EY
Shape the future
with confidence

Ernst & Young
Audyt Polska sp. z o.o. 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 Assertion 2025_SMIME* that for its Certification Authority (CA) operations in Szczecin, Poland, and supporting facilities in Łódź, Poland, throughout the period February 11, 2024 to February 10, 2025 for its CAs as enumerated in Attachment A, ADS has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - Certification Practice Statement version 7.11; and
  - Certification Policy version 5.1

  including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME 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

- 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 that are incorporated by reference

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.3.

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 – S/MIME Certificate v1.0.3.

Our independence and quality management

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 behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* which requires the firm to design, implement and operate a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner'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 (Revised), *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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME 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 S/MIME 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.

ADS management has disclosed to us the attached matters (Attachment B) that have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these comments in determining the nature, timing, and extent of our procedures.

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

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period February 11, 2024 to February 10, 2025, ADS management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.3.

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 – S/MIME Certificates v1.0.3, 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 – S/MIME Certificates 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.

Ernst & Young Audyt Polska sp. z o.o. sp.k.
Warsaw, Poland

Jakub Jerzy Walarus

Digitally signed by Jakub Jerzy Walarus
DN: cn=Jakub Jerzy Walarus, c=PL
Date: 2025.04.04 13:26:00 +02'00'

Jakub Walarus

Dokument podpisany przez Artur Żwak
Data: 2025.04.04 17:54:13 CEST

Artur Żwak

April 4, 2025

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk

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

asseco
DATA SYSTEMS

ASSECO DATA SYSTEMS S.A. MANAGEMENT'S ASSERTION

Asseco Data Systems S.A. ("ADS") operates the Certification Authority (CA) services as enumerated in **Attachment A**, and provides S/MIME CA services.

The management of ADS is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its website https://www.certum.pl/pl/repozytorium/, S/MIME key lifecycle management controls, and S/MIME 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 S/MIME CA services. Based on that assessment, in ADS management's opinion, in providing its S/MIME CA services in Szczecin, Poland, and supporting facilities in Łódź, Poland, throughout the period February 11, 2024 to February 10, 2025, ADS has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
    - Certification Practice Statement version 7.11; and
    - Certification Policy version 5.1

  including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycle; and
    - S/MIME 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

- 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 that are incorporated by reference

in accordance with WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.3.

Management of Asseco Data Systems S.A.

………………………………………………

April 4, 2025

Andrzej Dopierała
4 kwietnia 2025

SimplySign

Paweł
Barchwic

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	9736AC3B25D16C45A45418A964578156480A8CC434541DDC5DD59233229868DE	D8E0FEBC1DB2E38D00940F37D27D41344D993E734B99D5656D9778D4D8143624	- standard - SSL - SSL EV - Code Signing - S/MIME
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	AA2630A7B617B04D0A294BAB7A8CAAA5016E6DBE604837A83A85719FAB667EB5	5C58468D55F58E497E743982D2B50010B6D165374ACF83A7D4A32DB768C4408E	- standard - SSL - SSL EV - Code Signing - S/MIME
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	21d6d04a4f250fc93237fcaa5e128de9	rsaEncryption	4096 bits	sha512RSA	2011-10-06	2046-10-06	6B3B57E9EC88D1BB3D01637FF33C7698B3C9758255E9F01EA9178F3E7F3B2B52	B676F2EDDAE8775CD36CB0F63CD1D4603961F49E6265BA013A2F0307B6D0B804	- standard - SSL - SSL EV - Code Signing - S/MIME
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	d2de593eaf11206e7905e74176f23db4	id-ec PublicKey	521 bits	sha512 ECDSA	2018-03-16	2043-03-16	5A9BB21B040E90D330ED4148F348C8F38F2084E4	7A5FBB25D8F4945FB9BB38AD0A203624CDA78CC89FE2E5A5349437BF4B3E9844	- standard - SSL - SSL EV - Code Signing - S/MIME

