Using a finger or stylus to hand write a signature on screen;
- Digital authentication (for example, a biometric or a one-time password).

Medium and high assurance. As noted in the above discussion on level of assurance, the medium and high assurance levels require imposing some additional requirements in terms of identity, endorsement, integrity, and non-repudiation. There are various form factors on which these requirements might be implemented, such as:

- Plug-ins to PDF reader applications that allow digital-certificate-based electronic signing;
- Cloud-based signature solutions offering a secure remote signing service;
- A mobile app using secure elements in smartphones to generate signatures;
- A hardware token, such as a smart card containing a digital certificate on a chip.

These form factors do not, however, tell the entire story. Each form factor can be implemented as a medium- or high-trust signature depending on the various complementary people, process, and technology elements supporting them. Table 4 gives one example of how an advanced electronic signature (in the eIDAS framework) could be implemented using any of the above form factors.

In order for the same electronic signature solution to be considered qualified under eIDAS (instead of advanced) it would have to add additional complementary features, such as those provided in Table 5.

Table 4: Examples of advanced electronic signature implementation

Trust factor	eIDAS Requirement (AdES)	Implementation example
Identity of the signer	<i>Electronic signature uniquely linked to a signatory identity</i>	An ID document is verified during in-person or remote onboarding.
Data used for signing	<i>Must be under the sole control of the signer</i>	Digital authentication using a biometric or other authentication factor required for each signing transaction. ⁷¹
Integrity of the signed document	<i>Signed document cannot be modifiable after signing</i>	A digital certificate-based signing solution is used to ensure integrity of the document. ⁷²
Registration process	<i>Requires some assurance of the identity of the signatory</i>	An ID document is verified during in-person onboarding.

Table 5: Examples of qualified electronic signature implementation

Trust factor	eIDAS Requirement (QES)	Implementation example
Accreditation of digital certificate issuer	<i>Rigorous people, process, technology, and audit requirements</i>	The signature solution vendor is accredited as a QTSP by the competent Supervisory Body before issuing the digital certificates used in its products.
Device used for signing	<i>High-security, certified signature-creation device required⁷³</i>	The digital certificate used to generate the signature is stored securely in a specialized device meeting additional security requirements. ⁷⁴

6.2 THE ROLE OF PUBLIC KEY CRYPTOGRAPHY

Cryptography is the branch of applied mathematics concerned with converting messages into an apparently unintelligible form using a set of mathematical formulas and then restoring them to their original state. Public key cryptography, which is the basis for digital signatures, involves generating two unique keys using algorithmic functions that are mathematically related. One key is used to

transform a document into an unreadable format and create a digital signature, while the other key is used to verify the signature and confirm that the document has not been altered from its original form.

For high-risk transactions, cryptographic technologies can be deployed for electronic signatures to assure a high level of trust. In particular, cryptography can provide the highest available assurance of integrity and non-repudiation.⁷⁵

71 Biometric authentication refers to the automated recognition of individuals based on their biological and behavioral characteristics. For more, see Digital Identity Guidelines. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

72 Common products on the market integrating such technology include DocuSign and Adobe Sign, among many others.

73 In practice, this secure “device” can be implemented on a user-managed physical device as well as in cloud implementation models.

74 Both physical devices managed by the user and cloud-based implementation are possible.

75 Non-repudiation is only assured at the highest level of trust when, in addition to the digital certificate, the date of the signature is also assured by an accredited timestamp authority, a variety of trust service provider.

It should be noted, however, that cryptography does not provide any assurance of the identity of the signatory, or of their endorsement of a document. This is because a pair of cryptographic keys—which are a simple pair of numbers—have no inherent association with any person or entity. Additional measures are needed to link cryptography-based electronic signatures with a signatory. These measures include people and process

(identity verification at onboarding) as well as technology (identity authentication during signing) elements. Without such additional measures, a public-key-based electronic signature will fail to meet even the requirements for medium assurance.

The relevance of public key cryptographic to the main functions of electronic signatures is summarized in the Table 6.

Table 6: Relevance of cryptography to electronic signature functionalities

Functionality	Relevance of Cryptography
1 Identity	None
2 Attribution	None ⁷⁶
3 Endorsement	None
4 Integrity	Cryptographic hashing ensures that the content of a document has not been modified after signing.

One solution to this identification problem is to entrust a third party to associate a person with a specific public key. Such third parties are referred to as a certification authority (CA) or, in some frameworks (such as eIDAS), as a trust service provider (TSP). In order to create and maintain the key-person association, the CA needs to verify the identity of the signatories to whom it issues private keys, maintain a list of public keys that relying parties can use for verification, and manage revocation of any key pairs that have been compromised. PKI comprises the set of complementary people, process, and technology elements that, taken together, provide for the management of the association of key pairs with signatories. The private key is issued to the signatory with a PKI-based digital certificate.^{77 7677}

technologies, when implemented appropriately, can achieve a very high level of trust, giving parties the confidence to take even the riskiest transactions online, with compounding effects of digital economic development.

