Central Cencert Registration Point
tel. 22 720 79 55 | 666 028 044
Jagiellońska 78 03-301 Warsaw, 2nd floor, room 345

Contents of the GetValid Qualified Validation Service report

Table of contents

1. INTRODUCTION

This document describes the content of the GetValid validation report that presents the results of validation of electronic signatures and seals of an electronic document.

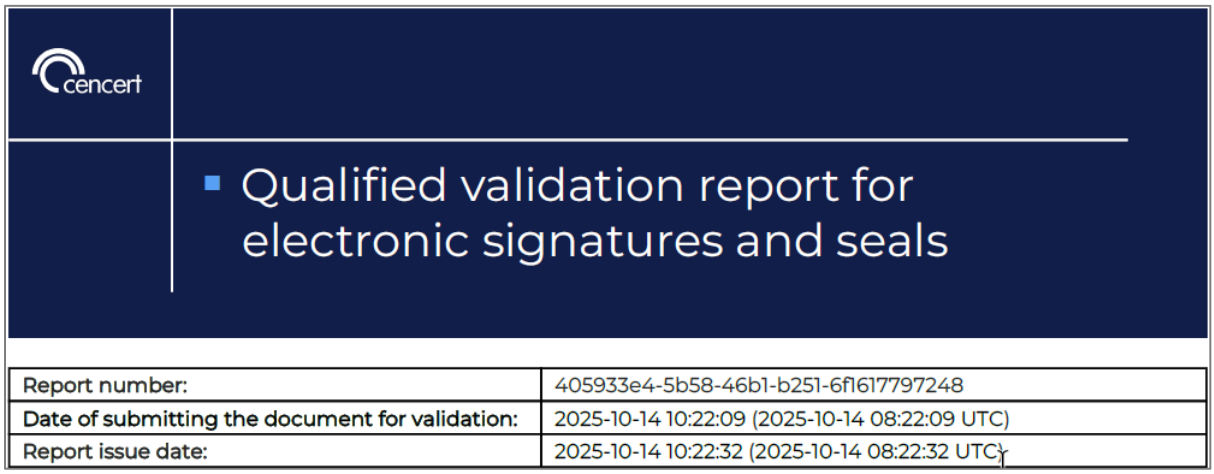
The description is presented on the example of the original report, for which the possible content and meaning of individual fields of the report are presented and discussed.

Since there are no technical differences between an electronic signature and an electronic seal, all information relating to signatures also applies to the seal, unless the content of the document clearly distinguishes between the two.

2. VALIDATION REPORT

2.1. The main page of the validation report

Report header



- **Report number** – a number that uniquely identifies the report.
- **Date of submitting the document for validation** – the date specifying the moment when the GetValid service server received the document for validation[1]. The date is given both in the official time of the Republic of Poland and in UTC time.
- **Report issue date** – the date specifying the moment the validation report was generated.
- **Date of existence of the document declared by the user** – information about the date of existence of the document appears in the report only if the user, entering the document for validation, indicated a specific date on which the signed document, according to the user, already existed. The significance of this date and when it should be introduced has been described in **Chapter 3**.

[1] In fact, no documents are sent to the GetValid server, only hashes from documents and the signatures themselves.

File name and SHA-256 file digest

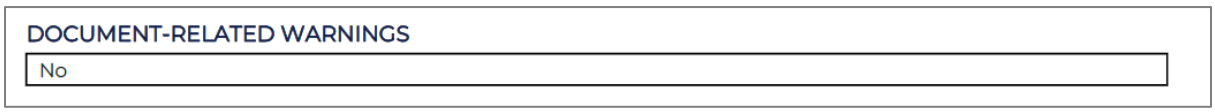
DOCUMENT FILES

File name	PAdES z efektem graficznym.pdf
SHA-256 file digest	BFD880F007341510D290D3521AC9289D5794D6F83A9334146EC3898F487D7800

A dedicated application, available at https://www.cencert.pl, is used to confirm that a specific validation report applies to a specific electronic document.

This section contains a list of files that make up the signed document (the signature under the document may be in a separate file or the document may have attachments). The report presents file names and SHA-256 hashes from their contents. This data allows associating the document with the validation report, however, in order to be sure that a given report refers to the indicated document, it is required to use a dedicated application available on the Cencert website, which performs such a check.