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	1ebf5950b8c980374c06f7eb554fb5ed	rsaEncryption	4096 bits	sha512WithRSA	2018-03-16	2043-03-16	8CFB1C75BC02D39F4E2E48D9F96054AAC4B34FFA	FE7696573855773E37A95E7AD4D9CC96C30157C15D31765BA9B15704E1AE78FD	- standard - SSL - SSL EV - Code Signing - S/MIME
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	788f275c81125220a504d02dddba73f4	id-ec PublicKey	384 bits	Sha384 ECDSA	2018-03-26	2043-03-26	8D06667424763AF389F7BCD6BD477D2FBC105F4B	6B328085625318AA50D173C98D8BDA09D57E27413D114CF787A0F5D06C030CF6	- standard - SSL - SSL EV - Code Signing - S/MIME
7	1	CN=Certum SMIME RSA Root CA C=PL,O=Asseco Data Systems S.A.,	CN=Certum SMIME RSA Root CA C=PL,O=Asseco Data Systems S.A.,	4212C0F546E05991DAD135455C2F8BC1	rsaEncryption	4096 bits	sha384WithRSAEncryption	2023-01-27	2048-01-26	3EDE0E9A077C0A645AB06C7B1DA8254AF48EAC78	08EF47A61F8D33B37B429FE3127B59F645E3BA4A82470F8380FFB21FDD3B2131	- standard - S/MIME
8	1	CN=Certum SMIME ECC Root CA C=PL,O=Asseco Data Systems S.A.,	CN=Certum SMIME ECC Root CA C=PL,O=Asseco Data Systems S.A.,	9AE84EF80016555FC27E5F0DB382D979	id-ec PublicKey	384 bits	ecdsa-with-SHA384	2023-01-27	2048-01-26	1B0FE091C0FDAD38279DA104A9F9E65ECA7162CE	0BA1591A23AFDE691EE7E9D4881B03E69A178AB6B5BD5FC2EE31E4BEC176C98B	- standard - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
9	1	CN=Certum Trusted Network CA 2; OU=Certum Certification Authority; O=Unizeto Technologies S.A.; C=PL	CN=Certum Trusted Network CA 2; OU=Certum Certification Authority; O=Unizeto Technologies S.A.; C=PL	00B8591 4713F57 DF8F31C 0333DD2 D6197A2 317B4EB	rsaEncryption	4096 bits	SHA512With RSA	2011-10-06	2046-10-06	9736AC3B2 5D16C45A4 5418A96457 8156480A8C C434541DD C5DD59233 229868DE	9F8B05137F20ACDE9B996410F4D0BF7971A1006DC99E094C346D279B93CFF7AE	- standard - SSL - SSL EV - Code Signing - S/MIME **Revoked** on 2023-01-23

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 Class I CA SHA2, O = Unizeto Technologies S.A., O = Unizeto Technologies S.A., C = PL	CN = Certum Trusted Network CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	00d147aa29b04289f7f5c64247009fd339	rsaEncryption	2048 bits	sha1withRSA	2014-09-11	2027-06-09	0E530BDC821962629B91CE6C83F565C2EEC698B3A14C7C65C220E7B8CF2E5DCA	2AB4DFF69D75BBF9541060B434CE5AD0C4DACB7AF0DBF21D3616AFCB473796DE	- standard - SSL - SSL EV - Code Signing - S/MIME
2	1	CN = Certum Class I CA, 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	177d3b09461efbe8f0faa4d35e2da799	rsaEncryption	2048 bits	sha1withRSA	2009-04-25	2024-04-25	31B17FEB3CC434980D301B5D895E91FFDF8667B97A365E108F017E196DFD626B	B34A33B44474FDB0078F113527BBDB76FE5BF81CA24BB86D628136C5016043E8	- standard - SSL - SSL EV - Code Signing - S/MIME
3	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	00c53c18bf8f3f9cc77306a9c6a13e84e7	rsaEncryption	2048 bits	sha1withRSA	2009-03-03	2024-03-03	B4D31633D83B3105CD26915F7C0E6BF8A0E38959A65EB6D83DD42F56D391A48E	2E481FF3A53D293BD49F3CD83976583682B3BD79A160FD6E9CA58725D93B945B	- standard - SSL - SSL EV - Code Signing - S/MIME
4	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	00d04b6fe5dd5bd221e7c74cf6468b3146	rsaEncryption	2048 bits	SHA256with RSA	2014-09-11	2027-06-09	33B683FC79A0CBB085F2C4DD76BE6CA3531958406E35F2C87467B58EFCB45FA1	9E852C59DFC6FD6ABD4E17EA80B5F4E56FC04192D107258D54DA8A92528670D6	- standard - SSL - SSL EV - Code Signing - S/MIME