While there is substantial overlap between digital and electronic signatures at the higher assurance levels (for example, qualified electronic signatures must implement digital signatures by definition), at lower assurance levels, they can be distinct. This relationship is summarized in Figure 6.

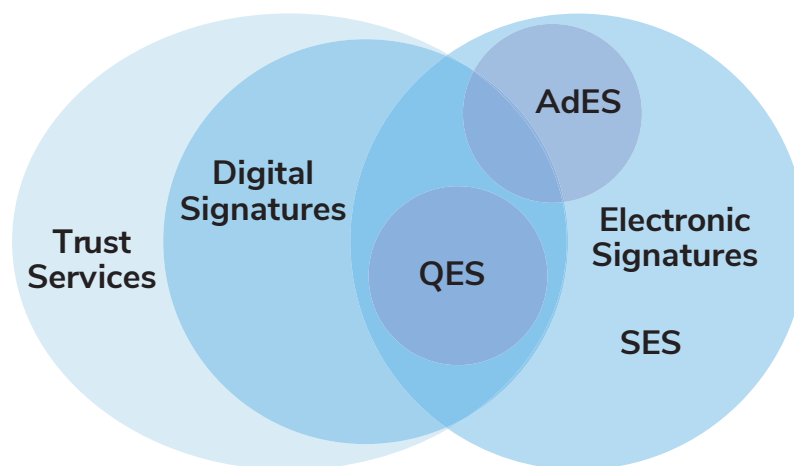
Current electronic signature regimes have a tendency toward excessive focus on the security benefits of certain sophisticated technologies, such as public key cryptography. This can lead to lower adoption, especially if requiring such signatures leads to high cost of low usability and creates unjustified friction for low-risk and everyday transactions. Conversely, such

The above diagram illustrates that while lower-trust electronic signatures may not need to be implemented as PKI-based digital signatures, such need is effectively a requirement for the higher trust levels. For example, the eIDAS requirements for the highest (qualified) assurance level must be based on a qualified certificate, which, in turn, must be issued by a qualified TSP—a role which, in practice, is fulfilled by a CA operating within a PKI. It is worth noting that various common legal frameworks, including not only eIDAS but also the UNCITRAL Model Law on Electronic

⁷⁶ In some technologically sophisticated implementations, a verifiable timestamp issued by a trusted timestamping authority can provide additional evidence of attribution. This can be relevant to use cases where repudiation of the timing of the transaction is a significant risk. Such implementations are typically limited to niche high-risk use cases and are outside the scope of this note.

⁷⁷ Digital certificates are governed by the X.509 ITU standard defining the format of public key certificates, assuring the binding between identities and public keys.

Figure 6: Digital and electronic signatures



Signature (MLES), implicitly endorse PKI technology for the higher trust levels, arguably undermining claims of technology neutrality. Ongoing discussions around the upcoming revision to the eIDAS framework have examined this technology specificity as a potential issue, especially from a perspective of potential incompatibility with the next generation of digital identity solutions.⁷⁸ The future-proofness of an exclusive reliance on PKI for high-trust electronic signatures is thus called into question.

Readers looking for details on operationalizing a PKI on a national level to support electronic signature implementation⁷⁹ are referred to the companion note to this document.⁸⁰

6.3 THE ROLE OF DIGITAL IDENTITY

Reliably establishing the identity of the signer—and the attribution of the signature to that identity—is fundamental to trust in an electronic signature. In a digital world, this implies a core role for digital identity.

When issuing a digital identity credential, it is common to require issuers to verify the identity attributes against a pre-existing foundational or legal ID system to ensure that the digital ID is issued to a real-world person and that this person will be the sole person in control of the digital ID credential issued. Due to the need to assure the identity of signers, the requirements for electronic signatures are very similar. Identity must be assured both at onboarding (for example, the initial issuance of a signing certificate) and during the signing transaction itself (authentication).

Table 7 shows the complementary roles of the digital ID and electronic signature solutions for a stylized high-trust electronic signature implementation.

Due to the technical and operational similarity of these processes, there are clear synergies and complementarities between digital ID systems and electronic signature frameworks and solutions. For this reason, digital ID and electronic signature can be implemented together, with a digital ID credential being linked to, or containing, a signing certificate. Examples of such countries include

78 Schwalm, S., Albrecht, D. & Alamillo, I., (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2022. Bonn: Gesellschaft für Informatik e.V.. (S. 63-74). DOI: 10.18420/OID2022_05

79 In addition to electronic signatures, PKIs can also support other types of services that require trusted cryptographic verification (sometimes referred to as “trust services”).

80 Christopher Tullis and David Black (2024), “Public Key Infrastructure: Implementing High-Trust Electronic Signatures,” Washington D.C: World Bank.

Table 7: Illustrative example of the roles of providers of digital identity and trust services

	Function	Assured through...	Primary actor
1	Identity	Identity checks during issuance of digital certificate used for signing	Legal identity ⁸¹ authority ⁸²
2	Non-repudiation	Authentication during signing	Electronic signature solution or external digital identity provider ⁸³
3	Endorsement	Authentication during signing	Electronic signature solution or external digital identity provider
4	Integrity	Digital certificate used for signing	Certification authority

Estonia,⁸⁴ Singapore,⁸⁵ Germany,⁸⁶ Georgia,⁸⁷ Spain,⁸⁸ and Argentina,⁸⁹ among others. The synergies also spill over into the regulatory framework, with the EU eIDAS framework being one example of a harmonized regulatory approach to mutual recognition and standardization of digital identity and electronic signatures.

