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.:

We have examined the assertion by the management of Asseco Data Systems S.A. (ADS) that in providing its Certification Authority (CA) services in Szczecin, Poland known as CERTUM providing non-qualified certification services for the CERTUM CA, CERTUM TRUSTED NETWORK CA, CERTUM TRUSTED NETWORK CA2, CERTUM Elliptic Curve CA, Certum Trusted Root CA, Certum EC-384 CA referenced in Appendix A, during the period April 15, 2017 through March 26, 2018, management of ADS has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statement and
  - Certificate Policy
- maintained effective controls to provide reasonable assurance that:
  - ADS's Certification Practice Statement was consistent with its Certificate Policy; and
  - ADS provided its services in accordance with its Certificate Policy and Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
  - the subscriber information was properly authenticated (for the registration activities performed by ADS); and
  - subordinate CA certificate requests were accurate, authenticated and approved
- 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
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

For Asseco Data Systems S.A.'s ROOT CA: CERTUM CA, CERTUM TRUSTED NETWORK CA, CERTUM TRUSTED NETWORK CA2, CERTUM Elliptic Curve CA, Certum Trusted Root CA, Certum EC-384 CA, based on the *Trust Services Principles and Criteria for Certification Authorities Version 2.1*.

ADS's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA), and accordingly, included (1) obtaining an understanding of ADS's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business 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 our examination provides a reasonable basis for our opinion.

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.

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. Furthermore, 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.

In our opinion, for the period April 15, 2017 through March 26, 2018, ADS management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the *Trust Services Principles and Criteria for Certification Authorities Version 2.1*.

The WebTrust$^{SM/TM}$ seal of assurance for certification authorities on ADS's CERTUM web site 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.

This report does not include any representation as to the quality of ADS's CA services beyond those covered by the *Trust Services Principles and Criteria for Certification Authorities Version 2.1*, nor the suitability of any of ADS's services for any customer's intended purpose.

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

Assertion by Management of Asseco Data Systems S.A. regarding its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations During April 15, 2017 through March 26, 2018

June 22, 2018

Asseco Data Systems S.A. (ADS) operates as a Certification Authority (CA) in Szczecin, Poland known as CERTUM Certification Authority (CERTUM CA) providing non-qualified certification services for the CERTUM CA, CERTUM TRUSTED NETWORK CA, CERTUM TRUSTED NETWORK CA2, CERTUM Elliptic Curve CA, Certum Trusted Root CA, Certum EC-384 CA referenced in Appendix A. ADS provides the following certification authority services (excluding qualified services):

- Subscriber key management services
- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate suspension
- Certificate status information processing (using an online repository)
- Integrated circuit card life cycle management

Management of ADS is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosures, set forth in its Certification Practice Statement and its Certificate Policy in ADS's CERTUM CA repository, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

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.

Management of ADS has assessed the disclosure of its certificate practices and controls over its CA operations. Based on that assessment, in ADS Management's opinion, in providing its CA services in Szczecin, Poland during the period April 15, 2017 through March 26, 2018, ADS has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statement and
  - Certificate Policy
- maintained effective controls to provide reasonable assurance that
  - ADS's Certification Practice Statement was consistent with its Certificate Policy
  - ADS provided its services in accordance with its Certificate Policy and Certification Practice Statement
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
  - the subscriber information was properly authenticated (for the registration activities performed by ADS); and
  - subordinate CA certificate requests were accurate, authenticated and approved
- 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
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity;

For Asseco Data Systems S.A.'s ROOT CA: CERTUM CA, CERTUM TRUSTED NETWORK CA, CERTUM TRUSTED NETWORK CA2, CERTUM Elliptic Curve CA, Certum Trusted Root CA, Certum EC-384 CA in accordance with the *Trust Service Principles and Criteria for Certification Authorities Version 2.1*, including the following:

CA Business Practices Disclosure

CA Business Practices Management

Certification Practice Statement Management
Certificate Policy Management
CP and CPS Consistency

Service Integrity

CA Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Archival and Destruction
CA Key Compromise
CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls

CA-Provided Subscriber Key Generation Services
Integrated Circuit Card Life Cycle Management
Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Suspension
Certificate Validation

CA Environmental Controls

Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Audit Logging

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

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