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 Level I CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	0de21c3ca714fe4b0a64ac469b1aaccc	rsaEncryption	2048 bits	sha1withRSA	2009-03-03	2024-03-03	7548E568CD2A00D1BE9C9583B7AAC00732C80F84977E94397F3AAF17C07BF8F7	55BB45D85F2157403DB9BAA033ED2CAD7EC9A0C490CC4C5CA8C5399E6EACB7D0	- standard - SSL - SSL EV - Code Signing - S/MIME
6	1	CN = Certum Level II CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	770ac6c2ba51a41c1d5d2f99b26b0c1a	rsaEncryption	2048 bits	sha1withRSA	2009-03-03	2024-03-03	405C2DC2933AC5AD5D5523844F3E59440804DF720FB04760AB9FB821B621DA25	FE716FF3996CD6561B6B63A8C440FDF5489CF48F7834283EEBD19B380F3FBC22	- standard - SSL - SSL EV - Code Signing - S/MIME
7	1	CN = Certum Level III CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	64fe29dccf38e030dcffe34d05689661	rsaEncryption	2048 bits	sha1withRSA	2009-03-03	2024-03-03	0D3EFB8F112406F0DD5A42C6CE47F9635FD580E14ECD575A27DBA440EC243FC4	DE8A6FD403447319FB31B471A9468A00A87DEDC062E6970D770A51603832688C	- standard - SSL - SSL EV - Code Signing - S/MIME
8	1	CN = Certum Level IV CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum CA O = Unizeto Sp. Z. o. o. C = PL	4ca5fec6617c48b056382a8280e0508c	rsaEncryption	2048 bits	sha1withRSA	2009-03-03	2024-03-03	F81D03826281E61584B8789BD349B68EF08958194E608D0D193326563695AC90	14239787E8FEC7DFFA5F4C570B721B96C169ACCA3F4E95BC3057A3F8A60D7EEF	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
9	1	CN = Certum Extended Validation CA, 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	7f510c05cfb39d04fff306ba2c56e827	rsaEncryption	2048 bits	sha1withRSA	2009-12-03	2024-12-03	33D8DFBD44CE117A9A91C0A5359874C48096735DAAB82A51F51F25E3515EB692	CF1EA15DC9C05ABC72AF0E62C48D93434AE0271B1AA4318BE3544126D24B6184	- standard - SSL - SSL EV - Code Signing - S/MIME
10	1	CN = GIS CA, O = GAZINFORMSERVICE Company limited, OU = CA, C = RU	CN = Certum Global Services CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	3d77a35b76b02931bc300d969f6161b6	rsaEncryption	2048 bits	SHA256withRSA	2014-09-30	2024-09-27	066CA18FAD76FB0A287064691E7735F6BDDDC4BF12CF7A86E0B0C8AFA541DE16	2E816BCF852D830245DDC3534BCF85A53B0B19991A525CD328626FD74A40FC82	- standard - SSL - SSL EV - Code Signing - S/MIME
11	1	CN = Certum Extended Validation CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum Trusted Network CA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	f18734d48395862a0c3af6e4b927381a	rsaEncryption	4096 bits	sha1withRSA	2013-01-24	2028-01-24	AF19834886EE88D4BC7F3907AEAC1BE6033C7C65D85D8EC482AE5F2D8C849F8B	7816C7B0566B46783B1C15D8A28D8B0D20CFEB20B3D13F79446E15C4A51C91DF	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
12	1	CN = Certum Class I CA, O = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL	CN = Certum Trusted Network CA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	b47de80b8745855c6e9c4e6bb189abb4	rsaEncryption	4096 bits	sha1withRSA	2013-01-24	2028-01-24	5ABEECD5E79ED66D094BFEAD76BE58BBFAC93A9AAC8EC6FC21E35C8664A390BE	337AC56F39FB8877B9F0524554B755D1835A807FFC9058DFC6DE1B707F696123	- standard - SSL - SSL EV - Code Signing - S/MIME
13	1	CN = SpaceSSL CA, O = Unizeto Technologies S.A., OU = SpaceSSL Certification Authority, C = PL	CN = Certum Global Services CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	2539661f537d7b5cea2c999db63c083e	rsaEncryption	2048 bits	sha1withRSA	2014-04-16	2024-03-02	467DF2EEFF6D1A02D081E5D1CF893BD48D1BC03A6D602BDBDBB3F4976B889982	3A29828F3DDCA85FBD18628A052476431360AD67E89420282771C1236207D43C	- standard - SSL - SSL EV - Code Signing - S/MIME
14	1	CN = Certum Domain Validation 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	26ddd22b46c9c44d5a694d39807e72ad	rsaEncryption	2048 bits	SHA256with RSA	2014-09-11	2027-06-09	4B801B24D1AFC92E7B9F3270BFCB0F31430BF151D2A87D6F6E205FB5D3DC12B2	129FB5DE501E24041CD14A81075FD1CDE257408D4A353E636912E38BDDA2D3FB	- standard - SSL - SSL EV - Code Signing - S/MIME
15	1	CN = Certum Organization Validation 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	00b5ad0f63854cc4622e4b3923b2900216	rsaEncryption	2048 bits	SHA256with RSA	2014-09-11	2027-06-09	E751AF78A36BA498ED1A95D8E500F1D37B3761343069089CE9D581AA8DF35FAB	FD02362244F31266CAFF005818D1004EC4EB08FB239AAFAAAFFF47497D6005D6	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
16	1	CN = Certum Extended Validation 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	00c5a2d3f6eb4d193c17a90aa38a296e54	rsaEncryption	2048 bits	SHA256with RSA	2014-09-11	2027-06-09	1D82D7F1FA9711B377367EFEE640C26A06DBCD99D2A17B0FFAB0316D92788AC3	6C47D365C13BC8CC3D6DEF5D8F07AB8DBEA3C8D4945D651AA9854A9C9A3CC71C	- standard - SSL - SSL EV - Code Signing - S/MIME
