MULTI PARTY SIGNATURES AND ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Václav Stupka / Pavel Loutocký / Antonín Dufka / Petr Švenda

Václav Stupka, Ph.D., postdoc researcher; Masaryk University, Faculty of Informatics, Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: vaclav.stupka@law.muni.cz;

Pavel Loutocký, Ph.D., postdoc researcher; Masaryk University, Faculty of Informatics, Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: pavel.loutocky@law.muni.cz;

Antonín Dufka, Mgr., doctoral researcher, Masaryk University, Faculty of Informatics; Botanická 68a, Brno, CZ; e-mail: xdufka1@fi.muni.cz

Petr Švenda, Ph.D., associate professor, Masaryk University, Faculty of Informatics; Botanická 68a, Brno, CZ; e-mail: svenda@fi.muni.cz

Keywords: ***criminal procedure, cryptography, multiparty computing, electronic evidence, chain of custody***

Abstract: *This paper is devoted to a legal analysis of the possible use of multiparty threshold cryptographic protocols in the handling of electronic evidence in criminal proceedings. In contrast to standard digital signing, multiparty protocols require participation of more than one party to create resulting electronic signature. In the context of criminal proceedings, such signatures can be used to sign documents or data multilaterally to ensure confidentiality and reliability of the chain of custody, in procedural acts and in the transmission of documents. In this article, we describe the functioning of the technology and the technical limits of its use, analyse the nature of signatures generated by it from the perspective of EU law and the possibilities of using this technology in criminal proceedings, taking into account the specifics, practices and limitations of the Czech legal environment.*

1. Introduction[1]

As a result of the increasing penetration of technology into all activities of human society, electronic evidence is increasingly being used in criminal proceedings. When dealing with electronic evidence, which is often of a non-material nature, law enforcement authorities must regulate the procedures in place. This can often lead to inefficiencies in the process or even reduce the reliability of evidence and legal certainty. It is therefore advisable to look for tools and procedures which, taking into account the nature of electronic evidence, can ensure a high level of integrity and confidentiality of the evidence and a high level of efficiency in the evidentiary process. This paper therefore explores the possibilities and advantages of using multi-party signatures in criminal proceedings. This technology brings new possibilities for handling and accessing data and for ensuring the integrity and authenticity of digital evidence. In this article, we explain the technology, analyse its legal nature, and identify parts of the criminal proceedings where the use of this technology would be potentially beneficial.

[1] This article is a result of a research project no. VJ01010084 Electronic evidence in criminal proceedings, which was supported by the Ministry of interior of the Czech Republic in a project scheme Strategic support of the security research 2019 – 2025 (IMPAKT-1). This article expresses opinions of the authors and the project team, these are not the opinions of the institutions the authors represent nor the Ministry of interior.

2. Multi-party signatures

In cryptography, multi-party signatures (MS) are a type of digital signature, which is constructed using multiple keys, and without which it cannot be created. This type of signature satisfies all the properties required from standard (single-party) digital signatures. In fact, a multi-signature can be represented as a regular electronic signature (e.g., RSA or ECDSA signature), with the only difference being that instead of a single signing key, multiple keys have been used during its construction.

Multi-party signatures can also be constructed in a threshold mode, in which a parameter called *threshold* is set when the keys are created. The parameter specifies the minimal number of keys that are required to create a signature. Whether the signing parties can be identified among the eligible signers depends on a particular multi-party signature construction.

Construction of multi-party signatures

To analyze the legal nature of multi-party signatures, we divide them into three classes based on their construction and properties.

Simple multi-party signatures. The simplest way of constructing multi-party signatures is to join multiple single-party signatures of a document into a single object. To verify such a signature, the verification software needs to be provided with public keys (or certificates) of all the signing parties, verify the included signatures individually, and signal validity whenever there have been included more valid signatures than the required threshold. Disadvantages of this approach are that the resulting signatures are not compatible with software designed only for single-party signatures, and the signature size and its verification time depend on the number of signing keys.

