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

Building a better working world

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 assertion that for its Certification Authority (CA) operations at Szczecin, Poland, throughout the period April 15, 2017 to March 26, 2018 for its CAs as enumerated in Appendix A has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement; and
  - Certificate Policy

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by ADS)

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

And, for its CAs as enumerated in Appendix A:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the *WebTrust$^{SM/TM}$ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*.

Building a better working world

Certification authority's responsibilities

ADS's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the *WebTrust℠/™ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*.

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 assertion 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 assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of ADS's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of ADS's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL 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

Building a better working world

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 April 15, 2017 to March 26, 2018, ADS management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the *Web Trust*$^{SM/TM}$ *Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3.*

This report does not include any representation as to the quality of ADS's services beyond those covered by the *Web Trust*$^{SM/TM}$ *Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*, 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 – SSL Baseline with Network Security 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

Artur Żwak

Partner

June 22, 2018

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

Management's Assertion Regarding the Effectiveness of Its Controls Over the SSL Certification Authority (CA) Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3

June 22, 2018

We, as the management of Asseco Data Systems S.A. (ADS), are responsible for operating the SSL Certification Authority (CA) services at Szczecin, Poland for the Root CA(s) in scope for SSL Baseline Requirements and Network Security Requirements listed at Appendix A.

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

The management of ADS has assessed the disclosure of its certificate practices and its controls over its SSL Certificate Authority (CA) services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Szczecin, Poland throughout the period from April 15, 2017 through March 26, 2018, ADS has:

- Disclosed its SSL certificate lifecycle management business practices in its;
  - Certification Practice Statement; and
  - Certificate Policy

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the [name of company] website, and provided such services in accordance with its disclosed practices

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

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and

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

Tel./fax
+4858 550 95 00
+48 58 550 95 51

asseco
DATA SYSTEMS

- Maintained effective controls to provide reąsonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

for the Root CA(s) and [Subordinate CA(s)] in scope for SSL Baseline Requirements and Network Security Requirements at Appendix A, based on the WebTrust℠/™ Principles and Criteria for Certification Authorities –SSL Baseline with Network Security –Version 2.3.

Management of Asseco Data Systems S.A.

Z upoważnienia Zarządu
Asseco Data Systems S.A.

Andrzej Łuciński

Z upoważnienia Zarządu
Asseco Data Systems S.A.

Tomasz Litarowicz

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

Appendix A

ROOT NAME	SERIAL NUMBER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT
CERTUM CA	01 00 20	N/A	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
CERTUM TRUSTED NETWORK CA	04 44 c0	08 76 cd cb 07 ff 24 f6 c5 cd ed bb 90 bc e2 84 37 46 75 f7	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:B7:68:C4:40:8E
CERTUM TRUSTED NETWORK CA2	21 d6 d0 4a 4f 25 0f c9 32 37 fc aa 5e 12 8d e9	b6 a1 54 39 02 c3 a0 3f 8e 8a bc fa d4 f8 1c a6 d1 3a 0e fd	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
Certum Elliptic Curve CA	00 d2 de 59 3e af 11 20 6e 79 05 e7 41 76 f2 3d b4	5a 9b b2 1b 04 0e 90 d3 30 ed 41 48 f3 48 c8 f3 8f 20 84 e4	1F:CE:27:F1:A6:E7:C9:49:76:CC:61:35:81:A8:CA:59:CB:28:50:C9:4C:5B:37:82:28:62:82:23:8C:59:C8:7B
Certum Trusted Root CA	1e bf 59 50 b8 c9 80 37 4c 06 f7 eb 55 4f b5 ed	8c fb 1c 75 bc 02 d3 9f 4e 2e 48 d9 f9 60 54 aa c4 b3 4f fa	FE:76:96:57:38:55:77:3E:37:A9:5E:7A:D4:D9:CC:96:C3:01:57:C1:5D:31:76:5B:A9:B1:57:04:E1:AE:78:FD
Certum EC-384 CA	78 8f 27 5c 81 12 52 20 a5 04 d0 2d dd ba 73 f4	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