17	1	CN = nazwaSSL, O = nazwa.pl S.A., OU = http://nazwa.pl, C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	528a14cda91a4b45a5637c03647f42c1	rsaEncryption	2048 bits	SHA256with RSA	2014-09-30	2024-09-27	B0F86924C397D7F40422330DFE72F2F988A8C643B4A411922BB73E323F70C9BC	749CC529CDAAB9AE2858147C4B001AE1D5BE058FC165C3E74AF9704131C5E1C1	- standard - SSL - SSL EV - Code Signing - S/MIME
18	1	CN= Shoper® SSL O = Dreamcommerce S.A., OU = 2Dreamcommerce S.A., C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	4e4f65e01f6b735afe9c072c607c4abf	rsaEncryption	2048 bits	SHA256with RSA	2014-09-30	2024-09-27	BB6AB346B01D98DAFE31ECACBA98BDC7B50D31A2D8673B93E0E4D3867FFAC45E	277CF4B65F530FCC07285EF89D8311884884004E4F2C7DBE7CA006E96536CD62	- standard - SSL - SSL EV - Code Signing - S/MIME
19	1	CN = SpaceSSL CA, O = Unizeto Technologies S.A., OU = SpaceSSL Certification Authority, C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	3d5dfff1eb3144fc808cfa46bf8cc17b	rsaEncryption	2048 bits	SHA256with RSA	2014-09-30	2024-09-27	00E5F2E90785457AF72DEDA3CBD5541D57344D8E8DA1F0D0B1E15071A0D1968C	65DE322A1EF7AFFEDEB7387138C26060825B08CC27E1992DD9EAC8337297957B	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
20	1	CN = Yandex CA, O = Yandex LLC, OU = Yandex Certification Authority, C = RU	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	e40547830e0c6452976f7a3549c0dd48	rsaEncryption	2048 bits	SHA256with RSA	2015-01-21	2025-01-18	2CD15EFB2738FCD65B255CA7A7101E01DF9BAD4DC43F019BB7017A55E52323F6	C333B61638B0315FA801CCE21CC4EA96EF7F65A3999450186A99D19BB20128F7	- standard - SSL - SSL EV - Code Signing - S/MIME
22	1	CN = www.lh.pl, O = LH.pl Sp. z o.o., OU = LH.pl, C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	0a21d80af794ed9046816a3c5db3dd33	rsaEncryption	2048 bits	SHA256with RSA	2015-01-28	2025-01-25	48F7E52533DF6D183A356624C6B39AA96163914CFA77A7F17BC3CE72D3F2105A	59A3456E750E325FCB1359DC29E828189B4982C119C64FACFD6728711B30532F	- standard - SSL - SSL EV - Code Signing - S/MIME
22	1	CN = Certum Digital Identification 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	66daef03db8461916b25ba83fb174e13	rsaEncryption	2048 bits	SHA256with RSA	2015-04-21	2027-06-09	41D72A22FD8E3CDB03EF9C37D9DF6D303C9A8B6F82973491B7FE3D8B4598C1B5	0F672D92A0B06CEE948F03B272502602C6E37D2A2AD694A31D5DE313196E9282	- standard - SSL - SSL EV - Code Signing - S/MIME
23	1	CN = nazwaSSL, O = nazwa.pl sp. z o.o., OU = http://nazwa.pl, C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	606c62dc97d1a0392ee9cb12b21d6dd9	rsaEncryption	2048 bits	SHA256with RSA	2015-12-31	2025-12-28	016E94F2A3EA935D78ADF976B008621229B63DFD26ABF45BFC17964A554088FE	A69C59966EBBCDFEC7F4FF0288C86FF60356FA7860208B93B43A095B0600CC1E	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
24	1	CN = Certyfikat SSL O = home.pl S.A., C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	311d7edde4920208bbd85ef7262bba	rsaEncryption	2048 bits	SHA256with RSA	2016-06-08	2026-06-06	E4F2788C1D6C8C9E64C776B40ECDA7A093DCD3B64E6FFCB5BD1D6D375B7916C4	A95F23B52AF10895886FB65323D29A9876EA7D396F805E4CA280D561C26E3DAD	- standard - SSL - SSL EV - Code Signing - S/MIME
25	1	CN= 4fastssl.com, O = 3S2N Sp. z o.o., OU = 3S2N Sp. z o.o., C = PL	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	7c0876ae51f52f127a953247b4834b62	rsaEncryption	2048 bits	SHA256with RSA	2017-04-18	2027-04-16	B0DED8BF4A93CA35BE0494DF933755BD8C5DD44C5417097772FC1B2F3B64E457	31AC346B31073DC0D134E29FC212CC4A15ED3530EEA1EDCFC8DACB36492D5DE4	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
26	1	CN = TrustAsia DV SSL CA - C3, O = TrustAsia Technologies Inc., C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	f15cc09c2dcc610208b80ea3057243a9	rsaEncryption	2048 bits	SHA256withRSA	2017-10-23	2027-05-14	9190F5AC0872754718C7F8878B043EC6C87DDA275CE42AF2BECE3ED8C7909E99	C25F1E96000BC36E2AA5CD54BF24F48B76890A162E1AD8E104992650510626C2	- standard - SSL - SSL EV - Code Signing - S/MIME
27	1	CN = TrustAsia OV SSL CA - C3, O = TrustAsia Technologies Inc., C = CN	CN = Certum Global Services CA OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	309e97b6ccd8672842fa2059592920a8	rsaEncryption	2048 bits	SHA256withRSA	2017-10-23	2027-05-14	8446516F46817F287FD72A22EC82369B44D0FC90A42605B07CB6678BB9595076	7A142B1A5E16215183A13E840A862A437E293D9366921DB07EDB54F138AC0D78	- standard - SSL - SSL EV - Code Signing - S/MIME
28	1	CN = TrustAsia EV SSL CA - C3, O = TrustAsia Technologies Inc., C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	178666a8554accbfe73457e6451a686c	rsaEncryption	2048 bits	SHA256withRSA	2017-10-23	2027-05-14	DF3BE1AFD14BA31FFA1CAF822EF47FC04E172908EDA83BF334FC52AF433C8DE6	BC0878CBBC4E0DAF7A9DA464AB16262A235BFDAED33B9F9569BA18FF34997580	- standard - SSL - SSL EV - Code Signing - S/MIME