Threshold multi-party signatures. An alternative construction approach is based on techniques from the field of threshold cryptography[2]. Multi-party signatures created using threshold cryptography provide several benefits over the simple construction. These multi-party signatures can be represented as a standard singleparty signature (e.g., ECDSA or RSA) yet they required multiple parties to participate in their construction. The verification of such signatures is very efficient, as it requires only a single public key corresponding to the joint signature that can be found either in joint certificate or constructed from individual certificates. However, if the signing threshold does not require all eligible parties to partake, it is no longer identifiable which parties from the eligible signers did not partake (or equivalently, which did).

Accountable multi-party signatures. Cryptography also provides approaches for constructing multi-party signatures that can identify all signers and are more efficient than simple multi-party signatures[3], yet they are also not compatible with standard signature formats. The verification of such signatures is also efficient but can no longer rely on standard, widely used algorithms.

Usage scenarios

Multi-party signatures can be used in various setups, differing in how many keys are constructed, the required threshold for successful signing, and how individual keys are controlled. The following paragraphs discuss practical settings for the use of multi-party signatures.

Two persons, both required. In this scenario, there are two keys, each of which is held by a different person. If both persons participate in document signing, they are able to create a valid signature and thus express their

[2] See Desmedt, Y.G. (1994), Threshold cryptography. Eur. Trans. Telecomm., 5: 449–458. https://doi.org/10.1002/ett.4460050407.

[3] See Silvio Micali, Kazuo Ohta, and Leonid Reyzin. 2001. Accountable-subgroup multisignatures: extended abstract. In Proceedings of the 8th ACM conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, USA, 245–254. https://doi.org/10.1145/501983.502017.

joint agreement with the document. This setup can be used in cases that require the agreement of two parties. For example, to sign a document by both company co-owners or to sign an employment contract by an employee and the employer.

Three persons, two required. In this scenario, three persons own keys, but only two of them have to partake to create a signature. With the use of threshold multi-party signatures, the party that did not participate in signing is not identifiable. This setup may be considered in situations where a majority vote is needed. For example, if two of the three company owners suffice to perform some act, they can demonstrate their agreement by issuing this type of signature.

Single person with automated signing device. In this scenario, a single person holds one key, and the other one is stored on a remote server that cosigns according to some policy. The main advantage of this approach over single-party signing is its security, as the signature construction requires both keys. For example, the automated signing device can enforce compliance with some policy before the signature can be issued. Furthermore, this setting eliminates the need for certificate revocation lists, as the signatures cannot be created when one of the parties disallows it.

Two persons, one automated device, two required. In this scenario, there are three keys, two of which are held by persons, and the third one is operated by an automated device acting according to a policy. This setup can create a valid signature in two cases: when one of the persons signs jointly with the automated device and when two persons create the signature jointly.

Key protection. Threshold signatures can also be used by a single person who divides their key among multiple devices under its control. The benefits of this approach are two-fold: security and resilience. Unless more than a threshold of devices gets compromised, an attacker cannot create signatures, thus increasing security. Furthermore, unless more than a certain number of signing devices become inaccessible, the signer is still able to create signatures with the remaining devices, thus improving resilience against device loss.

Other scenarios can be considered generalizations of those that were discussed.

3. Legal nature of multi-party electronic signatures

The technical design and possible scenarios relevant for multi-party signatures have been described above. However, from a legal point of view, it is important to assess whether such a signing method is relevant when assessing legal acting, and thus it is necessary to examine whether and how the legal definition of what can be considered an electronic signature is met.

