Guidelines concerning the provision of the on-line electronic signature verification service

Revision 5.1

Issue date: 13.05.2020.

MADKOM SA
Al. Zwycięstwa 96/ 98
81-451 Gdynia
Poland

Contents list

1. Introduction

The Guidelines concerning the provision of the on-line electronic signature verification service (referred to in the text as the Guidelines), remaining in line with the requirements of the Polish act of September 5th, 2016, on trust services and electronic identification, describe the type, scope, technical and organisational solutions of the provided non-qualified on-line services spanning the verification of electronic signatures and electronic stamps by MADKOM SA. The activity of MADKOM SA within the scope of the provided services is based on legal provisions presently in force in the Republic of Poland.

2. Terms and definitions

Trust services supplier – entity recorded in the public register of trust service providers kept by the Polish Minister responsible for issues of digitalisation

Electronic verification confirmation (EVC) – document containing the complete result of verification of the electronic signature or electronic stamp including the date and time of generation along with a unique verification identifier.

Guidelines – the present document entitled *Guidelines concerning the provision of the on-line electronic signature verification service*

Electronic service provision – execution of a provided service without the presence of the parties (e. g. remote execution), by way of transmission of data at the individual request of the User, transmitted and received through the use of electronic data processing devices, together with digital compression and data storage, which is sent, received or transmitted in its entirety via a telecommunications network as understood by the Polish act of July 16th, 2004 – Telecommunications law.

Verification identifier – a marker allowing the confirmation of correctness and truth of the EVC and allowing the re-creation of the verification result.

Services – services provided electronically pursuant to the present Guidelines.

User – an entity using the Services, or one with whom an electronic service provision contract was concluded.

Service provider – the company MADKOM SA.

3. Legal foundations for the provision of the Services

The provision of Services is effected taking into account the following intra-community and domestic regulations:

- the Polish act of July 18th, 2002, on the electronic provision of services (e. g. Polish Journal of Laws of 2013, item no. 1422, as amended)
- Regulation (EU) 2016/ 679 of the European Parliament and of the Council of April 27th, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (GDPR)
- 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 (eIDAS)
- the Polish act of September 5th, 2016, on trust services and electronic identification (e. g. Polish Journal of Laws of 2019, item no. 162)
- the Polish act of May 10th, 2018, on personal data protection (e. g. Polish Journal of Laws of 2019, item no. 1781)

- the Polish act of February 17th, 2005, on the introduction of digital solutions to entities providing public services (Polish Journal of Laws of 2005, no. 64, item no. 565)
- the Polish act of July 16th, 2004, telecommunications law (e. g. Polish Journal of Laws of 2018, item no. 1954, as amended)
- the Polish act of September 6th, 2001, on access to public information (e. g. Polish Journal of Laws of 2019, item no. 1429)

MADKOM SA is the Supplier of trust services and operates in line with the law in force in the Republic of Poland, on the basis of its registration in the register of non-qualified Suppliers of trust services kept by the Polish National Certification Centre spanning the verification of certificate status as item no. 1, acquired on May 16th, 2017.

4. Types and scope of provision of trust services

The Service provider provides the following trust services
a) Electronic signature verification service
b) Electronic verification confirmation authenticity certification service

The services are provided with the aid of a website and network services. The system fulfils the requirements of the eIDAS directive and uses the EU Trust Service List (TSL) for signature verification.

a. Electronic signature verification service

The electronic signature verification service is characterised by properties described in detail in the table below.

Service access	https://verifysignature.eu
Supported signature and stamp formats	XAdES – ETSI EN 319 132 PAdES – ETSI EN 319 142 CAdES – ETSI EN 319 122 ASiC – ETSI EN 319 162
Signature profiles	XAdES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA PAdES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA CAdES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA
Trust Service Lists	TSL per ETSI TS 119612
On-line certification status	CRL OCSP
Profile extensions	XAdES: - enveloping - enveloped - detached CAdES: - enveloping - detached PAdES: - enveloping ASiC: - ASiCS:XAdES - ASiCE:XAdES

Time stamp verification	Yes
Recreation of certification path for signature certificates	Yes
Recreation of certification path for time stamps	Yes
EVC formats	JSON file PDf file HTML file
Abbreviation function algorithms	SHA-1, SHA-256, SHA-384, SHA-512
Signature algorithms	RSA, RSA-MGF1, DSA
Signed data integrity control	Yes
Detection of SHA-1 collision attacks	Yes
Maximum number of simultaneously verified files	No restriction
Signing certificate verification status	Positive Conditionally positive Negative

The result of verification of the electronic signature and stamp varies over time due to the expiry of validity of data used to affix signatures, stamps and time stamps. Hence, for proof purposes, the system generates electronic verification confirmations that the user may store. The EVC contains a unique verification identifier allowing users to verify the content of the verification result from the time of verification.

NOTE: If the electronic signature or stamp contains a time stamp, then the verification is performed for the time included in the time stamp, else – for the present moment.

b. Electronic verification confirmation authenticity certification service

The service allows the acquisition of certification of authenticity for the EVC through the acquisition of access to the full verification result, exclusively through the use of a unique verification identifier. This allows for the recreation of the result of verification from the moment of verification of the signature and stamp, for which the user holds their verification identifier.