29	1	CN = TrustOcean Certification Authority, O = QiaoKr Corporation Limited, C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	1509b3b352d6689b5a7272f372e7e028	rsaEncryption	2048 bits	SHA256withRSA	2017-10-23	2027-05-14	02A9F195518772E132C01750C6770EA0C05DDB0FA274D95FA031274E0131E52E	A416A2BA490C454E23B85BF087DB7B137F4F47D9747E60F8692FF4C8DF0E062B	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
30	1	CN = GDCA TrustAUTH R4 DV SSL CA G2, O = "Global Digital Cybersecurity Authority Co., Ltd.", C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	9e9cb69426c45cc4306d3e1cc2a79efc	rsaEncryption	2048 bits	SHA256with RSA	2018-01-26	2027-05-20	71FB108FAF19908C9B935817EA18B359A72813B86FA8936E8CDBB6134DE7FF78	6CDF9DCBF3510A3BB402761D62D0C5E4E7AFC51D9CFF01F02BD53256DC567ADF	- standard - SSL - SSL EV - Code Signing - S/MIME
31	1	CN = GDCA TrustAUTH R4 OV SSL CA G2, O = "Global Digital Cybersecurity Authority Co., Ltd.", C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	b0efd02a81bf1ce89f7a18c294e4c33c	rsaEncryption	2048 bits	SHA256with RSA	2018-01-26	2027-05-20	5FF9034491B2A3582BE57812E211A4035247D7D45B9F4FA301DC51906C0E7E2B	E81B01F9F5692CF3823C6FD35886542BFAEEFC5EA94F4E246E42C4A9FC5FE8AB	- standard - SSL - SSL EV - Code Signing - S/MIME
32	1	CN = GDCA TrustAUTH R4 EV SSL CA G2, O = "Global Digital Cybersecurity Authority Co., Ltd.", C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	d5f83e8ddaf67c8829e89016b7877d13	rsaEncryption	2048 bits	SHA256with RSA	2018-01-26	2027-05-20	1A57EB460C3D8D6F55342ED8D5A5C3B13B0787A7543C012E77C7E1CCE3BE11D6	6869242CD8AD2AC77BC028947BC7D0C4F6E9CBF0899D65709810D89F94B5D70D	- standard - SSL - SSL EV - Code Signing - S/MIME
33	1	CN = GoGetSSL Domain Validation CA SHA2, O = EnVers Group SIA, OU = GoGetSSL Certification Authority, C = LV	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	b0a20c009da4b5eba644c79c228270c5	rsaEncryption	2048 bits	SHA256with RSA	2018-01-26	2027-05-20	A75F396D8C6214EF99C0A015FA6227787C3EBEE1F6AEAA589033B28CA37B0F21	B5F62EC38131CD14B1FC95B877F4D210BE4BFACC7E6A6AA1422D89E34B7AC4C1	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
34	1	CN = GoGetSSL Business Validation CA SHA2 O = EnVers Group SIA, OU = GoGetSSL Certification Authority, C = LV	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	c557eac31e7e21fb026f20e096b6bad4	rsaEncryption	2048 bits	SHA256withRSA	2018-05-20	2027-05-20	5A125BD51863EBE5177ED55491E555E4288E6707D617881DB24115BF25A93713	18958D03AFB409687A1BC263860D0D735A25A004AB60E0F0E45D6333587437AE	- standard - SSL - SSL EV - Code Signing - S/MIME
35	1	CN = GoGetSSL Extended Validation CA SHA2, , O = EnVers Group SIA, OU = GoGetSSL Certification Authority, C = LV	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	27c6c981d3d15d0f78377121f8233e00	rsaEncryption	2048 bits	SHA256withRSA	2018-05-20	2027-05-20	04F102C7AC0DABDD29F20BB462927515CD03C7B8744A692D7832B9C439974F96	EEDA15BA000B006EAD49A21BBE769F3BA6CE75C9249F0114D8DD882DFC0F2C1B	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
36	1	CN = Abitab SSL Domain Validated, O = Abitab S.A., OU = IDdigital, C = UY	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	101d422255e1fe416660c480177611	rsaEncryption	2048 bits	SHA256withRSA	2018-08-22	2027-05-02	F708359316E5FDEC3EE7EEEDA5AB6D3CFBBF8FD6E00DCB64B9C364A4E1BE53AB	E67D18639367C5B29BF7A5683B56B0F0C23155C8FE9452BCFE51681436023742	- standard - SSL - SSL EV - Code Signing - S/MIME
37	1	CN = Abitab SSL Organization Validated O = Abitab S.A. OU = IDdigital, C = UY	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	f0d59415c6decb4f888f2837e606810f	rsaEncryption	2048 bits	SHA256withRSA	2018-08-22	2027-05-02	13818B0ED4C4C0EED409E02D3BC89B6CEBBA14B671488502FDF07321B339995E	EEF9066424C23508E9C65F84671B14E16DA1BEC358E75FC6382ECA070AE861BE	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
38	1	CN = Abitab SSL Extended Validation O = Abitab S.A., OU = IDdigital, C = UY	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	63e9b37a0fea72231484b67eed4ba9e3	rsaEncryption	2048 bits	SHA256with RSA	2018-08-22	2027-05-02	CB629A02C53555F25F5914183DEAB71D5C4ED4656BC12C38C46ABBAD226DC882	93B281BD81D83CF986659DFFD0AF57993B92E6E4614162539F750524CE11BBCB	- standard - SSL - SSL EV - Code Signing - S/MIME
39	1	CN = QIDUOCA 2018 DV SSL, O = "Suzhou Qiduo Information Technology Co., Ltd.", OU = Domain Validated SSL, C = CN	CN = Certum Global Services CA SHA2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL	d8f02e7002e2f53fa539ea253a264d3a	rsaEncryption	2048 bits	SHA256with RSA	2018-08-22	2027-05-02	1E34F5D6EC5BD1D5D7C599E1E8552611654750BB52B4F6752CBCD161D91DA2A6	E372221266A330DD13EB1388DFAAF1FAB11DF254B63385CB637BFEF8FB5FB675	- standard - SSL - SSL EV - Code Signing - S/MIME