Despite numerous national ID systems successfully incorporating digital certificates and high-trust electronic signatures into national ID credentials, these solutions have seen remarkably low adoption. The adoption rates of these capabilities have been less than optimal. This can largely be attributed to inadequate understanding of the technology, usability challenges, ambiguity surrounding

use cases, and an excessive emphasis on security and high-trust signatures, which may appear daunting to the average citizen. Looking forward, it's imperative that future iterations of these systems, as well as new ones, take a more balanced approach. By better harmonizing digital ID frameworks with electronic signature regulations, it's possible to enhance the offerings of low to medium trust electronic signatures. This can also lead to making qualified signatures more user-friendly, thereby significantly boosting their usage among citizens. This dual approach, focusing on both the low-trust and high-trust ends of the spectrum, will likely yield a higher degree of engagement and adoption.

81 Legal identification systems provide recognition before the law and proof of legal identity. Principles on Identification for Sustainable Development: Toward the Digital Age. Washington, D.C.: World Bank Group. <http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age>

82 Because certificate issuance is a one-time process, it is common to use traditional legal ID credentials such as a national ID card or passport. In principle, this identity verification can take place either in person or online.

83 One standard definition of a digital identity provider can be found in NIST 800-63-3 Digital Identity Guidelines: "Identity provider (IdP): The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials." In the context of an electronic signature implementation, the digital ID provider could be the same entity that provides signature or certification services, or an external digital ID could be used. Since online authentication is a requirement for electronic signature, it is not possible to use a traditional ID credential unless it has digital ID functionality allowing it to be used for authentication online.

84 Estonia's national ID card includes a chip that contains two certificates: one for proving identity (authentication), and another for digital signing (digital signature). The Mobile-ID offers similar architecture, with the difference that the certificates are stored on the SIM card of the mobile phone while the Smart-ID version offers a software-based solution in which storage of the digital certificates are split between a smartphone app on the user's device and the cloud. <https://www.id.ee/en/article/digital-signing-and-electronic-signatures/>

85 The Singaporean smartphone-based digital ID includes a service called "Sign with Singpass" allowing high-trust PKI-based electronic signatures to be generated using the mobile app. Cooper, Adam Kenneth; Marskell, Jonathan Daniel; Chan, Cheow Hoe. National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX. Washington, D.C.: World Bank Group. <http://documents.worldbank.org/curated/en/099300010212228518/P171592079b3e50d70a1630d5663205bf94>

86 The German national ID card (Personalausweis) has an embedded chip for electronic signatures. Germany also launched a smartphone app (AusweisApp2) that acts as a card reader, allowing online use of the national ID card for electronic signatures. <https://www.ausweisapp.bund.de/en/how-to-use-the-eid-function>

87 The Georgian national ID card contains a chip with a digital certificate allowing generation of high-trust electronic signatures. Currently, the national ID card issuer - the Public Service Development Agency - is the only accredited qualified trust service provider in the country, and the national ID card is the only option for generating electronic signatures benefiting from full legal equivalence to handwritten signatures. https://sda.gov.ge/?page_id=5090

88 The Spanish national ID card (DNI electrónico) includes a digital chip containing two digital certificates: one for authentication and another for electronic signing. The card can be used in combination with a card reader attached to a computer to sign documents online. Additionally, a smartphone app called DNle en el móvil (DNle on mobile) allows electronic signature generation using a smartphone. <https://www.dnielectronico.es/portaldnie/>

89 Argentina's national identity authority has a smartphone app called Mi Argentina. The app includes a digital certificate allowing generation of electronic signatures with the same legal validity as handwritten signatures. <https://www.argentina.gob.ar/aplicaciones/mi-argentina>



7 CONCLUSIONS

The section includes suggestions for practitioners implementing electronic signatures frameworks at national and international levels.

7.1 STRATEGIC

Take a strategic approach based on the requirements of specific signing use cases and their corresponding transaction risk levels:

- **Focus on the functions of an electronic signature to determine the right technology.** Whether handwritten or digital, signatures provide four related but distinct functions: (1) identifying the signer, (2) preventing the signer from subsequent disavowal of their signature (non-repudiation), (3) indicating the intent of the signer to endorse the contents of the signed document, and (4) ensuring that the document is not modified after signing (integrity). Different use cases will put a premium on different functions, and the technology choices should follow from these requirements, not the other way around.
- **Properly manage the people, process, and technology elements to ensure trust.** Understand that trust is rooted not only in technology used but also the people and process elements of an electronic signature framework. In particular, the real-world identity of the signer is vulnerable to compromise if the people and process elements, used to associate the data required to create and bind electronic signatures (the user account) to a real-world entity (natural or legal person), are not rigorously controlled to maintain trust in an electronic signature framework, particularly at the higher levels of assurance.
- **Design according to demand.** Situate the design of an electronic signature framework within an analysis of the demand for electronic signatures by relying parties and individual users. Use cases will differ depending on country or sectoral context as well as the maturity of local digital ecosystems, and understanding these constraints and opportunities is necessary to ensure that the electronic signature framework is fit-for-purpose.