The electronic signatures are primarily codified in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("the eIDAS Regulation"). A „simple" electronic signature, as the lowest level of this instrument, is defined in Article 3(10) as „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". This definition shows that such type of the signature can cover very broad situations. Furthermore, this legislation introduces an advanced electronic signature which should already identify the signatory, be inextricably linked to him, be under his exclusive control and be protected against alteration of data.[4] The highest level of signature is a qualified electronic signature, which, unlike an advanced electronic signature, is based on recognised certified procedures and reliably proves the identity of the person and the data inserted in the certificate.[5]

[4] See Art. 26 of the eIDAS Regulation.

[5] For the definition see more in Art. 3 point 12) of the eIDAS Regulation.

However, it is questionable whether the above-presented multi-party signatures are able to fulfil the required legal features and can be considered as a kind of electronic signature in the context of legal relevance. Consequently, we proceed to evaluate the different scenarios in light of the legal regulation contained in the eIDAS Regulation. In general, however, it should be noted that it will always be necessary to assess whether a given scenario allows the signature to be used by the signatory (in the case of a „simple" electronic signature) or whether it then presents the possibility of identifying the signatory (whether on the basis of a privately chosen approach – an advanced electronic signature – or on the basis of a certified scheme – a qualified electronic signature).

Two persons, both required. If both signatures are merged, a signature that still carries the information about the signers (if any) is generated. It must be noted in the context of this procedure (and many other stated below) that the signing method must be considered not only as a „simple" electronic signature, from the described technological approach (a private certificate is used for signing the given signature), the conditions of an advanced electronic signature will be also met (the technology used actually aims primarily at this level of signature).

Three persons, two required. In this scenario, the situation may be more complicated, given that the signature does not necessarily represent (and does not represent) the will of all signatories. This case can be further divided into two possible situations. In the first case and according to the technological settings of the signature, it may not be possible to determine who signed in the resulting signature (there will be a "merging" of identities). In this case, the definition of the signature at any level will not be fulfilled and it will not be possible to determine who has legally acted in what way (the resulting multi-party signature will not be complete, and it will not be possible to state at least for some persons that they can be identified, and the signature is inextricably or anyhow else linked to them). In the second case, (due to the technological setting) it will be possible to identify the persons acting from the resulting signature, in which case the requirements even for an advanced electronic signature will be met.

Single person with automated signing device. In the case of this use of multi-party signatures, it should be noted that the legislation contained in the eIDAS Regulation is intended to be technology neutral, i.e., it is not specified how exactly to approach the design (although standards and security are moving towards asymmetric cryptography). Thus, if the signing takes place at the moment when the will of the signatory is linked to the activity of the machine, this does not contradict the definition of an electronic signature, even at the level of an advanced electronic signature. In the specific case, it should be noted that there is already a scheme based on this approach which is certified to the level of a qualified electronic signature on the basis of the eIDAS Regulation – this is the Estonian provider SK ID Solutions AS, which offers Smart-ID[6].[7]

Two persons, one automated device, two required. This scenario can be seen as a modification and linking of the second and third scenarios. As a result, if it is possible to identify the signing person (either one or both) after linking their parts into one signature, it will be seen as an advanced electronic signature. If, however by technological setting it is not possible to assess, who signed (as the separate certificate merged and blurred) the same the pitfalls mentioned for the *Three persons, two required* scenario are relevant.

Key protection. The use of threshold signatures for splitting a key of single person among multiple devices seems to us to be highly practical from a legal perspective. On the one hand, it can be considered that the definition of higher levels of signature will be fulfilled (and thus the scheme can also be certified), and on the other hand, it provides an increased level of security compared to existing approaches at higher levels.

