computation

MDPI

Article

Digital Transformation of Signatures: Suggesting Functional Symmetry Approach for Loan Agreements

Viktor Titov [1,*], Pavel Shust [1], Victor Dostov [1], Anna Leonova [2], Svetlana Krivoruchko [3], Nadezhda Lvova [1], Iurii Guzov [1], Angelina Vashchuk [1], Natalia Pokrovskaia [1], Anton Braginets [1] and Mikhail Zaboev [4]

[1] Modern Financial Technology Laboratory of St Petersburg University, Saint Petersburg State University, 199034 St. Petersburg, Russia; p.shust@spbu.ru (P.S.); v.dostov@spbu.ru (V.D.); n.lvova@spbu.ru (N.L.); y.guzov@spbu.ru (I.G.); a.vashchuk@spbu.ru (A.V.); n.pokrovskaia@spbu.ru (N.P.); a.braginets@spbu.ru (A.B.)
[2] Russian Electronic Money and Remittance Association, 107078 Moscow, Russia; leonova@npaed.ru
[3] Department of Banking and Financial Markets, Financial University under the Government of the Russian Federation, 125993 Moscow, Russia; skrivoruchko@fa.ru
[4] Department of Information Systems in Economics of St Petersburg University, Saint Petersburg State University, 199034 St. Petersburg, Russia; m.zaboev@spbu.ru
* Correspondence: v.o.titov@spbu.ru

Abstract: This article aims to formulate proposals for regulatory bodies whose implementation would ensure the effective introduction of civil circulation into electronic signatures, with minimal costs for economic entities. While electronic signatures have been widely discussed in academic literature, there are still gaps in the understanding of similarities and differences between electronic and handwritten signatures, the functional specifics of the relationship between them, and the role of electronic signatures for electronic contract. Our research has allowed us to overcome this gap adopting a functional symmetry approach based on measuring the distance between fuzzy sets and the Mamdani fuzzy inference algorithm. This made it possible to form an estimate of the degree of functional symmetry between different types of signatures in a fuzzy and exact form. Correspondingly, we argue that the signature can be viewed as a set of procedures rather than as a single act in order to achieve functional symmetry with a handwritten signature. The case of online lending was used to test and prove this hypothesis. Therefore, regulating electronic signatures needs to focus on the efficiency of this processes for ex ante identification, capturing the intent, ensuring the inalterability and providing reliable evidence, irrespective of the type of electronic signature that is used. It was also revealed that the proposed functional symmetry approach can be combined with a fuzziness index analysis to provide new prospects for further research.

Keywords: electronic signature; handwritten signature; electronic signature regulation; digital economy; fuzzy model; online lending; loan agreement; digital transformation

Citation: Titov, V.; Shust, P.; Dostov, V.; Leonova, A.; Krivoruchko, S.; Lvova, N.; Guzov, I.; Vashchuk, A.; Pokrovskaia, N.; Braginets, A.; et al. Digital Transformation of Signatures: Suggesting Functional Symmetry Approach for Loan Agreements. *Computation* **2022**, *10*, 106. https://doi.org/10.3390/computation10070106

Academic Editor: Shengkun Xie

Received: 27 May 2022
Accepted: 19 June 2022
Published: 24 June 2022

1. Introduction

Handwritten signatures have been used in day-to-day interactions for centuries. However, growing reliance on remote communications as well as usage of new technical devices have made lawmakers and regulators introduce equivalents of handwritten signatures that can be used in non-face-to-face environment.

This has led to the introduction of electronic signature (e-signature) regulation. The tables have turned, for while the handwritten signature has never been regulated in much detail, the e-signature regulation is almost a separate universe with its own regulatory framework that has often very specific and impenetrable technical standards. This is partly why some jurisdictions are still struggling to implement relevant regulations, as this is certainly a case where one size does not fit all. Meanwhile, market players are finding themselves between a rock and a hard place, being either under significant regulatory

pressure (which may jeopardize the growth of online businesses) or having no regulatory protection at all (piling up risks in the system and eventually jeopardizing consumer trust).

The goal of this article is to formulate proposals for regulatory bodies whose implementation would ensure the effective introduction into civil circulation of electronic signatures, with minimal costs for economic entities. To achieve this goal, a comparative analysis of handwritten and electronic signatures, the functions of different types of signatures, as well as their practical application in certain situations was carried out. This goal suggested the following main research questions:

- What are the common functions of the handwritten and electronic signatures?
- What characteristics of electronic signatures should be functionally equivalent to handwritten signatures?
- What approaches are relevant for policy makers and private actors to ensure the functional equivalence of electronic and handwritten signatures?

We build upon the notion of functional symmetry that implies, as put by Savin [1], that 'like should be regulated alike' (i.e., similar functions shall entail similar regulatory requirements). Following Veerpalu's research on functional symmetry [2], we claim that to ensure actual equivalence, a signature needs to be seen as a set of procedures rather that an instrument.

We apply the principle of functional symmetry to handwritten and electronic signatures to verify the appropriate regulatory approach. Our analysis shows that instead of functional symmetry, current regulatory framework tends to be more instrument-specific and this is potentially detrimental to e-signature usage by businesses and, in particular, individuals (due to over-regulation). Outcome-based regulation, on the other hand, can be a more efficient alternative to instrument-specific approaches. We suggest that 'deconstructing' the concept of the signature may allow for more precise risk assessment and the saving of resources by using cheaper alternatives to qualified electronic signatures that require complicated regulatory framework and expensive infrastructure. Otherwise, there is a risk of falling into a 'digitization trap' whereby the attempt at digitizing inefficient processes leads to digitizing efficiency, rather than minimizing it.

There is a somewhat patchy coverage of signatures (both electronic and handwritten) in academic literature. The legal concept of handwritten signatures has been well discussed through in-depth analysis by Stephen Mason [3] which covered both the legal and historical aspects of this phenomenon. Lon L. Fuller [4] has contributed significantly to the understanding of the handwritten signature in an oft-cited work on the functions of legal formalities. Yet, the handwritten signature itself is mostly discussed in the context of forensic examination: for example, using pattern recognition technologies [5], neural identification of a signature [6], biometric identification [7], using deep convolutional neural networks [8], etc. There has been wider discussion surrounding electronic signatures, however, most of these authors look at the e-signature more as a technology rather than as a 'signature'. Applied aspects in mobile-based e-signatures [9], using electronic watermarks [10] are good examples of such technology-focused research. Implementation of electronic signature legislation has also spurred multiple papers on local regulatory approaches, e.g., for Hungary [11], China [12], the United States [13], and the European Union including comparative analysis [14].

Another body of research is dedicated to those electronic contracts which are intrinsically related to signatures [15], as well as the act of 'signing', and mostly cover consumer protection issues: for example, material clauses disclosure [16,17], usage of standard electronic contracts and contracts on consuming digital content [18]. However, despite a seemingly wide coverage of electronic signatures in academic literature, there are still gaps in understanding of the similarities and differences between electronic and handwritten signatures, the functional specifics of their relationship and the role of the electronic signature for electronic contract.

The research problem is that, in fact, the electronic signature has been implemented in the business processes of various organizations on a global scale. Different countries use

different technologies to implement the electronic signature technology. However, studies related to the extent to which various technologies of "electronic signatures" correspond "in terms of strength" to handwritten counterparts in various fields of activity are practically absent. The complexity of this assessment is due to the fact that it is multifaceted, since it must be analyzed by various specialists, from lawyers and economists to IT specialists and mathematicians. Such problems can be solved with the help of expert evaluation methods; our article is therefore devoted to these issues.