In particular, any decision to implement a national-scale PKI should be evaluated and scoped against the specific demand for PKI-based electronic signatures.

- **Design to promote adoption.** Do not assume that adoption will follow straightforwardly from provision, as global experience shows that multiple barriers to adoption including cost, usability, access, lack of demand, and poor understanding of benefits—on the side of individual users as well as relying parties—can undermine uptake of electronic signature frameworks. To achieve widespread adoption, design implementation should balance security and usability, and follow standards that allow interoperability.

7.2 LEGAL AND REGULATORY

Build a trust framework based on a risk-based approach to provide multiple, complementary levels of assurance:

- **Adopt a risk-based approach to accommodate various levels of transaction risk.** Implementation of electronic signature should follow a risk-based approach that allows for solutions that serve the needs of low- to high-risk transactions. While the latter may focus on security, the priorities of the former may prioritize usability, adoption, and cost-efficiency, among other factors. Clearly defined, outcome-based levels of assurance can form the basis of a trust framework that serves the needs of transactions at all risk levels.
- **Extend trust through regulation to scale the digital economy.** Electronic signature regulation should be based on a “do no harm” principle. To this end, existing trust relationships between contracting parties should continue to underpin trust in transactions. Furthermore, regulators should see their role as extending existing sources of trust—through standards and transparency—to allow electronic transactions to scale the digital economy beyond the current confines of existing trust relationships. This extension can include scaling to new

sectors, new untrusted parties, and new risk levels, where electronic transactions would not be possible without the transparency and trust supplied by regulation.

- **Incorporate existing sources of trust into trust frameworks to avoid a trust monopoly.** While trust frameworks are necessary to extend trust, regulation should not be so stringent as to crowd out existing sources of trust. Existing relationships, practices, and products may already provide adequate trust for certain transactions; a trust framework should avoid disrupting such well-functioning trust relationships. Regulators should seek complementarity with sectoral regulations. In a similar vein, legal equivalence of electronic signatures should not scope creep into legal preference, since even the most advanced digital economy may still need analogue measures as backup (for example, if the internet goes down).
- **Deploy electronic signatures as part of a holistic digital economy reform.** While electronic signatures and the trust frameworks that enable them are a cornerstone of a trusted digital economy, they should be deployed in the context of complementary enablers. Robust foundational and digital ID systems are needed to allow the electronic signature regime to be implemented in a trusted way. The “functional equivalence” principle that underpins electronic signature trust frameworks should also apply to other aspects of the digital economy, such as electronic communications, electronic commerce, and electronic transactions in the broad sense. Additionally, many of the same principles (and implementation approaches) that promote trust in electronic signatures for individual signers can also be applied to authenticating documents issued by legal persons (such as governments or firms) either through electronic signature legislation or through complementary trust frameworks (e.g., for electronic stamps or seals).

7.3 TECHNICAL

Technical and financial considerations to promote adoption, innovation, and sustainability include:

- **Maintain technology neutrality.** This is necessary to allow for innovation and product differentiation to cater to different use cases. It also prevents the need to revise legal and trust frameworks to keep up with natural technological evolution. Outcome-based standards, such as levels of assurance, should be preferred over technology-based

specifications. Technology neutrality also allows systems to extend and scale to new use cases, new technologies, and keep pace with evolving requirements.

- **Consider how the electronic signature framework interacts with the ID ecosystem.** Having some assurance of the identity of the signer is an essential component to all but the lowest-trust electronic signatures. Therefore, identity must be assured both at onboarding (e.g., issuance of a signing certificate) and during the signing transaction itself (e.g., authentication). Linkages with legal identity systems that provide for digital verification of attributes and/or digital authentication can help improve trust in the binding between electronic signatures and the signers authorized to create them. There are dividends to stack-based thinking, considering electronic signature as part of the national digital public infrastructure. Integration of electronic signature capability into the legal ID system itself—as done somewhat successfully with smartcards, and increasingly in mobile form factors – is another potential avenue.
- **Align with international standards to facilitate mutual recognition.** Cross-border recognition of electronic signatures created in one market and used in another requires trust in not only the technology used but also the supporting people and process elements. If electronic signatures are perceived not to follow international norms, it may affect their recognition abroad. Countries can maximize recognition by aligning their levels of assurance with international standards as much as possible.
- **Promote sustainable business models for trust service providers.** While project financing can provide for initial expenditures, especially if in-house infrastructure is opted for, these systems can become costly to maintain over time and can atrophy without sufficient demand for electronic signature services. Ongoing cost drivers are particularly high in PKI-based implementations.⁹⁰ Facilitating participation of the private sector as providers of electronic signatures should be expressly considered as a means of ensuring ongoing financial sustainability.
- **Promote usability and cost-efficiency.** The high costs of implementing electronic signatures lowers adoption for service providers, who may be wary of turning users away from their service or passing higher transaction costs onto users. Flexible, technology-neutral, and risk-based approaches can lower cost to end users and remove barriers to adoption.

