BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2024 • Vol. **81**, pp. 23-28
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.81.24.03

The Role of The Concept of Trust in Trust Services in Cyberspace to Enhance Cyber Security

Milen Gospodinov

University of Library Studies and Information Technologies,
119, Tsarigradsko shosse Blvd. 1784 Sofia, Bulgaria
Email: m.gospodinov@unibit.bg

Abstract: Trust services from Regulation (EU) No. 910/2014 is a cornerstone issue in enhancing cyber security. Building of trust in the online environment ensures legal security for users when using trust services. Achieving a higher level of cyber security can be achieved through technology in terms of the technical dimensions of the matter, and in legal terms through a trust service provider. Users need technical and legal security to be able to rely on the various services of the information society. They must have certainty in the specific technology used. Users should have the confidence that the technology is sufficiently protected from unregulated access and use to feel at ease when conducting electronic transactions in cyberspace. The persons using the trust services should be guided by the belief that the technology itself and the service provider have passed a complex check of the legally set conditions and that they meet the mandatory requirements according to Regulation (EU) No. 910/2014.

Keywords*:* *trust services; concept of trust; trust; cyber security*

1. Introduction

Digital transformation and cyber security are today's two most important prerequisites for achieving business success and sustainability. Digital transformation makes significant changes in various aspects of an organization and these changes can be measured through sets of indicators related to the stages of operational readiness, organizational readiness, and business value and return on investment [1]. On the other hand, the advent of digitization is related to the need to ensure the protection of information through the timely identification of various malicious software [2]. Another important direction is the development of

reliable identification of users to protect information [3] including information security and cybersecurity [4]. Nevertheless, these efforts, cyber security remains a challenge for e-commerce. In e-commerce, the most important is the role of trust in services and that is why the current article addresses some aspects of the concept of trust in trust services in cyberspace.

2. Regulatory Framework of Trust Services

Trust services from Regulation (EU) No. 910/2014 play an essential role in enhancing cyber security. The concept of trust occupies a central place because building trust in the online environment ensures legal security for users when using trust services. Achieving a higher level of cyber security can be achieved through technology in terms of the technical dimensions of the matter, and in legal terms through the trust service provider.

The normative basis of the trust service is Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of July 23, 2014, published by the European Commission in 2014, on electronic identification and trust services for electronic transactions in the internal market, commonly referred to as eIDAS (derived from the initial letters of the English name – electronic **ID**entification, **A**uthentication and trust **S**ervices**)**. The adoption of this regulation was dictated by the desire to build trust in the online environment because it is precisely the matter of trust that builds economic and social development. The aim is to provide citizens with trust services with a high level of legal certainty, and this, in turn, will ensure stability and peace of mind when conducting electronic transactions and generally facilitate electronic commerce. Regulation (EU) No. 910/2014 repeals the previously effective DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on the Community legal framework for electronic signatures. In the national Bulgarian legislation as an example of the legislation of EU country member, the Regulation was transposed into the Law on the Electronic Document and Electronic Trust Services, promulgated, SG No. 34 of 04/06/2001 (LEDETS) [5].

Article 3, item 16 of Regulation (EU) No. 910/2014 provides a legal definition for ordinary trust services and defines it as "an electronic service, usually provided for a fee, which consists of:

- the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered mail services, as well as certificates related to these services; or
- the creation, verification and validation of website certificates of authenticity; or

- the storage of electronic signatures, seals or certificates related to these services;"

As can be seen from the definition, trust services are characterized by several features. On the one hand, they are electronic services, which means that their distribution is only possible in electronic environment. On the other hand, trust services are for-profit legal transactions in which trust service providers provide their services to users, who in turn typically remunerate the providers for using the trust services.

Regulation (EU) No. 910/2014 unlike Directive 1999/93/EC, which is the foundation for the electronic signature, introduces many new institutes such as electronic seal, electronic identification, electronic time stamp, website authentication and electronic registered mail which increases the level of trust in cross-border electronic transactions in EU member states.