5. Signature and electronic stamp verification result

As a result of the conducted verification of the electronic signature and stamp, the system presents the following data for every signature and every stamp separately:

Basic data	
File name	The name of the file, in which in course of verification at least one electronic signature (or stamp) was found.
Integrity	The result of verification of the integrity of the signed data.
Signing party	The data contained in the common name of the certification of the signing entity or the identifier of the entity using the trusted profile for trusted signatures (Poland only) and the name of the signing party for personal signatures (Poland only).
Authentication type	Information about the type of the electronic signature, for trusted signatures additionally the common name of the electronic stamp.
Declared signature affixing time	Declared time of signing/ affixing of the stamp, from the signing device, contained in the content of the electronic signature along with an information on the time in the proper time zone of the verifying user.

Detail data	
Abbreviation function	The abbreviation function used in the signature/ stamp, e. g. SHA-256, represented as a label.
Signature/ stamp profile	Signature/ stamp profile, see table under heading 4.a.
Signing party	Data contained in the common name of the certificate of the signing entity or the identifier of the entity using the Trusted Profile for trusted profiles (Poland only) and the name of the signing party for personal signatures (Poland only).
Declared signature affixing time	Declared time of signing/ affixing of the stamp, from the signing device, contained in the content of the electronic signature along with an information on the time in the proper time zone of the verifying user.
Authentication type	Information on the type of electronic signature, in case of trusted signatures additionally the common name of the electronic stamp.
Document/ file signed	Information on the signed document, including the file name, external file name (if signed) and information on the number of the signed revision for PDaES signatures.
Reason	Detailed information for the reason of lack of positive verification.
Trusted signature	If applicable, the following data is presented: Trusted Profile account identifier, first name, last name, PESEL personal identification number (Poland only).
Time stamp	The time indicated in the time stamp along with the information about the time in the correct time zone of the verifying user, the time stamp type, the issuer of the time stamp and the stamp verification result.
Signing party certificate	Data contained in the public key certificate, including: the common name, organisation, the country, serial number, the name of the issuing entity, the information on the trusted or non-trusted issuer (TSL), the certificate status, the certificate validity period, the information on the result of the verification of the status of the CRL and OCSP certificates.
Signature components	Reference list for components covered by the signature/ stamp, including identifiers and file names, results of verifications of the signature and of the data included in the certificate.
Full certification path	As under 'Signing party certificate' for all higher-order certificates.
Full certification path for the time stamp	As for the time stamp.

NOTE: The interpretation of the electronic signature, stamp and time stamp verification result depends only and exclusively on the User.

6. Data processing, including personal data processing

The services provided by the Service provider pursuant to the present Guidelines are provided for the benefit of Users on the basis of data acquired from them, which are processed by the resources of the Service provider.

The issue of data processing, including with respect to personal data, on end user devices, was covered in the Privacy policy under https://verifysignature.eu/cookies.

The Controller of data processed as part of the provided services is:

> MADKOM SA with seat in Gdynia, Poland (81-451), address Aleja Zwycięstwa 96/98, registered with the district court Gdańsk Północ, 8th commercial department of the Polish National Court Register, KRS (court register no.): 0000394954; NIP (tax identification) no.: 586-227-27-56; REGON (statistical) no.: 221508925, with which contact can be initiated at the data indicated above or via e-mail at madkom@madkom.pl.

The Controller had appointed a personal data protection inspector representative, with whom contact can be made at the address of the Controller or by e-mail at iod@madkom.pl.

COLLECTION AND PROCESSING OF DATA AS PART OF THE PROVIDED SERVICES – SCOPE, PURPOSE, BASIS, TIME

The administrator processes the data of the service users (server log and cookies, although it is not true data thanks to which Madkom SA can independently identify a specific natural person), including data transmitted via the contact form, which you can use to contact the service provider. contact (data such as name, surname, telephone number or email address is provided in this way).

In the scope of the Services, the Administrator processes data, including personal data contained in files sent to the Administrator's resources by Website Users who want to use the Services and these are the data contained in the submitted files to verify the signatures and electronic seals stored in them. The scope of data entrusted for processing depends only on Users. Users using the service available generally by sending files that will be processed to obtain the result of verification do so by accepting the Policy of providing services and the Privacy Policy in force on the website. Processed documents as part of the service are not collected by Madkom SA, but as part of the service they are processed, and after verifying the signature (s) they are deleted immediately. It is also possible to use the service via the API (application programming interface) - in this case the service is terminated based on the Personal Data Processing Agreement.

The data processing processes take place without human interference, i.e. at no stage of the service the Service Recipient's data are not processed by human. The data used in the processes of providing services are deleted from the Administrator's resources immediately after the services have been provided. However, the Administrator's resources still include the results obtained as part of the implementation of electronic signature verification services, enabling later verification of the authenticity of the verification certificate issued by the Electric System, including public data from the certificate that may contain personal data.