⁹⁰ For additional discussion, see the companion note to this document, Christopher Tullis and David Black (2024), *Public Key Infrastructure: Implementing High-Trust Electronic Signatures*, Washington D.C.: World Bank.



8 APPENDICES

APPENDIX 1: GLOSSARY OF KEY TERMS

Certification Authority (CA), or certificate issuer, is an authority trusted by one or more entities to create and digitally sign public-key certificates. Optionally, the certification authority may create the subjects' keys.⁹¹

Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but it does not necessarily need to uniquely identify the subject in all contexts.⁹²

Digital public infrastructure refers to foundational and reusable digital platforms and building blocks—such as digital ID, digital payments, and data sharing—that underpin the development and delivery of trusted, digitally-enabled services across the public and private sectors.

Digital signature is a technical construct and means “an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature.”⁹³

Electronic authentication is the process of establishing a level of confidence in whether a statement is genuine or valid when conducting a transaction online or by phone. It helps build trust in an online transaction by giving the parties involved some assurance that their dealings are legitimate. These statements might include: identity details; professional qualifications; or the delegated authority to conduct transactions.⁹⁴

Electronic transaction means a transaction, action, or set of actions of either a commercial or non-commercial nature, and includes the provision of information and/or e-government services.⁹⁵

Electronic seals provide assurance of the origin and integrity of a data message that originates from a legal person.⁹⁶

Electronic signature is a legal construct that means “data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.”⁹⁷

eIDAS Regulation, short for Electronic Identification, Authentication and Trust Services Regulation, governs electronic signatures in the EU. Formally, eIDAS is made up of EU Regulation 910/2014 of 23 July 2014 as revised by EU Regulation 2024/1183 on 20 May 2024.

Functional equivalence means that an electronic signature will have the same legal effect as the paper-based signature, including its evidentiary value in courts as it could be both (a) admitted and (b) potentially recognized as valid evidence in legal proceedings as fulfilling part, or all, of the functions that a signature normally serves (be it proof of identity, endorsement, integrity, or non-repudiation). This is based on the “functional-equivalent approach” underlying the UNCITRAL Model Law on Electronic Commerce, which

91 Information technology–Open Systems Interconnection–The Directory: Public-key and attribute certificate frameworks. ITU X.509. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-201910-!!!PDF-E&type=items

92 Digital Identity Guidelines. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

93 Ibid.

94 Australian Government e-Authentication Framework: An Overview, Department of Finance and Administration, Commonwealth of Australia http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication

95 SADC Model Law on Electronic Transactions & Electronic Commerce, Establishment of Harmonized Policies for the ICT Market in the AC. Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA). https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

96 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>

97 UNCITRAL. 2001. *Model Law on Electronic Signatures*. Vienna: UNCITRAL. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.⁹⁸

Interoperability is the ability of one entity to communicate with another entity.⁹⁹

Legal identity is the basic characteristics of an individual's identity (e.g., name, sex, place and date of birth) recognized under applicable law. Legal identities may be issued and managed by civil registration systems or other authoritative sources of identity data in a country.¹⁰⁰

Mutual recognition frameworks extend a **trust framework** (see definition below) beyond national borders, enabling cross-border recognition and interoperability of electronic signatures.

Level of assurance frameworks describe the requirements that digital identity and electronic signature systems and services must meet in order to provide a certain level of assurance in their reliability.¹⁰¹

Non-repudiation means protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.¹⁰²

Public key cryptography, which is the basis for digital signatures, involves generating two unique keys using algorithmic functions that are mathematically related. One key is used to transform a document into an unreadable format and create a digital signature, while the other key is used to verify the signature and confirm that the document

has not been altered from its original form.

Public key infrastructure, or PKI, is the infrastructure able to support the management of public keys that support authentication, encryption, integrity, or non-repudiation services.¹⁰³

Presumption of reliability allows whoever is claiming the electronic signature to presume, by law, that the electronic signature introduced before the court constitutes valid evidence of key parameters, such as the identity of its author and the integrity of the contents of the data or document.¹⁰⁴

Relying party is an entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.¹⁰⁵

Trust framework is a generic term often used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements.¹⁰⁶

Trust service means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving, and electronic registered delivery services.¹⁰⁷

Trust service provider is a person or legal entity who enters into an arrangement with a subscriber for the provision of one or more trust services.¹⁰⁸

98 UNCITRAL. 1996. *Model Law on Electronic Commerce*. Vienna: UNCITRAL. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

99 Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf>

100 ECOSOC resolution E/CN.3/2020/15. United Nations Economic and Social Council. <https://unstats.un.org/unsd/statcom/51st-session/documents/2020-15-CRVS-EE.pdf>

101 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>.