The scenarios outlined above, which have been analysed on the basis of the legal regulation contained in the eIDAS Regulation, show that it is generally possible to meet the legal definition even of an advanced electron-

6 See https://www.smart-id.com/.

7 This particular certificate is issued by: EID-SK 2016 qualified certificates for electronic signatures.

ic signature in most cases within the multi-party signatures approach (for summary of the analysis see Table 1. This way of signing is thus very promising not only in terms of the use of specific technological solutions but also in terms of legal relevance. If the multi-party signature is appropriately constructed (according to the specifics defined above), this supports wider possibilities of its use also in terms of legal aspects and even to think about the possibilities leading to have it as qualified electronic signature (if the certification scheme is relevant for such approach).

	n-of-n persons	*t-of-n persons*	*n-of-n person + device*	*t-of-n persons + devices*	*Key protection*
Simple MS	AdES+	AdES+	AdES+	AdES+	AdES+
Threshold MS	AdES+	X	AdES+	X	AdES+
Accountable MS	AdES+	AdES+	AdES+	AdES+	AdES+

Table 1: Achievable level of electronic signature for given setup depending on multi-party signature construction. AdES+ denotes the level of advanced electronic signature or higher. Parameter n is the number of parties and $t < n$ is the threshold.

4. Technologies for digital evidence handling in criminal procedure

Currently, the circulation of documents between the individual participants in the criminal procedure is often carried out through paper documents or poorly secured emails; the transfer of evidence is traditionally carried out on physical media and, to a lesser extent, electronically according to the mechanisms set up between the individual stakeholders (i.e., ISPs and law enforcement authorities). In cross-border transfers, the situation is no better when requests for international judicial cooperation, investigation orders or electronic evidence are transmitted physically, by fax, email, and other legacy tools.

This situation is problematic for several reasons. The first is security – some of the methods of transferring documents and evidence are completely inappropriate as they do not meet any of the three requirements of the security triad. Confidentiality is not assured in the case of analogue communication via email or fax, and verification of the sender's identity by traditional methods is inadequate in this day and age of phishing. Nor is the integrity of documents and evidence transmitted through unsecured channels as they may be altered or replaced during transfer. Another reason is speed – the transfer of electronic data and documents by traditional criminal justice methods is lengthy and requires complicated verification processes. This issue is particularly crucial in relation to electronic evidence, which is highly volatile and speed in securing it is a major prerequisite for the success of an investigation. Compatibility is also relevant in international cooperation – authentication mechanisms, requirements for security standards or the technologies used may differ from country to country, which can complicate or slow down cooperation.

Efforts to address these shortcomings exist, for example in the form of projects aimed at developing appropriate technical tools. An example is the EU Evidence project[8], which aimed, among other things, to create a tool for the transfer of data and documents[9]. However, the prototype tool developed has not been widely used. It envisaged the deployment of a new solution that interfered with existing processes and the use of dedicated infrastructure.

[8] See http://www.evidenceproject.eu.

[9] See description of the tool and its architecture in the project deliverable here: http://s.evidenceproject.eu/p/e/v/evidencega-608185-d5-2-416.pdf.

5. Multi-party signatures use cases

Based on the analysis above it is safe to state, that the technology of multi-party signatures is not only at a high technological and security level, but its parameters also meet the requirements set for the highest level of security and signing standard recognized by the EU legislation. Another clear advantage is that it is not necessary to build any complicated infrastructure to use this technology and that it is compatible with current tools used for electronic documents and signatures. In addition, individual scenarios of its use offer specific features that are useful in ensuring a high level of reliability and evidentiary value of digital evidence and security of communication within the criminal procedure. Let's explore possible use cases for individual usage scenarios.

Two persons, both required. There are several procedures in criminal proceedings that require counter-signing, or a multi-party decision. If a procedural action of the law enforcement authorities is to be carried out, it is often necessary that its execution is approved or ordered, for example, by the public prosecutor or the supervising judge. The use of the multi-party digital signatures for approving a decision or order to carry out an investigative measure would ensure a high level of reliability of the process, integrity of the signed documents, the possibility of verifying their authenticity and, at the same time, the swiftness and flexibility of the approval process. A higher level of efficiency would therefore be achieved without loss of quality and security, which is a particularly important factor affecting the success of criminal proceedings when securing volatile electronic evidence. A significant advantage is that the signature generated in this way is easily verifiable by anyone (i.e., by obliged persons, their legal representatives etc.) using common tools available for working with electronic signatures implemented in the most common office applications.