Document-related warnings

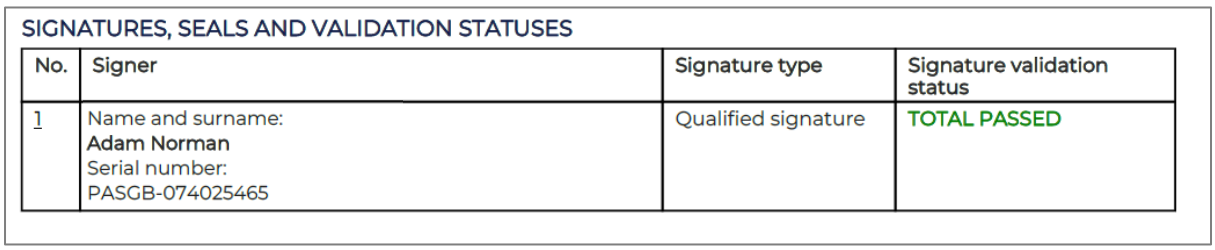


DOCUMENT-RELATED WARNINGS

No

The GetValid service examines not only the validity of signatures and seals, but also tries to warn the user against such manipulations that, without violating the validity of the signature, may mislead the user as to the content of the document. For example, an additional paragraph can be added to a signed contract in PDF format, without violating the signature, and thus attempt to manipulate its content. A detailed description of possible warnings can be found in the **Chapter 3.2.**

List of signatures, seals and validation statuses



SIGNATURES, SEALS AND VALIDATION STATUSES

No.	Signer	Signature type	Signature validation status
1	Name and surname: **Adam Norman** Serial number: PASGB-074025465	Qualified signature	TOTAL PASSED

This section contains basic information about signatories, signatures and validation results.

Column	Meaning
Signatory	For signatures, the column contains: o Name and surname of the person who signed the document o PESEL number or the number of a document uniquely identifying the person who signed the document

	For seals, the column contains all the fields of the distinguished name of the owner of the certificate used to sign.
Signature Type	Specifies the type of signature. For a complete list, see **Chapter 3.4 .**
Signature validation status	It contains the result of validation of a given signature: o Positive – the signature is valid o Negative – the signature is invalid o Indeterminate – the collected premises do not allow to clearly determine the result of validation The "**positive**" and "**negative**" results are final and repeating the validation process will not obtain a different result, unless the date of signing the document is amended, i.e. the user repeats the validation entering a different date of existence of the signed document. Result "**indeterminate**" means that the service is not able to determine either the validity of a given signature or its invalidity. Further actions of the user should depend on the information described in the **Validation Status Details** in the part of the report containing the details of the validation of a given signature (**see chapters 2.2 and 3.5**).

2.2. Signature validation details

- **Signatory**

Signer	Country: PL Given name: **Adam** Surname: **Norman** Serial number: PASGB-074025465 Common name: Adam Norman

This field contains full information about the distinguished name of the owner of the certificate used to sign.

- **Pseudonym used**

A pseudonym was used	No

This field indicates whether the certificate owner's ID contains a pseudonym in place of the name and surname. Possible values: Yes, No.

- **Commitment type**

Commitment type	Proof of creation

Commitment type arises from established standards and has been defined, among others, in the following standards: ETSI EN 319 122 (CAdES), ETSI EN 319 132 (XAdES) i ETSI EN 319 142 (PAdES).

- **Purpose of the signature declared by the user**

Purpose of the signature declared by the user	Potwierdzam dokładność i integralność tego dokumentu

When the reason for signing is included in the PDF signature (e.g. in Adobe Reader), it will be displayed in this field in the report.

- **Signature type**

Signature type	Qualified signature

For a complete list of available signature types, see **Chapter 3.4.**

- **Signature form** for XAdES, PAdES, CAdES, ASiC.

Signature form	PAdES B

- **Validation status**

Validation status	TOTAL PASSED

Possible values are described in the section "List of signatures, seals and validation statuses" in the **Chapter 2**.