CA #	CERT. #	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	DIGEST ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
40	1	CN=IKARUS mail.security O=IKARUS Security Software GmbH C=AT	CN=Certum Global Services CA SHA2 O=Unizeto Technologies S.A. OU=Certum Certification Authority C=PL	83E06505E0B5D1ACDC0858527EF53177	rsaEncryption	2048 bits	sha256WithRSAEncryption	2023-06-13	2027-05-20	89A399FD6194EAEC5F21CA956B28273EF5C4CB06	002E6D642C2EE639B40FBED1020EE7BEEDF2E521F9B2BDE46C958D32E6353E9D	- standard - S/MIME
41	1	CN=Certum SMIME RSA CA O=Asseco Data Systems S.A. C=PL	CN=Certum Trusted Root CA O=Asseco Data Systems S.A. OU=Certum Certification Authority C=PL	0CE13227A82CE6A3D0F357C36CB61E86	rsaEncryption	4096 bits	sha512WithRSAEncryption	2023-08-01	2038-07-23	66FBC30FBEF4BFE09CC9AB4DDE4719BDC0CAA668	ABC27367A236EC90F91B6457CBAEF942BF657C9C97E87F4A2CC8302160A67AB8	- standard - S/MIME
42	1	CN=Certum SMIME ECC CA O=Asseco Data Systems S.A. C=PL	CN=Certum EC-384 CA O=Asseco Data Systems S.A. OU=Certum Certification Authority C=PL	8A2527AD93733CC2276C488C437433B2	id-ecPublicKey	384 bits	ecdsa-with-SHA384	2023-08-01	2038-07-23	4997927052227E313FC3415B31F792AD03AA0693	1131362B431A474A0BC5F2BFEC5B3CC5B5D5E1BDE9FAE64C50AC8E26CE295B56	- standard - S/MIME
43	1	CN=Certum Global Services SMIME RSA CA O=Asseco Data Systems S.A. C=PL	CN=Certum Trusted Root CA O=Asseco Data Systems S.A. OU=Certum Certification Authority C=PL	0BA3582EDD7AB32A93A1E32B27D04ACA	rsaEncryption	4096 bits	sha512WithRSAEncryption	2023-08-08	2038-07-30	7F9D5C72FF6C3AFF2827DBC12916724E6119E908	41C7155655F8DC27BA1128248980067D46836B6450CF4E1062C8C2772606773F	- standard - S/MIME
44	1	CN=IKARUS mail.security O=IKARUS Security Software GmbH C=AT	CN=Certum Global Services SMIME RSA CA O=Asseco Data Systems S.A. C=PL	2D4FAFA5AF0BBCDF2C8DFC4AC4C043E3	rsaEncryption	2048 bits	sha256WithRSAEncryption	2023-08-08	2028-08-01	7FD938B526A34BEFAE211E7D3214DA0CAEED0956	8006BF194B9856EAC36A0A1A4B88EAEB54018F06F8CED90E7669D5F373D71D59	- standard - S/MIME
45	1	CN=Certum SMIME G3 E39 CA O=Asseco Data Systems S.A. C=PL	CN=Certum SMIME ECC Root CA O=Asseco Data Systems S.A. C=PL	A72E8411370F77620930A9650C28726D	id-ecPublicKey	384 bits	ecdsa-with-SHA384	2024-04-02	2039-03-20	BB9B6C54980F670484CF28F7C5CE256CC6722E22	D286F91B30895B02FE557BC22B5B65A423833E3AE17FEEAA15534A657FAC1DAA	- standard - S/MIME