102 For additional discussion, see also UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>

103 Information technology-Open Systems Interconnection-The Directory: Public-key and attribute certificate frameworks. Recommendation ITU-T X.509. International Telecommunications Union. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>

104 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>

105 Digital Identity Guidelines. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

106 Trust Frameworks for Identity Systems. Open Identity Exchange. <https://openidentityexchange.org/networks/87/item.html?id=175>

107 UNCITRAL. 2022. *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*. Vienna: UNCITRAL. <https://uncitral.un.org/en/mlit>.

108 Ibid.

APPENDIX 2: ELECTRONIC SIGNATURE USE CASES

The following table gives a list of some typical transactions in various sectors, grouped according to the risk level of the transaction. The risk categorizations should be taken as indicative.

Table 8. Common electronic transactions across sectors grouped by risk level

Sector	Transaction Risk Level (<i>indicative</i>)		
	Low	Medium	High
Banking	Opening a basic savings account		
	Authorizing payments below a certain threshold	Opening higher value accounts (investment account)	Authorizing high-value payments (large international wire transfers)
	Accessing online banking (checking balance, viewing account history)	Authorizing payments	
	Acknowledging receipt or accepting terms and conditions ("I agree")	Contracts for financial products (mutual funds, derivatives)	
Credit	Submitting a loan application	Signing typical loan agreements	Signing high-value or corporate loan agreements
Insurance	Signing insurance policy change requests or other low-risk forms	Signing insurance policy applications and renewals	Signing high-value insurance contracts (life insurance, annuities)
		Signing claims forms	Signing insurance contracts with significant legal implications (reinsurance agreements, commercial policies)
Health	Health screenings (health history questionnaires, surveys)	Signing prescriptions	Signing prescriptions for controlled substances
	Consent for low-risk medical procedures (routine blood tests, immunizations)	Consent for complex medical procedures (surgeries, diagnostic tests)	Signing medical records or reports for legal or regulatory purposes
			Consent for medical directives with legal implications (end-of-life decisions, complex directives)
Education	Course enrollment	Signing student registration forms for academic courses or programs	Signing agreements related to clinical trials or medical research
	Attendance tracking (online classes)	Online exam submissions	Signing official academic documents, such as transcripts or diplomas

Sector	Transaction Risk Level (<i>indicative</i>)		
	Low	Medium	High
Commerce	Online order confirmations		Signing deeds, mortgages, or other real property documents
	Acknowledging and accepting terms and conditions (“I agree”)	Signing and executing typical contracts	High-value corporate transactions (such as mergers and acquisitions)
	Signing non-disclosure agreements (NDAs)		Signing documents with significant powers of attorney or other significant legal implications
Public Services	Accessing government portals to fill out basic forms (voter registration, driver’s license renewal)	Accessing secure government portals for confidential information (medical records, criminal history)	Accessing highly confidential government data (national security information, classified documents)
	Submitting simple requests for information or support	Applying for licenses or permits (construction permits, business licenses)	Signing legal agreements with government entities (leases, procurement contracts)
			Submitting tax declarations
Judiciary	Acknowledging receipt of documents or communications	Signing affidavits or declarations	Signing court orders or judgments

APPENDIX 3: GOOD PRACTICE LEGAL FRAMEWORKS

When it comes to international good practice for electronic signatures, two main texts are commonly referred to as references. Although there is continuous innovation in electronic signature legal regimes internationally, many countries have drawn upon at least one of these references.

UNCITRAL Model Laws

Model laws were developed by the United Nations Commission on International Trade Law (UNCITRAL) to harmonize legislation around the world on electronic commerce and electronic signatures.¹⁰⁹ Although these models are not legally binding, they serve as an example framework for countries to create or revise their domestic laws in line with international standards and best practices.

Many countries around the world have adopted these model laws either through direct implementation or as a basis for domestic law reform.¹¹⁰

Over the past three decades, there has been significant work by UNCITRAL on various conventions and model laws to promote trust in electronic commerce and transactions, building on each other to establish norms for regulation of electronic transactions and electronic signatures.

Two UNCITRAL model laws are of particular historical importance to establishing trust in electronic signatures. The earlier of the two is the 1996 Model Law on Electronic Commerce (MLEC), which established the **“functional equivalence approach,”** which is also the overall approach taken by this note. Functional equivalence is based on an analysis of the various requirements for paper-based documents in terms of their functions, in order to determine

how those same functions could be fulfilled differently using digital means.¹¹¹ It recognized the validity of electronic information and expanded the definition of a “writing” to encompass information accessible and usable, regardless of format. While the MLEC did not establish specific standards or procedures as substitutes for a signature, it provided some basic standards for electronic signatures, considering factors like identification methods and reliability criteria.

The MLEC was later extended in 2001 by the Model Law on Electronic Signature (MLES), which focuses specifically on the equal treatment of electronic and paper documents. The MLES contains a number of technology-specific provisions that focus on public key cryptography, while maintaining an overall technology-neutral approach with flexibility to accommodate other technologies as well.¹¹²

The various UNCITRAL texts as well as the key provisions of each are summarized in Table 9.