- **Validation status details**

Validation status details	

The field is filled in, if the validation status is other than positive and it indicates the reason for incorrect validation, e.g. certificate revocation or use of a compromised SHA-1 algorithm. A detailed list of causes with a discussion of their importance can be found in **Chapter 3.5** For more information on accepting signatures submitted using the SHA-1 algorithm, see **Chapter 3.8.**

- **Integrity verification**

Integrity verification	Positive

This field specifies the integrity verification status of the document. Possible values:

- Positive – the content of the document has not been modified after the signature has been made
- Negative - the content of the document or signature has been modified after the signature has been made

- **Certificate verification**

Certificate verification	Positive OCSP 2025-10-14 06:23:29 UTC Date of proof of signature existence: date of submission for validation 2025-10-14 06:23:08 UTC

This field specifies the validation status of the certificate used to verify the signature. Possible values:

- Positive – the certificate is valid for the given date of proof of the signature's existence
- Negative – the certificate is invalid for the given date of proof of the signature's existence
- Indeterminate – the validity of the certificate cannot be determined for the given date of the proof of the signature's existence

The status may be accompanied by additional information:

- Source of revocation information:
  - OCSP + [date of issuance of OCSP response] – the source is the OCSP server
  - CRL + [CRL issuance date] – the source is the CRL
- Source + date of proof of signature existence. Possible values are:
  - Qualified timestamp
  - Non-qualified timestamp
  - Date provided by the user
  - Date of submitting for validation

- **Timestamp**

Timestamp	No

The "Timestamp" field specifies whether the signature has been timestamped, and only timestamps that have been successfully verified and applicable to the signature type are listed[2]. Possible values:

- No – the signature has not been timestamped.
- Qualified + [date from the timestamp] – the signature has been marked with a qualified timestamp.
- Non-qualified + [date from the timestamp] – the signature has been marked with a non-qualified timestamp.

If the signature is marked with multiple timestamps, the date from the earliest marker is presented, i.e. the date placed at the moment closest to the moment of signature.

More about qualified timestamp **in the chapter 3.6**.

- **System signing time**

System signing time	2025-02-04 08:54:24 UTC

The field contains information about the time of signature placed in the signature structures by the signing application, based on the current time of the computer on which the signature was applied. This field has only an informative value and is not used during validation, because the current time of the computer on which the signature was placed could be incorrect or deliberately manipulated.

- **Certified date of signature**

Certified date of signature	Indefinite

Currently, technology does not allow to determine the exact date of signature. The qualified timestamp on the document after the signature is only used to establish that the signature was made "not later than" the date of the qualified timestamp. However, it is possible to specify the time period in which the signature was placed, provided that the document was also previously (before the signature) marked with a qualified timestamp. Such an earlier timestamp makes it possible to establish that the signature was made "not earlier than" the date of this timestamp.

Since the accuracy of the date of signature determination can be of significant evidential or legal importance for users, the GetValid service presents, in the "Verified Time of Signature" field, the time interval when the signature was made, determined by the qualified timestamps closest to the signature, which were made in the document before and after the signature. Possible values:

[2] If the verified **qualified** signature has **a non-qualified** timestamp, such a marker is not taken into account during validation and is not shown on the report.

- No - No qualified timestamps in the document
- Not later than + [date from the timestamp] – if the document was marked with a qualified timestamp only after the signature has been made
- Not earlier than + [date from timestamp]; not later than + [date from the timestamp] – if the document was marked with a qualified timestamp before and after the signature

For a given signature, qualified timestamps (previous and consequential) closest to the moment of signing are taken into account.

For the greatest accuracy in determining the time of signature, we suggest following the guidelines in the section **3.6**.

- **Revocation information obtained from**

Revocation information obtained from	OCSP 2025-10-14 06:07:28 UTC

This field indicates the source the GetValid service used to investigate whether the certificate is valid. Possible values:

- OCSP + [date OCSP response was issued] – the source is the OCSP server
- CRL + [date CRL was issued] – the source is CRL

- **Revocation date**

Revocation date	Not applicable

If the certificate has been revoked or suspended, this field contains information about the date of revocation or suspension.

- **Revocation reason**

Revocation reason	Not applicable

If the certificate has been revoked, this field contains information about the reason for the revocation of the certificate. This information is of little practical importance, since regardless of the reason, the revocation of the certificate results in the invalidity of the signatures submitted after this fact.