This article aims to identify a relevant approach to ensure the functional symmetry of electronic and handwritten signatures in terms of digital transformations. From a methodological perspective, Veerpalu's [2] research provides the valuable rationale to develop functional regulation for the innovative processes and services. Therefore, the research methodology is based on a comparative analysis of the existing handwritten and electronic signature regulation and synthesis of the outcome-focused approaches to achieving similar results in similar circumstances of online lending.

The article is structured as follows. First, we look at the concept of the handwritten signature and academic perspectives to identifying its functions. Then, we provide a brief overview of regulatory approaches to electronic signatures and symmetrically transpose the main functions of the handwritten signature to the e-signature. In the empirical section, we describe the case of electronic contracts between borrower and lender in online lending services to identify the procedures that may strengthen reliability of online interaction between these two parties. Finally, we outline conceptual conclusions and identify policy implications and recommendations for the public and private actors. The areas for further research are discussed as well.

2. Rationale for the Research Methodology

2.1. The Handwritten Signature and Its Functions

Although handwritten signatures play a pivotal role in business, and despite their ubiquitous usage, legal definitions of the handwritten signature are scarce. In his excellent analysis, Mason [3] cites multiple definitions of a handwritten signature. In Russian legal practice, the handwritten (or personal) signature is a set of symbols inscribed by hand with the purpose of identifying a person (See: (1) Appeal ruling of Leningrad regional court of 11.09.2019 in case No. 33-5452/2019; (2) decision of the Kalininsky district court of Chelyabinsk of 09.10.2018 in case No. 2-3245/2018; (3) Appeal ruling of Krasnodar regional court of 29.05.2018 in case No. 33-13084/2018; (4) decision of Armenian city court of the Republic of Crimea of 04.04.2017 in case № 2-1/2017(2-370/2016;)~M-329/2016; (5) decision of Chertanovsky district court of Moscow of 09.09.2016 in case No. 2-4890/2016; (6) Absentee decision of the Vasileostrovsky district court of Saint Petersburg dated 16.05.2016 in case No. 2- 168/2016 (2-5045/2015;)~M-4869/15; (7) decision of Rudnichny district court of city Prokopyevsk of 03.12.2015 in case No. 2-1769/2015)). Hays [19] refers to the United States Uniform Commercial Code which defines a signature as 'any symbol executed or adopted by a party with present intention to authenticate a writing'. If read altogether, all definitions of handwritten signatures boil down to a popular meaning: this is a sign of authenticity upon a durable medium that may be based on the name of the signatory.

Notably, the indication of the name is not the defining feature of the signature. Both popular and legal meanings of a signature are technology-neutral. There is significant variability in how a handwritten signature can be effected:

(a) in terms of medium: signature can be affixed either on a paper sheet, wood, napkin or anywhere else;
(b) in form: either 'name in cursive', name in block capitals, initials, a cross, a 'tick' or inked fingerprint;
(c) by the 'instrument': technically, a wet signature might be affixed by pen, pencil, a knife (e.g., for carving), not only by hand by also by keeping a pen in mouth (which is relevant for incapacitated persons).

Medium, form or instrument reflect the 'instrumental' approach to defining the handwritten signature. This is different from the 'functional' approach which is focused on the functions of a signature (Table 1) and can be applied to symmetrically integrating electronic ones.

Table 1. Functional approach to defining handwritten signature.

Research Examples	Functions of a Handwritten Signatory
Fuller [4] does not explicitly state the scope of formalities. Yet, he recognizes that it would be safe to assume that a signature is one of them.	**The evidentiary function**: the signature confirms that the contract exists. Although a consumer can enter into an agreement in a multitude of ways (e.g., by stating the will to enter into an agreement orally, by implicative actions or even by keeping silence), the signed paper is a durable medium that acts as evidence of a contract being concluded.
	The cautionary function: i.e., a 'check against inconsiderate action' by the signatory. Formality is a significant action that acts a symbol that the agreement imposes certain duties and responsibilities upon the signatory. Unlike evidentiary function, cautionary one is less tangible, as it is dependent on the social and psychological characteristics of the signatories.
	The channeling function: means that a legal formality shall signalize the enforceable promise. In other words, a handwritten signature would assure the parties that they can use the signed document as evidence in court and the judge will consider this contract enforceable. It is important to note that Fuller looked at legal formalities and not the handwritten signatures specifically. This explains why these functions do not explore the issue of reliability, although this is a necessary prerequisite for their effective execution.
Mason [3] develops Fuller's analysis and other research to identify the additional functions of the handwritten signature	**Primary evidential function** that confirms approval of the contents by the signatory. Consequently, the signatory also agrees that the document is binding upon him/her.
	Secondary evidential function: signature authenticates the signatory (i.e., is linked to the concrete person), as well as 'provides a record of the intent of the signatory, and, in turn, physical evidence of the originality and completeness of the document itself, including the time, date and place of the act of the affixing of the signature to the document' and confirms that no alterations to the document have been made.
	Protective function: a signature shall protect the party that the opposite signatory is who he/she claims to be and that the signatory affirmed the content of the document. In other words, this legal formality shall protect against backtracking of another party.
	Record keeping function: a handwritten signature is affixed to a durable medium that can be preserved over time.
Reed [20] simplified the functions of the signature to three main elements	**To authenticate the identity of a signatory.**
	Intention to sign.
	Intention to adopt a document.

We reveal that previous systems of functions do not address the question of reliability. The reliability of the handwritten signature is guaranteed by business practices, not legal requirements. This, in our opinion, is fundamental in correspondence to innovations related to the introduction of an electronic signature and defines the most significant functions to study.

- **Identification** (We use the term 'identification' instead of 'authentication' (used by Reed [20], Mason [3] and Fuller [4]) as it covers both ex-ante and ex post scenarios). The signature shall be linked to the signatory and provide protection against impersonation or backtracking. There can be ex ante identification (i.e., when a signature confirms the identity at the time of affixation) and ex post identification (i.e., when a

signature is used as forensic evidence to subsequently establish or confirm the identity of the signatory).

- **Expression of intent**. The opposite party needs assurance that the signatory expressed intent to be bound by the contract and this expression of will is admissible evidence in case of dispute (including redress in court). It is important to note that there is a difference between an understanding of the contents of a contract and intent to sign it. There are customers who may understand the contract and not sign it and customers who sign a contract without really understanding its contents.
- **Inalterability**. The signatory affixes the document, making sure that the original that is kept with the opposite party will not be altered.
- **Evidential**. Signed document might be used as evidence in case of disputes (including legal redress).

While cautionary and ex ante identification functions are relevant in the moment of affixing a signature, expression of intent, inalterability, ex post identification and evidential functions provide ex post protection. As seen from previous research, functions of a handwritten signature can be classified as 'inward' and 'outward'. 'Inward' functions are aimed at the signatory and would ceteris paribus address a cautionary function. As mentioned above, awareness would depend a lot on the characteristics of the signatory himself/herself, as well as the particular circumstances. Other functions of the handwritten signature are mostly focused 'outwards', benefiting those parties different from the signatory (e.g., protecting from the signatory backtracking). It is important to note that, again, in different circumstances the efficiency of these functions may vary significantly.