European Union

As mentioned in the above sections, a more recent legal framework for electronic signatures that is often referred to as good practice is the eIDAS Regulation which is binding on all EU member states. eIDAS Regulation¹¹⁴ has come to serve as a reference beyond the EU since it incorporates and expands on internationally-recognized standards, including some which had been introduced under previous texts such as UNCITRAL’s MLES as well as Directive 1999/93/EC of the European Parliament and of the Council.¹¹⁵ As such, eIDAS Regulation reiterates key principles from previous good practice such as the **“non-discrimination principle”**¹¹⁶ while reiterating the **“functional equivalence approach”** as

¹⁰⁹ While the model law on e-commerce was developed in 1996, that on electronic signatures was developed later in 2001.

¹¹⁰ Legislation based on or influenced by the Model Laws on Electronic Commerce and Electronic Signatures has been adopted in 38 States (39 jurisdictions) and 83 States (163 jurisdictions), respectively. Comprehensive lists are maintained by UNCITRAL.

https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce/status

https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

¹¹¹ The specific functions analyzed in the MLEC, which applied to electronic documents in general and not to signatures specifically, included functions such as legibility, inalterability, reproducibility, authentication through signature, and acceptance by public authorities and courts. UNCITRAL. 1996. Model Law on Electronic Commerce with Guide to Enactment. Vienna: UNCITRAL. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

¹¹² UNCITRAL. 2001. Model Law on Electronic Signatures with Guide to Enactment. Vienna: UNCITRAL. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.

¹¹³ The full name is the United Nations Convention on the Use of Electronic Communications in International Contracts.

¹¹⁴ EU Regulation 910/2014.

¹¹⁵ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

¹¹⁶ The non-discrimination principles holds that a signature should not be denied legal effect solely on the grounds that it is in electronic form or that it does not meet the requirements for high-trust signature (“qualified” signature).

¹¹⁷ See Article 29.

Table 9. UNCITRAL texts and key milestones

UNCITRAL text	Key milestones
<i>Model Law of Electronic Commerce</i> (1996)	Includes rules regarding writings and signatures and established the functional equivalence approach. Admissibility and evidential weight of data messages are also considered.
<i>Model Law on Electronic Signatures</i> (2001)	Focuses on legal recognition of electronic signatures, specifically their functional equivalence to paper signatures.
<i>E-Commerce Convention</i> (2005) ¹¹³	Establishes principles and rules that enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts.
<i>Explanatory note on Promoting Confidence in Electronic Commerce</i> (2007)	Offers guidance to States and businesses on fostering an enabling environment for electronic commerce.
<i>Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services</i> (2022)	Addresses the legal recognition of foreign identity management and trust services, providing a framework for cross-border mutual recognition.

well as the principle of **technological neutrality**. However, eIDAS Regulation goes beyond then-existing frameworks to offer a much more elaborate framework for cross-border and cross-sector recognition of electronic signatures and e-transactions, while delving much more than previous texts into the requirements according to which a high-trust (“qualified”) electronic signatures may be granted equivalent legal effect of a handwritten signature.¹¹⁷

Brazil

Brazil has embraced electronic signatures as legally binding since the enactment of the Provisional Measure No. 2200-2/2001, establishing a comprehensive legal framework that includes the Brazilian Public Key Infrastructure (ICP) for regulating e-signatures. This foundation is further strengthened by subsequent laws such as the Brazilian Civil Code, the Economic Freedom Act (Law 13.874/2019), and the Digital Government Act (Law 14,129/2021), facilitating a tiered approach to electronic signatures that accommodates varying levels of transaction risk. The legislation allows for a wide range of e-signature applications, from basic to advanced and qualified, with the latter requiring digital certificates from ICP-Brasil. Notably, Law 14,063/2020 specifies the use of electronic signatures in public sector interactions and health-related matters, introducing three categories of signatures: standard, advanced, and qualified. Each category has its own set of requirements and use cases, particularly emphasizing the necessity for qualified signatures in significant governmental acts and certain commercial transactions,

such as real estate dealings. Brazil’s legal framework for e-signatures demonstrates a commitment to technological neutrality, functional equivalence, risk-based approaches, and the facilitation of secure digital transactions across sectors.

South Africa

In South Africa, the Electronic Communications and Transactions Act 25 of 2002 governs the legal landscape of electronic transactions and signatures, aiming to facilitate and regulate these modern forms of communication and transaction. This legislation promotes the use of electronic transactions, especially among small, medium, and micro enterprises (SMMEs), and focuses on broadening access, human resource development, preventing information system abuse, and encouraging e-government services. It defines electronic signatures as data intended by the user to serve as a signature, whether attached to, incorporated in, or logically associated with other data. Furthermore, the Act introduces the concept of advanced electronic signatures, which are electronic signatures resulting from a process accredited by the Authority. This accreditation process is detailed, including application requirements and penalties for false claims of accreditation.