- **The signer certificate number**

The signer certificate number	03EB4193860284 74
Issued by	Country: PL Organization: Enigma Systemy Ochrony Informacji Sp. z o.o. Common name: CenCert QTSP CA Organization identifier: VATPL-5261029614

The fields specify the serial number of the signer's certificate and the distinguished name of the issuer of the certificate used to verify the signature.

- **Validity dates**

Validity dates	From: 2024-08-30 11:34:02 UTC To: 2026-08-30 23:59:59 UTC

This field contains the validity interval of the signer's certificate used to verify the signature.

- **Signed data digest**

Signed data digest	SHA-256 EC92F1208CDCCBD54E63A512B33391106CBB651AD87BCF5B0E88CF5BE6DD0BD1

The field contains information about the algorithm and hash value of the signed data.

- **Warnings**

Warnings	No

The field contains warnings associated with the signature that do not affect the result of signature validation, however the user should be informed about them. A description of available warnings can be found in the **Chapter 3.3.**

3. DETAILED INFORMATION

3.1. Date of existence of the document declared by the user

According to law, a signature is considered valid, if it was made at the time the certificate used for this purpose was valid. If the certificate was revoked, the service would compare the date of the signature with the date of the certificate revocation. If the signature was made before the moment of revocation, the signature is valid. If it was made after the moment of revocation, the signature is invalid.

How does the validation service know when the signature was made? The source to determine the date of signing[3] can be:

- Qualified timestamp.
- The moment of submitting the document for validation.
- The date declared by the user.

The most reliable solution is to mark the document with a qualified timestamp at the time of signature, or as soon as possible thereafter. Then the validation service is certain that the signature was added not later than the date of the qualified timestamp and at this point it will verify the validity of the signature certificate (more on the qualified timestamp in **chapter 3.6**).

If the document has not been time-stamped, then the validation service will verify the validity of the signature certificate as of the time the document was submitted for validation. If a long time has elapsed between the moment of signing and the moment the document is submitted for validation, the signature certificate may have expired or revoked, therefore the validation result will not be positive.

In such a situation, the only possibility to obtain a positive validation result will be to enter (declare) the date of existence of the signed document by the user. However, it should be remembered that the burden of proof of the correctness of this date rests with the user. The validation report will be valid, provided that if there is any doubt as to the existence of the document on a certain date, the user will be able to prove this fact on the basis of other evidence.

[3] In fact, the service determines the date of the signature with some approximation (not later than). It follows from the feature of the electronic signature that if the certificate was valid at some point in time, it was also valid at any earlier time, in particular at the time when it was actually used to sign. Therefore, for signature validation, it is sufficient to demonstrate the validity of the certificate at any time later than the signature.

3.2. Document-related warnings

Warning	Meaning
No warnings	No issues were detected with the document.
The document contains active content that can affect the content presented.	A PDF document contains JavaScript that can affect the content presented to the user when the document is displayed, e.g. by presenting different content of the document depending on the date. However, JavaScript can perform useful functions, e.g. validate the correctness of form fields.
In the document, on pages <page numbers> (and further pages, the total number of such pages is <number of pages>) there is content not covered by all signatures.	A PDF contains content which is not covered by all signatures. It could be a deliberate attempt at manipulation, but it could also be a completely intentional and harmless action, e.g.: • Comments or annotations have been added to the signed document. In this case, the annotations are not covered by the signature, but they are also not an attempt to manipulate the content of the document. • The author of the form signed the form, after which the user filled out the form and added his own signature. In this case, the two signatures cover different content.

3.3. Signature warnings

Warning	Meaning
The 'SigningCertificate' attribute is missing.	This warning applies to a specific signature and it means that the signed data does not indicate a certificate for the signature verification. This means that if there were two or more certificates issued to the same key, but containing different data of the certificate owner, it would not be possible to determine which certificate was the actual signature.

	Therefore, it would be possible to indicate another subscriber using the same key as the author. Acrobat Reader software, which is often used to sign PDF documents, has an option that sets the use of a signature format (PKCS#7) that is inconsistent with European law and does not contain the required attribute. Unfortunately, this option is enabled by default, which can mean that many PDFs are signed without this attribute. The risk of accepting a document without the 'SigningCertifiate' attribute seems to be low, because obtaining qualified certificates containing different subscriber data on the same public key is unlikely and the potential attacks are limited.