2.2. Types of Electronic Signatures

A technical overview of the electronic signature goes beyond the scope of this research. Yet, it is important to note that there are multiple modalities of how e-signatures might work. Unlike handwritten signatures, electronic signatures that are based on cryptographic mechanisms sign the unique hash-function of the electronic document, instead of the document itself. This ensures inalterability, as any meddling with the document might be detected. However, simpler signatures (such as one-time-passwords) may not be directly related to the document itself and represent only randomly generated codes or codes generated based on the date/time.

Lawmakers usually adopt the tiered approach to e-signature regulation. As shown above, this is quite different from virtually non-existent handwritten signature regulation. For example, eIDAS Regulation in the European Union instates the following types of electronic signatures:

(a) electronic signature (also dubbed in practice as 'simple electronic signature');
(b) advanced electronic signature;
(c) qualified electronic signature.

In practical terms, the **simple electronic signature (SES)** is the instrument with the lowest assurance level.

In general, SES itself references the signatory but does not necessarily authenticate a signatory person itself. Therefore, it is similar to the handwritten signature—quite vague in form, with the appropriateness of SES being defined by circumstances. Yet, as can be derived from the E-Sign definition, SES might provide evidence of intent. For example, per legal practice, automated signatures in email footers might be considered enforceable SES, if conditions of intent are met (Neocleous & Anor v Rees [2019] EWHC 2462 (Ch) (20 September 2019), available at: http://www.bailii.org/ew/cases/EWHC/Ch/2019/2462.html (accessed on 12 January 2022)). Despite the almost ubiquitous usage, SES have been mostly neglected in academic literature: possibly, because of the lower assurance level. In particular, Bell et al. [14] outright brushes the SES off the table (in our opinion, unfairly): 'everyone is better off using the 'advanced' signatures'.

Regulation also does not seem to favor simple electronic signatures: the characteristics of **advanced electronic signature (AES)** are more clearly defined.

AES requirements are very peculiar from a theoretical perspective. Linkage to the signatory, the identification and control over signature creation data mirror those of the handwritten signature and fall under the 'identification' function (namely, each signature shall be unique to the individual who can use it). 'Detectable data change' is an 'inalterability' function as AES generally fulfills all the functions of a handwritten signature. This leaves limited room for qualified electronic signatures. It is noteworthy to consider the advantages of the latter implying functional symmetry (Table 2).

Table 2. Functional symmetry comparison of SES and AES.

	Simple Electronic Signature	Advanced Electronic Signature
Identification function	-	+
Expression of intent	+	+
Inalterability function	-	+
Evidential function	+	+

Qualified electronic signatures (QES) have the same characteristics as AES but shall be created by a 'qualified electronic signature creation device' (as per eIDAS) and be based on a qualified certificate for electronic signatures. Qualified electronic certificates are issued by the qualified service providers which are subject to specific requirements and effectively act as trusted third parties. In other words, QES goes beyond the functions of a handwritten signature. Unlike the latter, it is issued by an independent party that the other parties rely on for ex ante identification.

Although the nomenclature seems very clear (from the least reliable to the most reliable e-signature), in effect the lines are very blurred. Multiple sources (Signicat, NautaDutilh, Cryptomathic) imply that QES is the only functionally symmetrical equivalent of the handwritten signature. Actually, this is not quite true. The EIDAS regulation states that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature (Article 25(2)). Yet, the recital 49 goes on to explain that 'it is for national law to define the legal effect of electronic signatures'. In other words, both SES and AES can be functionally symmetrical equivalents of a handwritten signature as well. The only question is where and how. Adding to this collision is the fact that lawmakers require a specific type of e-signature in some circumstances. For example, in Russia SES cannot be used for electronic exchange related to state secrets (See: paragraph 4 of art. 9 of Federal Law No. 63-FZ of April 6, 2011 'On electronic signature'). The practice varies in the European Union as well (For an excellent breakdown of e-signature requirements in different countries see https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/03/coronavirus-electronic-signatures-when-can-these-be-used-a-global-perspective.pdf (accessed on 15 May 2022)).

To put it simply, electronic signatures are confusing as a result of overregulation aimed at solving multiple problems at once. In particular, although AES generally fills the shoes of the handwritten signature, the regulatory gravitation towards QES is explained by the fact that a qualified electronic signature provides an ex ante identification function which the handwritten signature does not have. QES is lucrative to regulators because it implies reliance on the third party: unlike handwritten signature, QES is 'issued' to the person. Yet, most policies aimed at substituting handwritten signatures with QES are likely to fail, as, unlike handwritten signature, QES usage is conditional—the customer needs to go through identification by a trust service provider (TSP). TSP services cost money, the certificates have expiration dates and QES often requires usage of the specific signature creation device (such as token). Therefore, despite mandated 'legal equivalence', QES is certainly far from being a functionally symmetrical substitute of a handwritten signature in practical terms—it is more reliable yet more complicated to use. Gravitation towards QES might also be attributed to the marketing activities of trust service providers for which QES issuance and usage is a source of income.

We believe that this confusion and potential over-regulation might be solved by employing functional symmetry approach. This approach implies that a set of procedures are used to achieve the desired outcomes between certain institutional units based on signature functions that makes it possible to apply functional symmetry between different types of signatures in a fuzzy and exact form.

2.3. Mathematical Models for Expert Opinions Processing

Under a high degree of uncertainty inherent to socio-economic processes, approaches are effectively based on the following theories: probability theory, possibility theory and fuzzy set theory.

Causal relationships between factors can be described by probabilistic–statistical, fuzzy and expert methods, as well as their combinations.

One of the most common methods for expert assessment of the causality of relationships are methods that allow for the evaluation of various coefficients of causal relationships between factors: DEMATEL, MICMAC.

The Decision Making Trial and Evaluation Laboratory (DEMATEL) method [21,22] is a multi-criteria decision-making method that implies the efficient identification of causal relationships of a complex system based on aggregation of expert assessments. This method aggregates a collective expert opinion in order to exclude random relationships between indicators and criteria, and to identify the most important indicators that determine some integral characteristic based on causal relationships.

The Matrix d'Impacts Croises Multiplication Appliqué un Classement (MICMAC) method [23] is a procedure for constructing a classification matrix of factors cross-influence that aims to assess the degree of dependence of the influence of variables based on ranking. All factors belong to one of four clusters: autonomous, dependent, interconnected and independent. These factors are grouped on the basis of a potential and strength of influence. Autonomous factors are factors that have a weak potential and power of influence. Dependent factors are factors that have low potential but strong influence. Interconnected factors are factors that have a high potential and power of influence. These factors are causally related, that is, an action on one of them will lead to a change in the other. Independent factors are factors that have strong potential but little influence. All factors are plotted on a graph with four clusters, where the potential of the variable is on the Y-axis, and the strength of influence is on the X-axis [24].

Another effective approach for expert opinions processing is an expert survey model based on the theory of fuzzy sets. According to the theory of fuzzy sets, objects may have different degrees of membership to different sets, and the measure of this fuzziness is a parameter for evaluating the quality of various procedures and algorithms in pattern recognition, decision-making, information retrieval models, etc.

3. Expert Assessment of the Functional Correspondence between Electronic Signatures and Handwritten Signatures

An expert assessment of the functional correspondence of handwritten and electronic signatures can be implemented using fuzzy set theory. The advantage of this approach is that fuzzy logic is not binary, and therefore implies a non-mutually exclusive nature of the concepts of "true" and "false".