Three persons, two required. This scenario is usable for similar purposes as the previous one, i.e., mainly for secure signing of countersigned documents. However, it has the advantage of implicitly allowing substitutability due to its architecture. Suppose that a warrant for the seizure of evidence during a search must be signed by a prosecutor and a judge at the same time. However, the judge is not on the spot and not available at the time; the decision could be made by a substitute judge in such a case. Using multiple signatures via web or mobile apps would then make the whole process transparent, efficient, and secure.

Single/multiple persons with automated signing device. This scenario can also be effectively applied in criminal proceedings, especially where there is a need for securing automatically generated data against tampering or access control. The first case may arise in the need of the increasingly discussed use of automated extraction or analytical forensic tools directly by the investigator without the involvement of a forensic expert[10]. For example, when securing evidence at the scene, the image of the secured data may be automatically secured by the extraction tool used and subsequently signed by the investigator who used the tool. Similarly, when an automated analytical tool is used to perform forensic data analysis, its output may be secured in this manner. The advantage of this procedure is that the integrity of the evidence will be assured against any interference by the investigator or the user of the forensic tools, thus strengthening the evidentiary value of the evidence thus produced. As an indirect consequence, the criminal process may be less dependent on the availability and capacity of forensic experts, who usually guarantee the integrity of the evidence, but whose expertise is not necessary for some standard forensic tasks. The second case can be implemented in the transfer of evidence. For example, when the seized data is handed over by the service provider to law enforcement authorities, or to a forensic expert. In practice, there is often no uniform approach or tool for such transfers, but the transfer often takes place via online shared data storage. The use of "*n of n – person + device "* scenario can be used for identification and authentication of the access to the respective data source. In this use case, an investigator or an expert can use his/her signature to try to access the relevant data source, the system identifies him/her by means of a partial signature and verifies whether the relevant person has access rights, and only then

[10] On the discussion about the need for police investigators to be able to use forensic tools please see ie. Belshaw, Scott H. (2019) "Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education," Journal of Cybersecurity Education, Research and Practice: Vol. 2019: No. 1, Article 3. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/3.

the signature gets completed by automated counter-signing by the system which allows the decryption and access to the relevant data.

Key protection. This usage scenario is basically an extension of previous use cases implementing multi-factor authentication, which is not commonly used in the electronic signing process. In criminal proceedings, very sensitive information is handled and the impact of compromising the authentication process would therefore be significant. The possibility of using multi-factor authentication would be therefore highly beneficial.

6. Conclusions

The use of modern ICT tools in traditional criminal procedures has the potential to contribute to solving some of the challenges arising from technological developments and the increasing use of electronic evidence. The processing such evidence requires ensuring its integrity throughout the chain of custody and the confidentiality and availability of the tools used for its processing, as well as the efficiency and speed of securing and processing this highly volatile type of evidence.

One of these tools may be the use of multiparty threshold cryptographic protocols to process documents and control access to electronic evidence. In this paper, we therefore describe the nature of this technology and describe scenarios of its practical use. Subsequently, we analyse its nature in terms of the legal regulation of electronic identification and trust services in EU legislation and identify possible scenarios for the use of this technology in criminal proceedings.

Based on these analyses, it can be concluded that the use of this technology has a high potential to bring a high level of flexibility and efficiency to the processes of electronic evidence and to contribute and to contribute to achieving high credibility and reliability of the evidence produced. However, the deployment of these tools in practice will clearly be a challenge both for the criminal process and for the law enforcement authorities themselves. However, the high potential of their use should be a great motivation for the relevant authorities to discuss the ways and possibilities of their deployment.

Above all, this article is a contribution to the discussion on the possibilities of using modern technologies in traditional processes of authoritative application of law, which sooner or later will have to adapt to the social and technological realities of today's information society.