United Arab Emirates

The United Arab Emirates (UAE) modernized its electronic transactions framework with the Federal Decree Law No. 46 of 2021, superseding the original decree from 2006. This

new law categorizes electronic signatures into standard, advanced, and qualified types. It recognizes electronic signatures, documents, seals, and transactions as legally equivalent to their handwritten counterparts, ensuring their validity and enforceability across various contexts, including dealings with government entities. Moreover, the law endorses the use of any form of electronic signature for transactions and establishes a Digital ID system, sanctioned by the Telecommunications and Digital Government Regulatory Authority (TDRA), as a standard method for accessing government services and conducting electronic dealings.

The legislation distinguishes between different levels of electronic signatures based on the trust and security they offer. Qualified electronic signatures, which require a digital certificate from a trusted authority, are recognized for their high trust level. Similarly, advanced electronic signatures are noted for their security measures and technical requirements in identifying the signatory. This multi-tiered approach reflects the UAE's commitment to enhancing the security, reliability, and efficiency of electronic transactions within its legal and regulatory framework, promoting technological advancement and digital governance.

South Korea

South Korea's Digital Signature Act, revised in 2020, represents a significant advancement in the legal framework for electronic

signatures, promoting their use and ensuring the safety and reliability of electronic documents. The Act defines electronic signatures as electronic data attached to or logically associated with an electronic document to identify the signatory and to confirm that the document has indeed been signed by the signatory. This legislation also introduces accreditation measures for electronic signature certification, verifying the unique link between electronic-signature-creation data and a subscriber, thereby enhancing trust and security.

The previous legal framework had mandated the use of a certified electronic signature based on a public key certificate for legal validity. However, the 2020 amendment relaxed this requirement, equating electronic signatures with traditional handwritten signatures in legal standing and broadening the acceptance of various electronic-signature-creation devices. The amendment also set operational standards for electronic-signature certification services, aiming to increase the reliability of electronic signatures. These changes not only provided a framework for users and subscribers to make informed choices regarding certification services but also aligned South Korea's electronic signature regulations with international standards, facilitating trust and global interoperability in electronic transactions.

APPENDIX 4: FROM ANALOG TO DIGITAL TRUST

Not all sources of trust used in paper-based transactions can translate seamlessly into the digital world. Additional factors specific to digital interactions add a layer of complexity including difficulty in differentiating between original and duplicate messages, susceptibility of electronic data to be intercepted and modified, the capacity to process transactions in bulk, as well as the automation of processes. Considerable potential for fraud exists in exploiting these additional vulnerabilities introduced by technology.

Justifiably, hyper-focused attention to technology as part of the problem has sometimes led to a biased tendency to discuss technology-centric solutions. While there are sophisticated technologies available that can improve the level of security of electronic transactions, an excessive focus on such technology solutions overlooks the fact that the majority of electronic transactions worldwide do not make use of any particular signature technology.

For example, a customer might place an order with a supplier over email, and the supplier may deem the customer's typed name in the email as a sufficient signature to accept the order and dispatch the goods. There are number of potential reasons why these parties might trust this transaction enough to be unworried about a legal challenge, including: (a) a low transaction value; (b) a history of successful completion of similar transactions; (c) a secure communication channel, such as the order coming from a trusted email address; as well as (d) a wish to prioritize fluidity of transactions over security for commercial reasons.

In establishing regulations for electronic signatures, it is crucial to balance considerations, preventing excessively complex technological requirements that may have a chilling effect on electronic transaction volume. Trust in the digital world requires supplementing and preserving existing sources of trust in paper transactions, without assuming a deterioration in existing trust relationships. Over-formalization of digital trust, or over-reliance on technology-based trust, could overshadow non-technological sources of trust.

The additional vulnerabilities of electronic media, as well as the need to leverage digital technologies to reinforce trust, have caused the attention of electronic signature legal

frameworks to go beyond questions of identity and turn to additional concerns, including:

- The need to recognize the legal validity of the **electronic form** of signatures.
- The need for clear **rules and standards for the use**¹¹⁸ of electronic signatures across transactions and industries.
- The need to ensure the **security and reliability of electronic systems** issuing signatures.
- The need to recognize such **validity across jurisdictions**.

As highlighted in a recent study, the main obstacle to wider use of electronic signatures is the legal uncertainty regarding their validity and effectiveness. It is not always clear which transactions can be carried out effectively with electronic signatures (and with which type of electronic signature).¹¹⁹ The development of legal frameworks for electronic signatures that address these concerns is a key step to avoid creating ambiguity and inconsistency in how signatures are used electronically and helps foster legal certainty and trust in the use of electronic documents and transactions, which is key to the development of digital economies. It should be noted that the legal framework for electronic signatures does not address which type of electronic signature should be used for which type of document or transaction. These requirements, which are linked to the risk level of such transactions, are typically determined by the needs of signature users and verifiers, and may also be influenced by sectoral legislation (for example, in the financial sector).

118 Often referred to as "technical specifications," these standards are "a voluntary means of providing for interoperability between equipment and processes" (See S. Mason in *Electronic Signatures in Law*, Chapter 16, p.384, published by University of London Press; Institute of Advanced Legal Studies, available at: <http://www.jstor.com/stable/j.ctv5137w8.7>).

119 Neistadt, Maria. 2022. "Electronic Signatures: At a Glance." Brussels: European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2022\)739238](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739238).