Models based on fuzzy sets have a number of basic differences from traditional models that allow them to achieve a certain competitive advantage:

- the use of fuzzy numbers (a number of parameters in any models cannot be set unambiguously: expert opinions, results of marketing surveys, etc.);
- formalization of natural language words using the apparatus of linguistic variables: "better", "worse", "possibly", etc.;
- conducting qualitative assessments of the initial data and results in terms of their reliability, taking into account the interpretation of natural language words;

- modeling complex economic processes and systems with a given degree of accuracy based on fuzzy logic methods (the researcher does not spend much time finding out the exact values of variables and compiling regression equations).

To build fuzzy models for an evaluation of the symmetry of electronic and handwritten signatures, the previously defined compliance criteria will be used:

- identification function (IF);
- expression of intent (EI);
- inalterability function (FC);
- evidential function (EP).

Let's define three fuzzy sets:

- HS—functional symmetry of handwritten signature to itself;
- SES—functional symmetry of SES to handwritten signature;
- QES—functional symmetry of QES to handwritten signature.

According to the theory of fuzzy sets, for each set a universal set and a membership function must be given.

In our case, the universal set will be specified by the criteria of functional correspondence:

$$U = \{FI, FN, FC, EP\} \quad (1)$$

Fuzzy set HS:

$$HS = \sum_{i \epsilon U} \mu_{HS}(u_i)/u_i \quad (2)$$

Fuzzy set SES:

$$SES = \sum_{i \epsilon U} \mu_{SES}(u_i)/u_i \quad (3)$$

Fuzzy set QES:

$$QES = \sum_{i \epsilon U} \mu_{QES}(u_i)/u_i \quad (4)$$

where $\mu_{HS}(u_i)$, $\mu_{SES}(u_i)$, $\mu_{QES}(u_i)$ represent membership functions of the fuzzy sets HS, SES and QES, respectively.

In our research, we propose to evaluate the degree of functional symmetry of an electronic signature of two types and a handwritten signature based on the calculation of the distance between fuzzy sets.

One approach to determining the distance between fuzzy sets uses the Hamming relative distance formula:

$$I_L((, A,)) = \frac{1}{n} \cdot \sum_{i=1}^{n} |\mu_{HS}(u_i) - \mu_{SES}(u_i)| \quad (5)$$

where:

n represents the number of elements of fuzzy set and $\mu_{HS}(u_i)$ и $\mu_{SES}(u_i)$ represent the membership functions of the compared fuzzy sets HS and SES, respectively.

Let us consider the following expert estimates (Table 3).

Table 3. Membership function values.

Criteria (Signatory Functions)	HS	SES	QES
Identification function	1.0	0.2	0.6
Expression of intent	1.0	0.7	0.5
Inalterability function	1.0	0.25	0.7
Evidential function	1.0	0.4	0.6

The distance between fuzzy sets which characterized the functional symmetry of SES and HS based on Hamming relative distance (Formula (5)) is 0.61, and between QES and

HS is 0.4. Thus, the QES fuzzy set is closer to HS and functional symmetry between QES and handwritten signatures is higher.

One another important area where the elements of the theory of fuzzy sets are productively applied is the construction of fuzzy control systems. Fuzzy control systems allow the use of the main sources of information about the control object:

- mathematical models;
- actual observations of the behavior of the object;
- knowledge of people—experts in the field under investigation.

Basic components of the architecture of the fuzzy control system are: fuzzification block, base of fuzzy rules, fuzzy inference algorithm, defuzzification block.

Our research aims to build a fuzzy control model for estimating an integral indicator of the signatory equivalence between different types of electronic signatures and handwritten signature.

The main criteria of functional symmetry of signatures are the same:

- identification function;
- expression of intent;
- inalterability function;
- evidential function.

Therefore, our supposed experts suggest the following parameters for a Mamdani type fuzzy inference system (Table 4).

Table 4. Parameters of fuzzy inference system.

Linguistic Variable	Values of the Linguistic Variables (Fuzzy Sets)	Type of the Membership Functions	Parameters of the Membership Functions
Identification function symmetry	low middle high	high	[0.0 0.0 0.7] [0.1 0.5 0.9] [0.3 1.0 1.0]
Expression of intent symmetry	low middle high		[0.0 0.0 0.7] [0.1 0.5 0.9] [0.3 1.0 1.0]
Inalterability function symmetry	low middle high		[0.0 0.0 0.7] [0.1 0.5 0.9] [0.3 1.0 1.0]
Evidential function symmetry	low middle high	high	[[0.0 0.0 0.7] [0.1 0.5 0.9] [0.3 1.0 1.0]
Signatory equivalence	low middle high		[0.0 0.0 0.7] [0.1 0.5 0.9] [0.3 1.0 1.0]

To form the basis of fuzzy rules, experts can formulate vague statements in form, such as the one shown below:

$$\text{IF } \beta_1 \text{ is } A_1 \text{ AND } \beta_2 \text{ is } A_2 \text{ THEN } \beta_3 \text{ is } A_3 \quad (6)$$

$$\text{IF } \beta_1 \text{ is } B_1 \text{ AND } \beta_2 \text{ is } B_2 \text{ THEN } \beta_3 \text{ is } B_3$$

An example of fuzzy rule:

IF	Identification function symmetry	middle
AND	Expression of intent symmetry	middle
AND	Inalterability function symmetry	low
AND	Evidential function symmetry	low
THEN	Signatory equivalence	middle

The maximum number of the rules within above mentioned fuzzy expert system is 243, but in practice the rules base can be decreased and consist of a much smaller number of rules, due to excluding rare or obviously unrealistic combinations of the values of input factors and dependent variable [25].

The main stages of a Mamdani type fuzzy inference system algorithm are the following (considering rules in Formula (6) as an example):

Stage 1. Fuzzification (or introduction of fuzziness) of input variables: according to the actual exact values of the input variables $x_1^0 \in X_1$, $x_2^0 \in X_2$, where X_1 и X_2 are universal sets of input linguistic variables β_1 и β_2, degrees of truth are determined for the premises of each rule $\mu_{A_1}(x_1^0)$, $\mu_{A_2}(x_2^0)$, $\mu_{B_1}(x_1^0)$, $\mu_{B_2}(x_2^0)$.

Stage 2. Fuzzy inference, consisting of two actions—aggregation of premises and activation of rule conclusions. Firstly, the degrees of truth (power) of the rules (α_1 and α_2) are found, in the case of our model using the min operation, since the logical connectives "AND" are used:

$$\alpha_1 = \min\left(\mu_{A_1}\left(x_1^0\right), \mu_{A_2}\left(x_2^0\right)\right)$$

$$\alpha_2 = \min\left(\mu_{B_1}\left(x_1^0\right), \mu_{B_2}\left(x_2^0\right)\right)$$

Then "truncated" membership functions for rule conclusions are defined:

$$\mu'_{A_3}(y) = \min(\alpha_1, \mu_{A_3}(y))$$

$$\mu'_{B_3}(y) = \min(\alpha_2, \mu_{B_3}(y))$$

where:

$y \in Y$, Y—universal set of output variable β_3.

Stage 3. Accumulation of conclusions of fuzzy rules. "Truncated" functions are combined, and as a result constructed final fuzzy set for the output variable with a membership function:

$$\mu(y) = \max(\mu'_{A_3}(y), \mu'_{B_3}(y))$$

Stage 4. Defuzzification. Finding an equivalent to the generated fuzzy set for the output variable $\mu(y)$ in exact form using one of the following methods: center of gravity method, area center method, first or last maximum. In our case we used center of gravity method:

$$y^{=}\mathrm{COG}(\mu(y)) = \frac{\sum_{i=1}^{n} y_i \mu(y_i)}{\sum_{i=1}^{n} \mu(y_i)}$$

Using software environment Matlab and its application Fuzzy Logic Toolbox to construct fuzzy system, it is possible to evaluate the level of equivalence between handwritten and electronic signatures. For example, if the experts evaluated the levels of signatory equivalence between two types of electronic signatures (SES and QES) and handwritten signature for each criterion, presented in Table 3, then the integral indicator of the signatory equivalence will be in crisp form for SES—0.36, for QES—0.53.