One of the key issues set out in the preamble of Regulation (EU) No. 910/2014 is about building trust in the online environment through the newly introduced trust services. The presence of trust increases the legal certainty when conducting electronic transactions by consumers.

Therefore, the Regulation sets a clear and specific goal – "to increase trust in electronic transactions in the internal market by providing a common basis for reliable electronic interaction between citizens, businesses and public authorities, which will increase the efficiency of public and private online services, e-business and e-commerce in the Union" [5]. The application of the concept of trust is particularly pronounced in certain types of institutes as electronic signatures and electronic seals, where it is a priority that users have full confidence on the one hand in the technology used, both in a technical and legal aspect, and on the other hand – in the provider of trust services.

3. The Concept of Trust

The concept of trust is a fundamental cornerstone upon which the use of trust services rests. The concept of trust has already been examined in detail in the context of the previously effective DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on the Community legal framework for electronic signatures [6]. For the current Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services in electronic transactions in the internal market, the consideration of the concept of trust is more than necessary. The concept of trust is of even greater importance when considering Regulation (EU) No. 910/2014 , because the previously effective DIRECTIVE 1999/93/EC regulated only electronic signatures and the

concept of trust service had a narrower meaning , using the English term “trust services” [7], and now “trust services” [5] is commonly used.

In e-commerce, where trust services are used, there are two main perspectives on trust [8, 9]. Although the concept of “trust” has been criticized by some authors as not robust enough to be amenable to regulation [10], the term has gained and continues to gain wider use because of its direct connection to trust services and trust service providers.

First and foremost is the bond between the trust and the trust service to which it belongs. “Trust mainly refers to the degree of perception in the security of the service provided. Trust and security in electronic transactions are considered fundamental in the development of electronic commerce and public administration operations. Users need technical and legal security to be able to rely on the various services of the information society” [11]”. In the online environment where communication takes place trust in e-commerce operations work in a similar way to the black box of aircraft: the user is confident, that the machine will record all processes and maintain enough evidence to be able to reproduce what really happened [12].

Second, users need to be confident in the specific technology being used. They should have the confidence that the technology is sufficiently protected from unregulated access and use to feel at ease conducting electronic transactions in an online environment. “Technical security mainly refers to the use of secure mechanisms that guarantee the authenticity and confidentiality of transactions (security protocols, passwords, trust services, etc.)” [11]. This type of trust is called by some researchers “technical trust” [13], as such the defined term covers a computerized system and its components, i.e. that the system works as expected (reliability), is protected against attacks (security) and protects the user's interests (safety) [13]. In contrast to the concept of “technical trust”, another concept of “organizational trust” has been introduced [13], which is expressed in the honest intentions and desire for cooperation of other participants/users of the system [13].

Next, trust has a direct relation to the trust service providers and their activities. Users should not feel vulnerable when carrying out electronic operations, and therefore strict rules have been introduced aimed at regulating the activity of trust service providers. The persons using the trust services should be guided by the belief that the technology itself and the service provider have passed a complex check of the legally defined conditions and that they meet the mandatory requirements according to Regulation (EU) No. 910/2014, they are duly certified, in cases where is necessary and the regulatory authorities monitor compliance and non-violation of regulatory requirements. An interesting question arises as to which provides a higher degree of trust in the relationship between trust service providers and their users – the trust authority's checks or the

responsibility that trust service providers bear for non-compliance with the relevant regulations. The answer to this question is rooted in “users' trust in providers and procedures, which is based primarily on trust authority verification and only secondarily on the responsibility of trust service providers for breaches of their legal obligations” [14].

4. Conclusion

The requirements that were discussed above, namely – the security of the technology and the reliability of the trust service providers must be cumulatively present in order to form user trust in the respective trust service.

The renowned researchers on Regulation (EU) No 910/2014 and Regulation (EU) No 910/2014 Jos Dimortier and Niels Vandesande in the consideration of the concept of trust in trust services, two parties are introduced: trustor and trustee [12] which are mainly relevant in clarifying the relationship between the provider of trust services and the users of the services. There is always a certain degree of risk-taking involved in making a particular transaction, and it is of utmost importance in this transaction that the fiduciary gives a level of trust to the transaction so that the other party can trust him [12].