The full verification result containing all data from the signing certificates of the verification of the authenticity of the Electronic Verification Confirmation is stored for a period of 20 years, because the electronic document, which is created as a document of legal action, is signed with an electronic signature (similar to a paper document signed with a pen). The attestation may be used in redress processes where the full verification result may be necessary. After this time, the verification result will still be stored and available in the verification history, but without the signer's personal data (including names, surnames, numbers containing PESEL), which will be deleted by us. It will still provide the opportunity to confirm the veracity and certainty of the verification certificate, as it will contain the most important information, i.e. the status of the signature's validity and other data regarding the result of verification of the electronic signature.

DATA RECIPIENTS

The recipients of the data, including of personal data, upon whom the Controller may bestow data, shall be providers of legal and information services, including entities dealing with the hosting (storage) of data for the Controller. The recipients of data, whom the Controller may provide data, are public administration

bodies.

The data collected by us, including personal data, is not transferred to international organisations or to third countries. Personal data may be processed by other entities in line with EU or national law.

7. Obligations and liability

a. Obligations in terms of the provided services

The service provider guarantees that the Services are provided in line with the present Guideline. In addition, the organisation has implemented operation procedures and security management procedures that exclude any possibility of manipulation of the verification result. For this purpose, the Service provider has implemented and certified a Security Management System in line with ISO/IEC 27001.

b. Liabilities and obligations of MADKOM SA

The Service provider states that their activity as well as the provided services are lawful, and that in particular they do not violate the copyrights or licence rights of third parties, and that they employ persons having knowledge, qualifications and experience relevant for the execution of functions related to the provided services, including covering the following fields:

- automatic data processing in telecomputer networks and systems
- network and telecomputer systems security mechanisms
- hardware and software used for electronic data processing.

The Service provider ensures personal data processing security pursuant to Regulation (EU) 2016/ 679 of the European Parliament and of the Council of April 27th, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation).

The Service provider is not liable for damages and difficulties in operation of the Service. MADKOM SA is also not liable for temporary or permanent suspension of service availability, in particular damages or difficulties due to connection breakdowns or insufficient throughput of the service recipient.

The scope of liability related to the present Guidelines with respect to Users is limited to damage due to malice or neglect, unless common provisions of the law would state otherwise.

The Service provider is not liable for damage emerging as a result of usage of the Services if the Users are informed beforehand about the limitations in the provided services, and if these limitations may be recognised by Users.

The Service provider is not liable for damages due to User failure to adhere to the rules set out in the present Guidelines.

c. Dispute resolution

In case of submission of complaints or the emergence of disputes related to the usage of the Services, the Service provider will strive to achieve amicable settlement on the basis of written information.

When submitting damages, the burden of proof of the Service providers will or neglect rests with the User notifying the damage.

In case of failure to resolve disputes through mediation as well as in cases not governed by the provisions of the present Guidelines or individual contracts, the provisions of the law of Poland apply.

8. Fees

The services covered by the present Guidelines are free of charge, save for individually concluded contracts.

9. Event registration

For the purpose of supervision of efficient execution of Services and for the purpose of settlement of the activity of Users and service provider employees for their actions, the system registers all those events and activities that could have a material influence on the security of operation of the system and the Services provided therein. The event register may only and exclusively be viewed by authorised Service provider employees, and event register entries cannot be modified.

All documents transferred for verification by Users are removed immediately upon execution of verification.

10. Communication security

Communication between the computer of the User and the service server is encrypted through the SSL (Secure Socket layer). The SSL protocol is a type of security protection measure entailing the encrypting of data before its transmission from the user's browser and decoding it upon safe arrival at the server. The information sent from the server to the customer is also encrypted, to be decoded upon arrival. The SSL protocol encrypts, authorises and ensures integrity of messages.

11. Conclusion of activity or conclusion of service provision

Should services described in the present Guidelines cease to be offered, the Service provider shall make every effort to limit damage to Users. In case of emergence of such a situation, an information on the conclusion of activity shall be published with the required notice period, and users, with whom at that time commercial contracts shall be in force, shall be notified both by way of authorised e-mail as well as through traditional mail in due course (in line with the provisions of the individual contract).

12. Policy management

The policy document has versions for traceability, and every subsequent version of the Guidelines enters into force the moment it is approved and published. The reasons for the issue of subsequent document versions may be updates or errors present in the current version. Any new version in development is a 'document in progress' and is drawn up only and exclusively by authorised employees of the Service provider. The document is approved by the Chairman of the board of MADKOM SA.

13. Information security

MADKOM SA guarantees that all information held by it is collected, stored and processed in line with the present provisions of the law in this regard. The usage of the highest security standards for information is confirmed by MADKOM SA holding the current information security certificate per PN-ISO/ IEC 2 27001.

14. Document history

Date/ issue	Change description
05.2017./ issue 1	New document revision
10.2017/ issue 2	Update – service name change
01.2018/ issue 3	Update – service name change
06.2019/ issue 3.2	Update - correction
19.09.2019./ issue 4	Guideline update in terms of provided non-qualified services.
15.11.2019./ issue 5	Guideline update in terms of the website's currency.
13.05.2020./ issue 5.1	Update to clarify the period of personal data processing.