The fuzzy sets which correspond to integral equivalence between SES, QES and handwritten signature obtained from the fuzzy inference system are presented in Figure 1.

As an obtained result, the functional symmetry between SES and handwritten signatures is higher than between QES and handwritten. The similar modelling may be applied for other types of electronic signatures.

In the next section, we discuss the practical case of online lending through the lens of a functional symmetry approach.

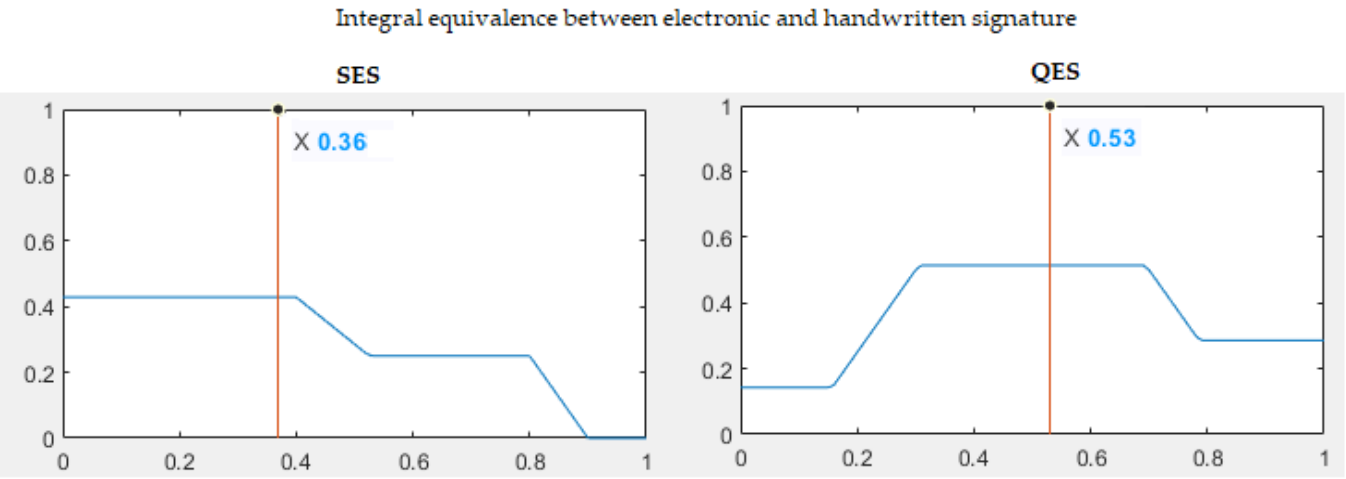

Figure 1. Integral equivalence between SES, QES and handwritten signature.

4. Signatures in the Financial Market: Case of Lending

4.1. Case Rationale

As usage of signatures and e-signatures is very circumstantial, their functions shall be discussed within a particular context to apply a suggested functional symmetry approach. We introduce the case of retail lending, taking in mind the following reasons: (a) lending requires established trust between the creditor and a borrower; (b) as a financial service it is heavily regulated, which means lasting duties and responsibilities between the parties are ensured; (c) lending is a case for information asymmetry between the professional lender and a consumer; (d) there is a growing number of lenders who provide their services completely online, moving away from traditional lending in a brick-and-mortar office; (e) the lending business is associated with risks of legal action; in case of defaults professional lenders are more likely to move to litigation (instead of just writing the debt off the books). Moreover, lending is also a good real-life example of how the nature of a business dictates the duties and responsibilities of the parties involved and how these are facilitated through signature and non-signature means. Using the methodology outlined above, we define the following outcomes and procedures that the parties would need to achieve in the course of lending-related contractual relations (Table 5).

Table 5. Signature functions and corresponding outcomes and procedures in case of lending.

Functions	Expected Outcomes	Outcome-Focused Procedures
Ex ante identification	The financial institution will need to conduct customer due diligence (CDD), as per anti-money laundering/combating financing of terrorism (AML/CFT) regulations. The financial institution will need to establish information about the borrower that will assist in collection of a loan (e.g., address, contact details). The financial institution needs to establish the financial standing (solvency) of the borrower.	Customer due diligence (identification and confirmation of identity), as per AML/CFT regulation
Expression of intent	The financial institution needs to obtain confirmation that the borrower agreed to the terms of a loan and has an intent to take it out.	Best practices for assent procedures
Inalterability	The borrower needs to make sure that the loan agreement is not changed by the financial institution unilaterally, thus leading to the unexpected expenses or losses.	Publishing authoritative copies on the website/making them available to the customer in other way
Evidence	Both creditor and borrower need to have admissible evidence of contractual relations, in case of in-court or out-of-court (e.g., through financial ombudsman) disputes.	Ensuring a reliable audit trail

Let us stress that not all discussed functions are necessarily intermediated by handwritten or electronic signatures. We look at each of these from the perspective of a functional symmetry approach to identify current practices and areas for improvement.

4.2. Case Analysis in the Context of Functional Symmetry Approach

4.2.1. Ex Ante Identification

Customer due diligence might be performed in a multitude of ways; most do not involve usage of any type of electronic signature at all: such as video identification, usage of digital identity, trusted third parties, etc. In essence there is a wide spectrum of approaches to establish the identity of the customer with different assurance levels, depending on the level of risks [26]. Since signatures (either handwritten or electronic) are not intrinsically designed for ex ante identification they do not constitute a reliable CDD method. The only exception is QES, which has an added authentication capability; however, this is almost never used as a sole authentication factor. Neither handwritten nor electronic signatures are useful for the purposes of facilitating collection or scoring: usually, other methods are used, such as obtaining information from a credit bureau [27].

Therefore, regulators need to ensure that financial institutions can use reliable non-face-to-face identification and verification of identity methods. These methods may or may not involve usage of QES and, as per FATF guidance, may depend on the level of risks defined by multiple factors. Scoring methods, such as access to credit bureaus or additional solvency information (e.g., obtaining a digital footprint) [28] play a pivotal role but do not require an e-signature per se. The specifics of the discussed problem in relation to auditing are discussed in Box 1.

Box 1. Case of lending: audit report and electronic signatures.

An audit report confirming the solvency and continuity of the client's activities is of serious importance for the implementation of lending. According to the International Auditing Standard No. 700 "Forming an opinion and drawing up an opinion on financial statements", the requirements for the form of the opinion are formulated as:

p. 20. The auditor's report must be drawn up in writing (written opinion).

p. A18. A written opinion is an opinion on paper and electronic media.

p. 47. The auditor's report must be signed by the auditor.

p. A65. Use of an electronic signature in the audit report is permitted, if this is permitted by law or regulatory act.

As a rule, the auditor's report and financial statements are signed by electronic signature on their own. However, the auditor's report and the client's statements must be stitched together during manual processing. When using an electronic signature, a document within a document is obtained. Technologically, this is not yet possible, which is a limiting factor in the introduction of not only electronic audit reports, but also smart contracts [29].