3.4. Types of signatures and seals

- Qualified signature
- Qualified seal
- Personal Signature – an advanced electronic signature made using the keys on the Polish ID card
- ePUAP signature – an advanced electronic signature made using the ePUAP platform
- Advanced signature verified by a qualified certificate
- Advanced seal verified by a qualified certificate
- Advanced signature
- Advanced seal
- Seal of the qualified validation service of e-signatures and seals
- Seal of the qualified registered e-mail service
- Seal of the qualified electronic delivery service
- Seal of the qualified service of preservation of signatures and Seals

3.5. Validation Status Details

3.5.1. Details for the "**invalid**" validation status

Value	Description
The digest from the document does not match the signed digest	The document or signature has been modified after the signature has been

	made, or the signature does not match the document.
Signature with a certificate after the validity period	The signature was made after the validity period of the certificate. **Possible action**: Consider whether there is evidence of the existence of the signed document earlier, during the validity period of the certificate; if so – enter the date of this evidence when calling the validation service again
Signature made with a revoked certificate	The signature was made after the certificate was revoked. **Possible action**: Consider whether there is evidence of existence of the signed document earlier, before the date of revocation of the certificate; if so – enter the date of this evidence when calling the validation service again.
Incorrect signature format	The document submitted for validation has a signature, the format of which is incorrect, making it impossible to validate.
The signature cannot be verified with the public key from the signature certificate	The document or signature were modified after the signature had been made, or the signature is not for this document.

3.5.2. Details for the "**indeterminate**" validation status

Value	Description
The attribute that indicates the certificate to verify the signature points to a different certificate than the one used to sign	Signature structure error (forgery or signing software error)
Certificate path validation error	The service is unable to verify the trust path for the certificate used to verify the signature. The occurrence of this error is extremely unlikely, as it would indicate an error on the part of the issuer of the certificate.
Unable to build a certification path for a signature certificate	It is impossible to build a trust path for the certificate used to sign, based on the given TSL lists.

	The reason is that the issuer of the certificate is not on the list of trusted issuers of qualified and non-qualified certificates recognized by the EU.
Cryptographic algorithm does not meet the validation conditions	A cryptographic algorithm was used to sign or issue one of the analyzed certificates and CRLs, which is questionable whether it is sufficiently secure. For more information on acceptance of the signatures made using the SHA-1 algorithm, see **Chapter 3.8.**
Incorrect order of timestamps	At least one of the timestamps attached to the document indicates an incorrect date (it was added later, but still points to an earlier date). The occurrence of this error is extremely unlikely, as it would mean an error on the part of the timestamp service provider.
Signature certificate unavailable	The certificate used to sign has not been attached to the document and is not available to the validation service.
The signature certificate has been revoked, but the date of proof of existence of the signature has not been specified or The certificate of the certificate issuer has been revoked, but the date of proof of existence of the signature has not been specified or The signature certificate is beyond validity period but the date of proof of existence of the signature has not been specified	The document submitted for validation was not timestamped, nor did the user manually indicate the date of the existence of the document, therefore the service assumed the current time as the date of existence of the signature. For such a date, there is an indicated problem with the validity of the certificate, which may not have occurred at the time of signing. **Possible action**: Consider whether there is evidence of the signed document earlier, before the date of revocation or expiration of the certificate; if so – enter the date from this evidence when the validation process is called again.
The cryptographic algorithm does not meet the current validation conditions, but the date of proof of the signature's existence has not been specified	The document submitted for validation was not timestamped, nor did the user manually indicate the date of the document's existence, therefore the service assumed the current time

	as the signature validity date. For such a date, there is a problem with the security of the indicated algorithm, which may not have occurred at the time of signing. **Possible action**: Consider whether there is evidence of the signed document earlier, before the date the algorithm is considered unsafe; if so – enter the date from this evidence when the validation process is called again. For more information on accepting signatures made using the SHA-1 algorithm, see **Chapter 3.8.**
Signature certificate suspended or Issuer's Certificate suspended	The certificate has been suspended by the issuer, so the validity of the signature cannot be determined until the certificate is resumed, suspended or revoked. **Possible actions:** Repeat the validation process after a certain period of time (certificate suspension time usually does not exceed a few days). Alternatively, consider whether there is evidence of the signed document earlier, before the certificate was suspended; if yes – enter the date of this evidence when calling the validation service again.
CRL/OCSP not available or ARL/OCSP not available	The validation service does not have access to the revocation information that should be published by the issuer, so the validity of the certificate used to verify the signature cannot be verified. The lack of access can be caused by a failure / may be due to a failure on the issuer side of the signature certificate. **Possible actions:** Repeat the validation process after a period of time.

