Building a better
working world

Ernst & Young sp. z o.o.
Business Advisory sp. k.
Rondo ONZ 1
00-124 Warszawa

+48 22 557 70 00
+48 22 557 70 01
warszawa@pl.ey.com
www.ey.com/pl

INDEPENDENT ASSURANCE REPORT

To the management of Asseco Data Systems S.A. (ADS):

Scope

We have been engaged, in a reasonable assurance engagement, to report on ADS management's statement that for its Certification Authority (CA) operations in Szczecin, Poland, throughout the period March 27, 2018 to March 04, 2019 for its CAs as enumerated in Attachment A, ADS has:

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in its:
  - Certification Practice Statement of Certum's Certification Services v6.0 and
  - Certification Policy of Certum's Certification Services v4.4

including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the ADS website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV CS certificates it manages is established and protected throughout their lifecycles; and
  - EV CS subscriber information is properly authenticated (for the registration activities performed by ADS)

- maintained effective controls to provide reasonable assurance that:
  - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
  - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

- maintained effective controls to provide reasonable assurance that its EV CS Signing Authority and EV CS Timestamp Authority are operated in conformity with CA/Browser Forum Guidelines

in accordance with WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing version 1.4.1.

ADS makes use of external registration authorities for specific subscriber registration activities as disclosed in ADS's business practices. Our examination did not extend to the controls exercised by these external registration authorities.

Certification authority's responsibilities

ADS's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4.1.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.
The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding

compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor’s responsibilities

Our responsibility is to express an opinion on management’s statement based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s statement is fairly stated, and, accordingly, included:

1) obtaining an understanding of ADS’s EV CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates;
2) selectively testing transactions executed in accordance with disclosed EV CS certificate lifecycle management practices;
3) testing and evaluating the operating effectiveness of the controls; and
4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at ADS and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, ADS’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period March 27, 2018 to March 04, 2019, ADS management’s statement, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4.1.

This report does not include any representation as to the quality of ADS’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4.1, nor the suitability of any of ADS’s services for any customer's intended purpose.

Use of the WebTrust seal

ADS’s use of the WebTrust for Certification Authorities – Extended Validation Code Signing Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

EY, Warsaw, Poland

Ernst & Young.

....

Warsaw August 09, 2019

ASSECO DATA SYSTEMS S.A.'S MANAGEMENT STATEMENT

Asseco Data Systems S.A. (ADS) operates the Certification Authority (CA) services as enumerated in Attachment A, and provides Extended Validation Code Signing ("EV CS") CA services.

The management of ADS is responsible for establishing and maintaining effective controls over its EV CS CA operations, including its EV CS CA business practices disclosure on its website https://www.certum.pl/pl/ cert_wiedza_repozytorium_pl_en/, EV CS key lifecycle management controls, EV CS certificate lifecycle management controls, EV CS Signing Authority and EV CS Timestamp Authority certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ADS's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ADS management has assessed its disclosures of its certificate practices and controls over its EV CS CA services. Based on that assessment, in ADS management's opinion, in providing its EV CS Certification Authority (CA) services in Szczecin, Poland, throughout the period March 27, 2018 to March 04, 2019, ADS has:

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in its:
    - Certification Practice Statement of Certum's Certification Services v6.0; and
    - Certification Policy of Certum's Certification Services v4.4

including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the ADS website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and EV CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS subscriber information is properly authenticated (for the registration activities performed by ADS)

- maintained effective controls to provide reasonable assurance that:
    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

- maintained effective controls to provide reasonable assurance that its EV CS Signing Authority and EV CS Timestamp Authority are operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing version 1.4.1.

Management of Asseco Data Systems S.A.