4.2.2. Expression of Intent

As shown above, if properly implemented, both handwritten and electronic signatures are historically good at fixing the expression of intent with the caveat that 'intent' is very context specific. As already discussed, this issue is intrinsically connected with the 'readability' of the legal documents and understanding of contract terms. We have to admit that at this time there is no technical capability that would ensure that the customer has read a contract, let alone understood it (although attempts were made to identify approaches to ensure that material facts were not obscured within a long legal contract [30]). Another potential risk is where the relationship between a signature and the contract is either absent or weak ('Russian doll' contracts). This explains why regulators tend to mandate the consumer protection rules in legal acts, other than leave it up to the parties to agree upon. Another approach is introduction of two-tiered disclosure where the customers are presented brief key information documents with a clear description of the product features and risks (For example, the requirement for key information documents are included in

PRIIP regulation as well as delegated regulation within the EU Payment Account Directive) together with the full text of the contract.

Both electronic and handwritten signatures cannot minimize the risks of a contract being unread, obscurity of material facts or 'Russian doll' malpractice per se. Rather, there is a common consensus that these risks need to be mitigated by appropriate assent procedures. For example, the American Bar Association has developed principles that businesses need to follow to ensure that the assent in electronic interactions is not disputed by the courts [31]. A similar approach has been taken by the Russian Central Bank which identified malpractice where a bank official in a brick-and-mortar office asked customers to confirm a transaction using OTP without disclosing that this OTP is also an assent to enter into contract (which is a form of obscuring material facts). All these safeguards are relevant for online lending as well.

Therefore, the expression of intent to take out a loan under predefined conditions is not dependent on the type of electronic signature per se. Regulators might be advised to focus attention on the requirements towards the procedure of signing the document electronically (such as 'Viewing of Terms before Assent', or a clear presentation of terms) and by clearly defining the 'consent'. A good practical example of this is the EU General Data Protection Regulation definition of 'consent', which is not dependent on the type of actions/signatures used—'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article. 4 (11)). Another safeguard approach is to implement a two-tiered approach to disclosure of material clauses that includes clear and brief key information documents.

4.2.3. Inalterability

Handwritten signatures are efficient at ensuring the inalterability of a written contract but only if the appropriate procedure is used: i.e., each party receives the authoritative copy of the contract. In electronic interactions this is more complicated, as framework terms and conditions can be published in plain text of the financial institution website. This might tempt the financial institution to change the terms unilaterally without properly notifying the customer. For example, as shown by Loos and Luzak [32], unilateral changes to agreements with online service providers (such as Google, Facebook and others) might be considered unfair practice as per the Unfair Contract Terms Directive (as amended) if (a) the conditions for these changes are not disclosed at the moment of entering contract and (b) the consumer cannot terminate a contract after being informed about the upcoming change of terms.

Subsequent changes to contracts do not relate to the usage of a signature and this issue goes beyond the scope of this research. Moreover, it is a common practice to include 'consent by continued usage' clauses in contracts, meaning that the client agrees to new conditions not by active actions (e.g., effecting a signature) but by silent consent. This means that customer may have properly signed authoritative paper-based copy of paper contract which is later made obsolete by the subsequent changes in referenced terms and conditions. The same is true for the electronic signature: AES or QES might ensure inalterability of the initial contract through technical means but cannot safeguard from subsequent unilateral changes (i.e., a consumer may use QES when signing a Google agreement, but this might be unilaterally changed later).

In online lending, unilateral changes of contract terms may have significant consequences for the consumer. To minimize the risks to borrowers, regulatory safeguards might be used. In particular, in Russia, the Law on Consumer Credit limits the lender's rights for unilateral changes to loan agreements: if a floating interest rate is used, the borrower shall be informed about its rate and the basis of its calculation. Lenders are also allowed to change fixed interest rate, fees, and penalties but only if this does not worsen the terms of the contract (i.e., the lender may lower the interest rate and not increase it). In this case the lender still needs to notify the borrower about the changes and provide access to new

terms and conditions (Article 5). The EU directive on consumer credit agreements requires that the borrowers be informed of any change in the borrowing rate 'on paper or another durable medium, before the change enters into force' (Article 11 (1)). Obviously, the risk of unilateral changes of contract are higher for framework contracts as they are usually just published online.

Apart from the regulatory safeguards for particular contract clauses, the appropriate procedure might ensure the inalterability of online contracts, irrespective of the type of the e-signature used, such as:

The lender might be required to publish all editions of framework agreements on its official website, while paper-based authoritative copies hand-signed by the lender are also kept by them. This will ensure consumer access to the information as well as an audit trail (in case of disputes). This solution, however, does not protect from malpractice where a lender does not publish updated terms and conditions on its website.

Terms and conditions digitally signed by the lender might be deposited to a trusted third party. Terms and conditions not deposited to the trusted third party shall not be enforceable. The downside is the need for the services of third party which means additional costs that will be eventually borne by the consumers.

The lender might also be obliged to send the consumers an authoritative copy of the updated terms and conditions digitally signed by the lender, for future reference. This is very similar to the procedures currently used for paper-based contracts and inherit the same risks: the customers may lose their own copies. This might also not work for framework contracts which are often amended unilaterally (i.e., each new version will need to be sent to the borrower).

The issue of the considered function in relation to tax regulation is presented in Box 2.

Box 2. Case of lending: tax regulation aspects.

Inalterability is also important for the recognition of a lending contract by a third party, in particular by tax regulators. For example, the Federal Tax Service of Russia (FTS) is an important leader in the digitalization of public services and document flow with long experience in electronic services for both individuals and legal entities. FTS focuses on the preparation and submission of documents to taxpayers in electronic form, receipt of tax returns signed with an electronic signature, verification of the electronic signature key, and verification of machine-readable powers of attorney. Various types of electronic signatures are used in electronic tax services. In particular, for the filing of tax returns by individuals, an unqualified signature is sufficient. Since 2020, there has been a transition to the exclusive use of an enhanced qualified electronic signature issued by accredited certification centers in business document interaction. Since mid-2021, a qualified electronic signature has been issued free of charge by the Federal Tax Service, and from the first months it has been in high demand among Russian businesses. Directions of tax regulation for electronic signatures are used for electronic documents in interaction between business units and on electronic trading platforms. Formally, the tax authorities do not interfere in business processes. However, the recognition of electronic documents signed with an electronic signature, in particular lending contracts, is important for tax liabilities of corporate income tax, value added tax, and other taxes paid by businesses. The importance of the tax authorities' recognition of electronic signatures in business document interaction has also been emphasized in the framework of the OECD's report on the Digital Transformation of Tax Administration in 2020. The practice of digital interaction between government and business in Russia was highly appreciated in this report.

4.2.4. Evidentiary Function Is Derivative to All Other Functions of E-Signatures

As an ex-post functionality, this requires an audit trail proving that all other functions were executed properly. As such, quality of evidence will depend on the proper procedural approaches. As a rule of thumb, any action made by the lender or the borrower shall be appropriately logged by IT-systems that provide an unalterable audit trail, admissible in court or during regulatory inspection. This is nothing new in a financial sector where the obligation to implement audit trail procedures is a part of the BCBS Risk Management Principles for Electronic Banking and local regulatory requirements, thus leading to strong consensus on the importance of an audit trail among banks [33]. Moreover, some financial

institutions and regulators may look at innovative technologies (such as distributed ledgers) for tamper-resistant audit trails [34].