46	1	CN=Certum SMIME G3 R39 CA O=Asseco Data Systems S.A. C=PL	CN=Certum SMIME RSA Root CA O=Asseco Data Systems S.A. C=PL	048204600550ABECB16E9260C21FD87A	rsaEncryption	4096 bits	sha512WithRSAEncryption	2024-04-02	2039-03-20	B76F2EE26411FCE41E407957BE6E75A4547B4EDC	B7627C4F868250E2829D635435E52FB4CE71AA98D1DA449CBD6B6BBC43608C1F	- standard - S/MIME
47	1	CN=TrustAsia SMIME CA 2025 O=TrustAsia Technologies, Inc. C=CN	CN=Certum Trusted Root CA O=Asseco Data Systems S.A. OU=Certum Certification Authority C=PL	2E8B1C6883532694EFE243A3F83335	rsaEncryption	4096 bits	sha512WithRSAEncryption	2025-01-15	2035-01-03	151995DD372B19373DEC853DB922D9808D3D609C	E802A9679975DAD283EC482666D82A7CE54E1086873510F5A4CC49BD913CECAC	- standard - S/MIME

Cross-certificates

The cross certificates listed below are in scope only for the criterion 7.1 “Subordinate CA and Cross Certificate Lifecycle Management”.

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 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	0023e8290d71950418c008597e42f7481b	rsaEncryption	2048 bits	sha1withRSA	2008-10-22	2025-12-30	AA2630A7B617B04D0A294BAB7A8CAAA5016E6DBE604837A83A85719FAB667EB5	2D87FF20FE8AD2305DFB6F3992867ED2BF4FE3E1346212C4345991AAC02266E9	- standard - SSL - SSL EV - Code Signing - S/MIME
2	1	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	939285400165715F947F288FEFC99B28	rsaEncryption	2048 bits	sha1withRSA	2008-10-22	2027-06-10	AA2630A7B617B04D0A294BAB7A8CAAA5016E6DBE604837A83A85719FAB667EB5	949424DC2CCAAB5E9E80D66E0E3F7DEEB3201C607D4315EF4C6F2D93A917279D	- standard - SSL - SSL EV - Code Signing - S/MIME
3	1	CN = SSL.com Root Certification Authority RSA, O = SSL Corporation, L = Houston, ST = Texas, C = US	CN = Certum Trusted Network CA, = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	e4270495f68c91d6d0ec7b494ea4df1c	rsaEncryption	2048 bits	SHA256withRSA	2018-09-11	2023-09-11	d1c45377ebdcd618cd1651dc2e02c21d751e5aa9fcd1b3431ff6ecf6a31348fa	ACF718DF838E640051777D1947F51620E8D804BA186553AE52FC9811B5D34B8B	- standard - SSL - SSL EV - Code Signing - S/MIME **Expired**
4	1	CN = SSL.com EV Root Certification Authority RSA R2, O = SSL Corporation, L = Houston, ST = Texas, C = US	CN = Certum Trusted Network CA, = Unizeto Technologies S.A., OU = Certum Certification Authority, C = PL,	62f812a35f52bd74b718d610ac4b4783	rsaEncryption	2048 bits	SHA256withRSA	2018-09-11	2023-09-11	7cd67c248f69d83fc2f9bb01dcb1f7ad67a363d046043796d0984c3a231f6bb0	B97176F21B6ED64609267B2D1A2A9FAF0C4DEBD44644DC85EB6AE986FC867D56	- standard - SSL - SSL EV - Code Signing - S/MIME **Expired**
5	1	CN=Certum Trusted Network CA 2; 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	1BB58F252ADF23004928C9AE3D7EED27	rsaEncryption	4096 bits	SHA384WithRSA	2021-05-31	2029-09-17	6B3B57E9EC88D1BB3D01637FF33C7698B3C9758255E9F01EA9178F3E7F3B2B52	08E7EAC998A62C4155CC4CBC5EDA32F5B41A12C012F29AB3433BD366348149F0	- standard - SSL - SSL EV - Code Signing - S/MIME
6	1	CN = Certum Trusted Root CA O = Asseco Data Systems S.A., OU = Certum Certification Authority	CN = Certum Trusted Network CA O = Unizeto Technologies S.A.,	00D8E0744B5824919FBD08847DF72020FA	rsaEncryption	4096 bits	sha512WithRSAEncryption	2023-09-19	2028-09-19	8CFB1C75BC02D39F4E2E48D9F96054AAC4B34FFA	FB13890C7AB14FF7B94B2714503E31123BFDD340FC4D979743166E0469B47A88	- standard - SSL - SSL EV - Code Signing - S/MIME