Z upoważnienia Zarządu
Asseco Data Systems S.A.
Tomasz Litarowicz

Z upoważnienia Zarządu
Asseco Data Systems S.A.
Andrzej Ruciński

August 09, 2019

Attachment A: List of CAs in Scope

Root CAs

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
1	1	CN = Certum CA O = Unizeto Sp. z. o. o. C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	010020	rsaEncryption	2048 bits	sha1RSA	Jun 11 10:46:39 2002 GMT	Jun 11 10:46:39 2027 GMT	97 36 ac 3b 25 d1 6c 45 a4 54 18 a9 64 57 81 56 48 0a 8c c4 34 54 1d dc 5d d5 92 33 22 98 68 de	d8 e0 fe bc 1d b2 e3 8d 00 94 0f 37 d2 7d 41 34 4d 99 3e 73 4b 99 d5 65 6d 97 78 d4 d8 14 36 24	
2	1	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	0444C0	rsaEncryption	2048 bits	sha1RSA	Oct 22 12:07:37 2008 GMT	Dec 31 12:07:37 2029 GMT	aa 26 30 a7 b6 17 b0 4d 0a 29 4b ab 7a 8c aa a5 01 6e 6d be 60 48 37 a8 3a 85 71 9f ab 66 7e b5	5c 58 46 8d 55 f5 8e 49 7e 74 39 82 d2 b5 00 10 b6 d1 65 37 4a cf 83 a7 d4 a3 2d b8 c4 40 8e	

	2	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	23 e8 29 0d 71 95 04 18 c0 08 59 7e 42 f7 48 1b	rsaEncryption	2048 bits	sha1withRSA	Oct 22 12:07:37 2008 GMT	Dec 30 23:59:59 2025 GMT	aa 26 30 a7 b6 17 b0 4d 0a 29 4b ab 7a 8c aa a5 01 6e 6d be 60 48 37 a8 3a 85 71 9f ab 66 7e b5	2d 87 ff 20 fe 8a d2 30 5d fb 6f 39 92 86 7e d2 bf 4f e3 e1 34 62 12 c4 34 59 91 aa c0 22 66 e9	
	3	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	93 92 85 40 01 65 71 5F 94 7F 28 8F EF C9 9B 28	rsaEncryption	2048 bits	sha1withRSA	Oct 22 12:07:37 2008 GMT	Jun 10 10:46:39 2027 GMT	aa 26 30 a7 b6 17 b0 4d 0a 29 4b ab 7a 8c aa a5 01 6e 6d be 60 48 37 a8 3a 85 71 9f ab 66 7e b5	94 94 24 dc 2c ca ab 5e 9e 80 d6 6e 0e 3f 7d ee b3 20 1c 60 7d 43 15 ef 4c 6f 2d 93 a9 17 27 9d	

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
3	1	CN = Certum Trusted Network CA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	CN = Certum Trusted Network CA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	21 d6 d0 4a 4f 25 0f c9 32 37 fc aa 5e 12 8d e9	rsaEncryption	4096 bits	sha512RSA	Oct 06 08:39:56 2011	Oct 06 08:39:56 2046	6b 3b 57 e9 ec 88 d1 bb 3d 01 63 7f f3 3c 76 98 b3 c9 75 82 55 e9 f0 1e a9 17 8f 3e 7f 3b 2b 52	b6 76 f2 ed da e8 77 5c d3 6c b0 f6 3c d1 d4 60 39 61 f4 9e 62 65 ba 01 3a 2f 03 07 b6 d0 b8 04	
4	1	CN = Certum Elliptic Curve CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	CN = Certum Elliptic Curve CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	d2 de 59 3e af 11 20 6e 79 05 e7 41 76 f2 3d b4	id-ec PublicKey	521 bits	sha512 ECDSA	Mar 16 12:09:04 2018 GMT	Mar 16 12:09:04 2043 GMT	5a 9b b2 1b 04 0e 90 d3 30 ed 41 48 f3 48 c8 f3 8f 20 84 e4	7a 5f bb 25 d8 f4 94 5f b9 bb 38 ad 0a 20 36 24 cd a7 8c c8 9f e2 e5 a5 34 94 37 bf 4b 3e 98 44	

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
5	1	CN = Certum Trusted Root CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	CN = Certum Trusted Root CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	1e bf 59 50 b8 c9 80 37 4c 06 f7 eb 55 4f b5 ed	rsaEncryption	4096 bits	sha512WithRSA	Mar 16 12:10:13 2018 GMT	Mar 16 12:10:13 2043 GMT	8c fb 1c 75 bc 02 d3 9f 4e 2e 48 d9 f9 60 54 aa c4 b3 4f fa	a1 87 68 b9 35 3c ba 0b f3 00 aa 49 3a 29 70 49 0e 64 f9 d1 44 36 e0 23 6b f2 cb da 2a d0 9b 31	
6	1	CN = Certum EC-384 CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	CN = Certum EC-384 CA OU = Certum Certification Authority O = Asseco Data Systems S.A. C = PL	78 8f 27 5c 81 12 52 20 a5 04 d0 2d dd ba 73 f4	id-ec PublicKey	384 bits	Sha384 ECDSA	Mar 26 07:24:54 2018 GMT	Mar 26 07:24:54 2043 GMT	8d 06 66 74 24 76 3a f3 89 f7 bc d6 bd 47 7d 2f bc 10 5f 4b	6b 32 80 85 62 53 18 aa 50 d1 73 c9 8d 8b da 09 d5 7e 27 41 3d 11 4c f7 87 a0 f5 d0 6c 03 0c f6	