When considering the evidentiary function of an electronic signature, attention should be paid to the related issue of the electronic documents' storage. According to the Reference Model for an Open Archival Information System (OAIS) (Reference Model for an Open Archival Information System (OAIS). CCSDS.org. Website. available online: https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology https://public.ccsds.org/pubs/650$\times$0m2.pdf (accessed on 12 January 2022)), which is used as methodical basis by the leaders of electronic document management (e.g., USA, Estonia, Italy), the long-term preservation of electronic documents aims to ensure the authenticity of the document that is subject to such preservation. At the same time, the authenticity is defined as the degree to which a person (or system) regards an object as what it is purported to be. Thus, the authenticity of the document is not an absolute, but a relative value.

Authenticity is judged based on evidence. In case we do not have indisputable evidence of signing the electronic document by a particular person (e.g., if the electronic document signed with SES is extracted from the system of its origin and transferred to the other system) this does not automatically lead to the irreversible loss of its authenticity. The authenticity of the document does not disappear but needs to be evaluated based on the remaining evidence. Accordingly, the possibility of moving an AES or QES file together with an electronic document is not sufficient for asserting that these types of signatures surpass SES.

AES and QES are exposed to technological risks that increase as time goes on. The keys used to form AES and QES signatures have a limited validity period. As a result, after a certain period, verification of these signatures becomes difficult or even impossible [35]. The development of quantum computing technology threatens the reliability of cryptographic algorithms that are used in modern electronic signature infrastructure (PKI) (Kop, M. Establishing a Legal-Ethical Framework for Quantum Technology. Yale University, 2021, available online: https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology. (accessed on 12 January 2022)). Thus, the effectiveness of AES and QES in the context of long-term preservation of evidence should not be overestimated.

5. Conclusions

5.1. Conceptual Considerations

Nearly ubiquitous usage of electronic agreements has fueled the discussion about electronic signatures. As a result, many jurisdictions have created robust e-signature regulatory frameworks. These initiatives have been focused on the implied symmetry of the signatory function: documents signed with an electronic signature shall have the same power as documents signed with a handwritten signature. Yet, functional symmetry assumes that we know the left side of the equation (i.e., what handwritten signature is and what functions it has). However, there seems to be extremely limited research on this. This has led to the following implications. First, regulators have started to focus on assurance levels and creating private key infrastructure which, as our analysis shows, is not always required to ensure functional symmetry. Secondly, e-signature regulation seems to be falling into a 'digitization' trap where traditional processes and procedures are digitized by default—without examining whether these initial precedents were efficient. This approach mirrors that of Veerpalu's [2] where functional symmetry and corresponding signatory equivalence is judged by the ability to achieve a similar outcome, albeit through different processes.

Our research suggests two conceptual considerations that have reflected the objectives of our research. First, we suggest that the signature shall be viewed not as an act but rather as a set of procedures associated with affixing the signature itself. Correspondingly, 'deconstructing' the signature in a set of procedures might inform efficient policy and business decisions to symmetrically integrate electronic signatories. Secondly, our research shows the importance of a functional symmetry approach to policy making in the realm of

electronic signatures. We suggest that the efficiency of electronic signature regulation is assessed based not on the assurance levels or type of e-signature but on whether participants of legal relations have achieved the desired functions in a way that is symmetrical to a handwritten signature (i.e., ex ante identification, expression of intent, inalterability and creation of reliable evidence).

The assessment of the functional symmetry of handwritten and electronic signatures is a poorly formalized task, which requires the involvement of experts who must express their opinion. An effective approach to formalizing and processing expert opinions is the use of mathematical models based on the theory of fuzzy sets. The approaches proposed in this paper, based on measuring the distance between fuzzy sets and the Mamdani fuzzy inference algorithm, make it possible to form an estimate of the degree of functional symmetry between different types of signatures in a fuzzy and exact form. For example, numerical experiments have shown that QES has a higher level of symmetry with respect to a handwritten signature than SES.

5.2. Policy Implications

Based on our research, the following policy recommendations might be useful to achieve sufficient functional symmetry of handwritten and electronic signatures in a financial services sector (and other sectors as well, considering the specificity), irrespective of what type of e-signature is used.

For ex ante identification, regulators need to implement multiple options for non-face-to-face identification and confirmation of identity, as far as they are in line with the FATF recommendations and correspond to ML/TF risks. These options may not necessarily include usage of e-signatures.

To ensure proper capture of intent, regulators need to focus on implementing or recommending best practices regarding the process of signing electronic documents, to ensure capture of intent is retained irrespective of what type of e-signature is used. This implies specific, informed and unambiguous intent in the form of affirmative action. This might be supported by identification of malpractices aimed at confusing customers and pressuring them to unwillingly agree to contract terms.

To minimize information asymmetry, it is advisable to implement a two-tiered approach to the disclosure of material clauses in electronic agreements (e.g., by introducing key information documents) for improved readability of contracts for consumers, irrespective of what type of e-signature is used.

For the purpose of inalterability, the financial institutions might be required either to deposit authoritative copies of the electronic contract with a trusted third party (depositary) or send the digitally signed authoritative copy to the customer. Another option is to publish scanned and digitally signed copies of paper framework contracts on the financial institution website. The actors need to be mindful of the risks and costs associated with each of these options.

Regulations need to identify the scope of material clauses of framework contracts that cannot be changed unilaterally to the applying e-signatory (or without obtaining active affirmative action-based consent from the consumer).

Financial institutions need to ensure maintenance of an audit trail that would constitute admissible evidence, irrespective of the type of e-signature used by the consumer. Apart from transactional history, this audit trail needs to prove that all signature functions are implemented correctly (the identity of the consumer is verified, as per regulations, the consumer entered the contract willingly and knowingly, contract terms have not been amended unbeknownst to the customer). To ensure credibility of the audit trail, which is one of the key conditions for accepting it as reliable evidence, it is also possible to address a trusted third party. Long-term preservation of electronic documents signed with e-signatures is moving from passive data storage towards active operations aiming to ensure the availability and authenticity of electronic documents. As a result, the role of professional participants in this field is expected to grow.

These recommendations apply not only to the financial sector but also to any businesses that operate online, depending on level of risk. For example, food delivery services are not subject to AML/CFT requirements, therefore verification of identity does not require high level of assurance; yet the expression of intent might be relevant for them.

5.3. Further Research

The analytical framework developed in this research might be further improved by cross-country comparative analysis of e-signature implementation and correlation between regulatory approaches and actual application of e-signatures by the public. From our point of view, further research is needed in the context of the main areas of application of electronic signatures, including the spheres of activity of the public administration sector, corporations, non-profit organizations serving households, and relations with non-residents. For these new cases, the proposed functional symmetry approach can be combined with a fuzziness index analysis (as was shown above) that provide new prospects for further expert research.

In the context of the financial services sector, an electronic signature is in demand not only for the provision of these services by businesses to households, but also in a wide range of financial relations involving consumers, business and the state. Another important issue that might need to be reviewed is the risks of electronic signatures related to protecting personal data. We also believe that there is a need for more cross-disciplinary research that includes behavioral aspects, information security and AML/CFT considerations in devising best practices for the integration of electronic signature technology in different sectors of the economy.