CRL/OCSP expired and no date of proof of signature. or ARL/OCSP expired and no date of proof of signature	The document submitted for validation was not timestamped, nor did the user manually indicate the date of the document's existence, therefore the service assumed the current time as the signature validity date. For such a date, there is a question whether the information about revocations held by the service is up-to-date, which may not have occurred at the time of signing. Failure to provide sufficiently new information about revocations may be caused by a failure on the part of the signature certificate issuer. **Possible actions:** Repeat the validation process after a period of time. Consider whether there is evidence of the signed document earlier, before the current date; if so – enter the date from this document when calling the validation service again.
CRL/OCSP issued before the date of signature or ARL/OCSP issued before the date of signature	The validation service does not have access to sufficiently new revocation information that the certificate issuer should publish, so the validity of the certificate used to verify the signature cannot be verified. The lack of access can be caused by a failure on the side of the signature certificate issuer. **Possible actions:** Repeat the validation process after a period of time.

3.6. Qualified Timestamp

According to EU Regulation 910/2014 (eIDAS), a qualified electronic timestamp:

a) is based on a precise time source linked to Universal Time Coordinated,
b) associates the date and time with the data so as to sufficiently exclude the possibility of undetectable alteration of the data, and
c) is signed using an advanced electronic signature or the advanced electronic seal of a qualified trust service provider or other equivalent means.

As a result, in accordance with eIDAS, there is a presumption of the accuracy of the date and time it indicates and the integrity of the data to which the date and time are linked.

Moreover, according to Polish law, affixing a qualified timestamp to an electronic document is tantamount to giving the document the value of a certain date within the meaning of Article 81 §2 item 3 of the Civil Code.

3.7. Exact date of signature

In order for the GetValid service to be able to demonstrate the exact date of signature, the signatory must act consciously. The signatory must proceed as follows (this method only works for PDF documents):

1. Timestamp the prepared PDF document.
2. Sign the document.
3. Timestamp the signed document.

In this case, the GetValid service will show that the signature was made in the date interval between the first and second timestamps. Since the execution of the sequence: timestamping – signature – timestamping, can be performed in single seconds, the date of signature obtained this way will be known with such accuracy.

3.8. Accepting signatures with SHA-1 algorithm

SHA-1 was widely used for electronic signatures, but over time, effective attacks have been discovered, including those that demonstrate the ability to forge an electronic signature made using SHA-1. The practical execution of this forgery is still quite difficult, because the attacker has to create two specifically crafted versions of a PDF document, one of which is given to an authorized person to sign, and then the attacker can replace the signed document with the other version, without tampering with the signature. Therefore, the attack requires prior preparation and needs the forger to be a trusted person for the signatory and be able to plant the forged document for signature. It is still not possible to forge any signed document, but the discovered attacks were so serious that they currently exclude the use of SHA-1 for signatures.

Due to these weaknesses, SHA-1 is no longer considered secure in electronic signature standards and in the legal systems of various countries, therefore now SHA-2 family algorithms (SHA-256, SHA-512, etc.) are used for signatures. It is difficult to indicate a definitively accurate end date for the SHA-1 algorithm, as this is a legal issue and may depend on the context and specific use of the signature. The GetValid service has adopted the date specified in Article 137(1) of the Polish Act of 5 September 2016 on trust services and electronic identification, i.e. 1 July 2018 – signatures validated for a date falling before 1 July 2018

(i.e. signatures submitted before that date) are validated positively (at that time the attack on SHA-1 was unknown, therefore, there was no practical possibility of its execution), and signatures submitted later are validated with the status "Indeterminate ".