Other CA’s

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
1	1	CN = Certum Global Services CA O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	00 c5 3c 18 bf 8f 3f 9c c7 73 06 a9 c6 a1 3e 84 e7	rsaEncryption	2048 bits	sha1withRSA	Mar 3 13:06:12 2009 GMT	Mar 3 13:06:12 2024 GMT	b4 d3 16 33 d8 3b 31 05 cd 26 91 5f 7c 0e 6b f8 a0 e3 89 59 a6 5e b6 d8 3d d4 2f 56 d3 91 a4 8e	2e 48 1f f3 a5 3d 29 3b d4 9f 3c d8 39 76 58 36 82 b3 bd 79 a1 60 fd 6e 9c a5 87 25 d9 3b 94 5b	
2	1	CN = Certum Global Services CA SHA2, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	00 d0 4b 6f e5 dd 5b d2 21 e7 c7 4c f6 46 8b 31 46	rsaEncryption	2048 bits	SHA256with RSA	Sep 11 12:00:00 2014 GMT	Jun 9 10:46:39 2027 GMT	33 b6 83 fc 79 a0 cb b0 85 f2 c4 dd 76 be 6c a3 53 19 58 40 6e 35 f2 c8 74 67 b5 8e fc b4 5f a1	9e 85 2c 59 df c6 fd 6a bd 4e 17 ea 80 b5 f4 e5 6f c0 41 92 d1 07 25 8d 54 da 8a 92 52 86 70 d6	

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
3	1	CN = Certum Extended Validation Code Signing CA SHA2 O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	4e 96 c1 ba 06 25 8a 0c 2a ba 27 62 5e 90 64 d3	rsaEncryption	2048 bits	SHA256with RSA	Oct 29 11:55:39 2015 GMT	Jan 19 11:55:39 2027 GMT	2a 61 62 e4 4d fc 38 08 bd 88 8b 7b e2 37 2d ee 22 47 43 40 12 6e 33 8e c1 d2 b9 ec e1 43 bb c5	17 6a ae 8b dd 5d d0 6a 7d bd 42 86 2d c1 73 bd 83 8f fe 30 13 10 3b 09 7b 96 71 c3 7b a6 ae 14	
4	1	CN = WoSign Code Signing CA, O = WoSign CA Limited, C = CN	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	17 ef 72 b4 15 7d 6f 4b 68 e4 bd d5 75 e5 cc ae	rsaEncryption	2048 bits	SHA256with RSA	Nov 9 08:45:13 2016 GMT	Nov 9 08:45:13 2026 GMT	15 94 b4 17 ff c9 ec 51 f3 a4 da af db 67 e1 4d 96 75 9e cf 25 8a fa 84 6a 20 7d 35 fb 5d 8a 85	7b 0b c3 56 3d 43 30 91 18 f5 60 a6 c9 9a 22 1c 35 39 9b 10 29 3f 73 be 41 a1 2a ca 03 38 07 5f	

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
5	1	CN = WoTrus Code Signing CA O = WoTrus CA Limited, C = CN	CN = Certum Trusted Network CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	6e a1 d4 94 5f 0e 69 e9 d6 f1 48 2c 58 6a 71 af	rsaEncryption	2048 bit	SHA256with RSA	Apr 17 08:20:15 2018 GMT	May 18 08:20:15 2027 GMT	ac 81 41 56 41 a2 b9 20 72 51 59 78 be e9 09 cf 54 1c b5 86 4b 06 32 c9 f5 95 5a e8 db 65 dc 0f	08 29 CA B6 93 AA DF AF 21 C7 78 76 DB E7 6B B9 AC 74 91 60 8F FA EB F7 D1 D5 3C 28 9F C8 84 52	