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 05, 2019 to February 10, 2020 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 v6.5 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 05, 2019 to February 10, 2020, 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

May 18, 2020

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Tel./Fax.
+48 58 550 95 00
+48 58 550 95 51

asseco
DATA SYSTEMS

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 05, 2019 to February 10, 2020, 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 v6.5; 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.
Andrzej Ruciński

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

……………………………………….

May 18, 2020

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	2002-06-11	2027-06-11	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	D8E0FEBC1DB2E38D00940F37D27D41344D993E734B99D5656D9778D4D8143624	
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	2008-10-22	2029-12-31	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	5C58468D55F58E497E743982D2B50010B6D165374ACF83A7D4A32DB768C4408E	
	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	2008-10-22	2025-12-30	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	2D87FF20FE8AD2305DFB6F3992867ED2BF4FE3E1346212C4345991AAC02266E9	
	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	2008-10-22	2027-06-10	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	949424DC2CCAAB5E9E80D66E0E3F7DEEB3201C607D4315EF4C6F2D93A917279D	

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	2011-10-06	2046-10-06	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	B676F2EDDAE8775CD36CB0F63CD1D4603961F49E6265BA013A2F0307B6D0B804	
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	2018-03-16	2043-03-16	5A 9B B2 1B 04 0E 90 D3 30 ED 41 48 F3 48 C8 F3 8F 20 84 E4	7A5FBB25D8F4945FB9BB38AD0A203624CDA78CC89FE2E5A5349437BF4B3E9844	
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	sha512With RSA	2018-03-16	2043-03-16	8C FB 1C 75 BC 02 D3 9F 4E 2E 48 D9 F9 60 54 AA C4 B3 4F FA	FE7696573855773E37A95E7AD4D9CC96C30157C15D31765BA9B15704E1AE78FD	
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	2018-03-26	2043-03-26	8D 06 66 74 24 76 3A F3 89 F7 BC D6 BD 47 7D 2F BC 10 5F 4B	6B328085625318AA50D173C98D8BDA09D57E27413D114CF787A0F5D06C030CF6	

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	2009-03-03	2024-03-03	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	2E481FF3A53D293BD49F3CD83976583682B3BD79A160FD6E9CA58725D93B945B	
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	2014-09-11	2027-06-09	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	9E852C59DFC6FD6ABD4E17EA80B5F4E56FC04192D107258D54DA8A92528670D6	
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	2015-10-29	2027-01-19	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	176AAE8BDD5DD06A7DBD42862DC173BD838FFE3013103B097B9671C37BA6AE14	
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	2016-11-09	2026-11-09	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	7B0BC3563D43309118F560A6C99A221C35399B10293F73BE41A12ACA0338075F	
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	2018-04-17	2027-05-18	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	0829CAB693AADFAF21C77876DBE76BB9AC7491608FFAEBF7D1D53C289FC88452	