Trust services, from a technical point of view, can be summarized as specific technologies that can be trusted so that they change the user's perception of the vulnerability of a process they are involved in. It is of paramount importance that the user can recognize the service as reliable enough to trust and benefit from it.

The concept of trust includes the question of establishing the authorship of a particular electronic statement and whether the same was sent by the alleged author, as well as whether the electronic statement was tampered with in any way after it was sent. Although legally binding electronic declarations of intent can be made informally over the Internet, they do not offer any legal certainty as to the authenticity and integrity of electronic documents [15]. In the very act of electronic communication, it cannot be technically guaranteed that the secrecy of that communication will be preserved, which again relates to the concept of trust. By building trust between users and trust service providers in the provision of electronic trust services, a high degree of security is guaranteed in the realization of electronic transactions in cyberspace and it is essential to ensure a high level of cyber security.

References

1. Borissova, D., Naidenov, N., Yoshinov, R.: Digital transformation assessment model based on indicators for operational and organizational readiness and business value. In: Guarda, T., Portela, F., Diaz-Nafria, J.M. (eds) ARTIIS 2023.

Communications in Computer and Information Science, 1935, 457–467, 2024, https://doi.org/10.1007/978-3-031-48858-0_36.
2. Borissova, D., Barzev, I., Yoshinov, R., Kotseva, M.: Group decision-making models for selection of virtual machine software for malware detection purposes. In: 12th MECO, Budva, Montenegro, 2023, 1–5, https://doi.org/10.1109/MECO58584.2023.10155084.
3. Yoshinov, R., Iliev, O.: Sharing local resources within a community by enhancing the potential of Eduroam and EduVPN with mobile application for remote and local resources and through secure user identification over the network (MARLIN). Problems of Engineering Cybernetics and Robotics, 79, 3–36, 2023, https://doi.org/10.7546/PECR.79.23.01.
4. Gaidarski, I., Kutinchev, P.: Some aspects of information security and cybersecurity problem area. Problems of Engineering Cybernetics and Robotics, 79, 55–66, 2023, https://doi.org/10.7546/PECR.79.23.03.
5. Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and authentication services for electronic transactions in the internal market.
6. Dimitrov, G.: Liability of Certification Service Providers. VDM Verlag Dr. Mueller, Saarbruecken, 2013.
7. DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
8. Ratnasingham, P.: Trust in Web-based electronic commerce security. Information Management & Computer Security, 6(4), 162–166, 1998, https://doi.org/10.1108/09685229810227667.
9. McCullagh, A. E-commerce: It Is a Matter of Trust. https://cyber.harvard.edu/trusting/mccullough.html.
10. Sosna, S.: EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten: eIDAS-Verordnung. – ein Überblick über die wichtigsten Inhalte underen Konsequenten für Unternehmen. In: Computer und Recht, 30(12), 825–832, 2014.
11. Rico Carrillo, M.- El Reglamento europeo sobre identificación y servicios de confianza electronicos. Revista General de Derecho Europeo, p. 24, 2015.
12. Dumortier, J., Vandezande, N.: Trust in the proposed EU regulation on trust services? Computer Law & Security Review, 28(5), 568–576, 2012, https://doi.org/10.1016/j.clsr.2012.07.010.
13. Ølnes, J.: A Taxonomy for Trusted Services. In B. Schmid, K. Stanoevska Slabeva, V. Tschammer (Eds.), Towards the E-Society: E-Commerce, E-Business, and E-Government, 74, 31–44, 2001.
14. Schlauri, S.: Elektronische Signaturen. Dissertation der Rechtswissenschaftlichen Fakultät der Universität Zürich zur Erlangung der Würde eines Doktors der Rechtswissenschaft, Zürich, 2002.
15. Grigorjew, O.: Beweiseignung fortgeschrittener elektronische Signaturen, Kassel, ISBN 9783862199600, 2015.