Author Contributions: Conceptualization, V.T., P.S. and V.D.; data curation, M.Z.; formal analysis, V.T., P.S., V.D., A.L., S.K., N.L., I.G., A.V., N.P. and A.B.; funding acquisition, V.T. and I.G.; investigation, P.S., V.D., A.L., S.K., N.L., I.G., A.V., N.P., A.B. and M.Z.; methodology, A.L., S.K., N.L., I.G., A.V., N.P., A.B. and M.Z.; project administration, V.T. and P.S.; supervision, V.T., P.S., V.D. and N.L.; writing—original draft, P.S., V.D., A.L., S.K., N.L., I.G., N.P., A.B. and M.Z.; writing—review & editing, V.T. and A.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Savin, A. Rule Making in the Digital Economy: Overcoming Functional Equivalence as a Regulatory Principle in the EU. *J. Internet Law* **2019**, *22*, 1–31.
2. Veerpalu, A. Functional Equivalence: An Exploration Through Shortcomings to Solutions. *Balt. J. Law Politics* **2019**, *12*, 134–162. [CrossRef]
3. Mason, S. *The Signature. Electronic Signatures in Law*; University of London Press: London, UK, 2016; pp. 1–94. [CrossRef]
4. Fuller, L.L. Consideration and Form. *Columbia Law Rev.* **1941**, *41*, 799–824. [CrossRef]
5. Han, K.; Sethi, I.K. Handwritten signature retrieval and identification. *Pattern Recognit. Lett.* **1996**, *17*, 83–90. [CrossRef]
6. McCabe, A.; Trevathan, J.; Read, W. Neural network-based handwritten signature verification. *J. Comput.* **2008**, *3*, 9–22. [CrossRef]
7. Vargas, F.; Ferrer, M.; Travieso, C.; Alonso, J. Off-line Handwritten Signature GPDS-960 Corpus. In Proceedings of the Ninth International Conference on Document Analysis and Recognition (ICDAR 2007), Curitiba, Brazil, 23–26 September 2007; pp. 764–768. [CrossRef]
8. Hafemann, L.G.; Sabourin, R.; Oliveira, L.S. Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognit.* **2017**, *70*, 163–176. [CrossRef]
9. Ruiz-Martínez, A.; Sánchez-Martínez, D.; Martínez-Montesinos, M.; Gómez-Skarmeta, A.F. A Survey of Electronic Signature Solutions in Mobile Devices. *J. Theor. Appl. Electron. Commer. Res.* **2007**, *2*, 94–109. [CrossRef]
10. Zhu, L.; Zhu, L. Electronic signature based on digital signature and digital watermarking. In Proceedings of the 5th International Congress on Image and Signal Processing, Chongqing, China, 16–18 October 2012; pp. 1644–1647. [CrossRef]
11. Blythe, S.E. Hungary's Electronic Signature Act: Enhancing economic development with Secure Electronic Commerce transactions. *Inf. Commun. Technol. Law* **2007**, *16*, 47–71. [CrossRef]

12. Rambarran, I.A. I Accept, But Do They? The Need for Electronic Signature Legislation on Mainland China. *Pac. McGeorge Glob. Bus. Dev. Law J.* **2002**, *15*, 406–436. Available online: https://scholarlycommons.pacific.edu/globe/vol15/iss2/14 (accessed on 1 December 2021).
13. Wittie, R.A.; Winn, J.K. Electronic Records and Signatures under the Federal E-Sign Legislation and the UETA. *Bus. Law.* **2000**, *56*, 293–340. Available online: https://digitalcommons.law.uw.edu/faculty-articles/154 (accessed on 1 December 2021).
14. Bell, J.; Gomez, R.; Hodge, P.; Mayer-Schönberger, V. Electronic signature regulation: An early scorecard-comparing electronic signatures legislation in the US and the European Union. *Comput. Law Secur. Rev.* **2001**, *17*, 399–402. [CrossRef]
15. Freeman, E.H. Digital Signatures and Electronic Contracts. *Inf. Syst. Secur.* **2004**, *13*, 8–12. [CrossRef]
16. Clapperton, D.; Corones, S. Unfair Terms in 'Clickwrap' and other Electronic Contracts. *Aust. Bus. Law Rev.* **2007**, *35*, 152–180.
17. Kaviar, H. Consumer Protection in Electronic Contracts. *Int. Arab J. Inf. Technol.* **2011**, *2*, 96–104.
18. Helberger, N.; Loos, M.B.M.; Guibault, L. Digital Content Contracts for Consumers. *J. Consum. Policy* **2013**, *36*, 37–57. [CrossRef]
19. Hays, M.J. The E-Sign Act of 2000: The Triumph of Function over Form in American Contract Law. *Notre Dame L. Rev.* **2001**, *76*, 1183–1214.
20. Reed, C. What is a Signature? *J. Inf. Law Technol. (JILT)* **2000**, *3*. Available online: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (accessed on 1 December 2021).
21. Chen, F.H.; Chi, D.-J. Application of a new DEMATEL to explore key factors of China's corporate social responsibility: Evidence from accounting experts. *Qual. Quant.* **2015**, *49*, 135–154. [CrossRef]
22. Wu, H.-H.; Chgan, S.-Y. A case study of using DEMATEL method to identify critical factors in green supply chain management. *Appl. Math. Comput.* **2015**, *256*, 394–403. [CrossRef]
23. Khanam, S.; Siddiqui, J.; Talib, F. Modeling the TQM enablers and IT resources in the ICT industry: An ISM-MICMAC approach. *Int. J. Inf. Manag.* **2016**, *1*, 195–218. [CrossRef]
24. Nazarov, D.M. Classification of models and description of trends in assessing the causality of relationships in socio-economic processes. *Bus. Inform.* **2020**, *14*, 47–61. [CrossRef]
25. Zaboev, M. Adaptive Network-Based Fuzzy Inference System for The Operational Planning at The Enterprise. In Proceedings of the International Business Information Management Association Conference, Seville, Spain, 1–2 April 2020; pp. 3120–3127.
26. Shust, P.M.; Dostov, V. Implementing innovative customer due diligence: Proposal for universal model. *J. Money Laund. Control* **2020**, *23*, 871–884. [CrossRef]
27. Hwang, B.-H.; Tellez, C. The Proliferation of Digital Credit Deployments. *CGAP Brief* **2016**, *3*, 1–4. Available online: https://openknowledge.worldbank.org/handle/10986/24567 (accessed on 1 December 2021).
28. Berg, T.; Burg, V.; Gombović, A.; Puri, M. On the Rise of FinTechs: Credit Scoring Using Digital Footprints. *Rev. Financ. Stud.* **2020**, *33*, 2845–2897. [CrossRef]
29. Guzov, I.N.; Kovalev, V.V.; Marganiya, O.L. *Accounting in the XXI Century*; Scythia-Print: St. Petersburg, Russia, 2021.
30. Gindin, S.E. Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears. *Northwest J. Technol. Intellect. Prop.* **2009**, *8*, 1–37.
31. Kunz, C.; Del Duca, M.; Thayer, H.; Debrow, J. Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent. *Bus. Lawyer* **2001**, *57*, 401–429. [CrossRef]
32. Loos, M.; Luzak, J. Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers. *J. Consum. Policy* **2015**, *39*, 63–90. [CrossRef]
33. Abdou, H.; English, J.; Adewunmi, P. An investigation of risk management practices in electronic banking: The case of the UK banks. *Banks Bank Syst.* **2014**, *9*, 1816–7403.
34. Westerlund, M.; Neovius, M.; Pulkkis, G. Providing Tamper-Resistant Audit Trails with Distributed Ledger based Solutions for Forensics of IoT Systems using Cloud Resources. *Int. J. Adv. Secur.* **2018**, *11*, 288–300.
35. Stančić, H. Long-term Preservation of Digital Signatures. In Proceedings of the Technical and Field Related Problems of Traditional and Electronic Archiving, Radenci, Slovenia, 13–15 April 2016; pp. 481–491.