		C = PL	OU = Certum Certification Authority C = PL									
7	1	CN = Certum EC-384 CA O = Asseco Data Systems S.A., OU = Certum Certification Authority C = PL	CN = Certum Trusted Network CA O = Unizeto Technologies S.A., OU = Certum Certification Authority C = PL	DAFD4BF54121E027D68696225F1FCEE8	id-ecPublicKey	384 bits	sha512WithRSAEncryption	2023-09-19	2028-09-19	8D06667424763AF389F7BCD6BD477D2FBC105F4B	B72450ABF5047A8AF63EC9D87E331484850B1849A2550A82A86DB6B41ED38760	- standard - SSL - SSL EV - Code Signing - S/MIME

Attachment B: List of Bugzilla issues noted during the period under review.

Mozilla Bug # Link	Description	Date Reported	Date Resolved	Criteria
1879845	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** Certum has issued 96 SMIME certificates since January 16, 2024, with invalid content in SubjectAlternativeName. On January 16th 2024, Certum deployed a version with a new interface for retail customers, featuring a new flow for selecting CN for S/MIME. The problem appeared when a customer changed CN to a value differrent than emial - tit was copied into the SAN field, instead of keeping the email value. When the chosen CN happened to be an email, SAN had the correct entry - the email. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** All certificates affected by this mis-issuance have been revoked. New test scenarios were created for this and similar errors. Linting for SMIME issuing process was implemented.	12.02. 2024	02.10. 2024	S/ MIME 2.2.13
1888689	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** 49 of Asseco Data Systems' CRLs violated TLS BRs (v2.02): Section 7.2 and RFC 5280. These CRLs contained the revoked certificates field, however no revoked certificates were present. During the testing process, Certum did not detect that some CRLs disclosed to the CCADB were in violation of the TLS Baseline Requirements (BRs) and, by extension, RFC 5280. Specifically, these CRLs contained the revoked certificates field, but no revoked certificates were present. This was because Certum's testing was done on sample CRLs which did not include empty CRLs. Testing approach was to use pkilint on a limited number of samples, since Certum had configured the same profile for all the CRLs. Certum did not automate this testing process, but rather performed it manually. Certum made a wrong assumption that a few positive tests were enough to validate the CRLs. Certum overlooked the possibility of empty CRLs and did not include them as test scenarios. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** CRL module was updated by 2024-04-05**,** Manual tests were performed with pkilint for all CRLs by 2024-04-05, Linting for CRLs issuing process was introduced.	29.03. 2024	02.10. 2024	RFC 5280: Sect. 5.1.2. 6 TLS BR 7.2

1904494	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** Cross-certificate SHA-256 FINGERPRINT 949424DC2CCAAB5E9E80D66E0E3F7DEEB3201C607D4315EF4C6F2D93A917279D was not included in 2024 S/MIME Audit statement. The primary cause of this issue was a lapse in the verification process during the audit compilation. The Compliance Team did not cross-reference the List of CA certificates for Audit with the Audit Report accurately, resulting in the omission of a cross-certificate in the S/MIME Audit Statement, despite its inclusion in the TLS/ EV TLS/ Code Signing Audit. The CA list was manually compiled, leading to an error where one cross-certificate was not identified as capable of issuing S/MIME. The verification of the CA list relies on a script that cross-references certificate fingerprints to determine their inclusion in the report. Both preliminary and final reports were checked against the initial list, which contained the error, hence the double-checking by the Compliance Team and Auditor Teams did not catch this specific mistake. In recent years, such issues were not encountered because the CA certificate lists for TLS/ EV TLS/ Code Signing Audit were verified and found to be accurate. This year, the error occurred due to the new S/MIME audit, which led to an incorrect update of the list. Furthermore, the CCADB ALV check-up was conducted for both preliminary and final audit statements and did not highlight the missing cross-certificate. The intermediate certificate was only identified as missing after the audit was concluded and the case was closed. The combination of these factors resulted in the cross-certificate being left out of the audit report, and the oversight was not discovered until after the case had been closed. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** A script for additional verification of SHA256 fingerprints included in audit reports has been created and tested. As a result, it returns a list of SHA256 fingerprints that were not included in the audit report even though they should have been. Certum will use it to verify the preliminary and then for final audit reports they receive from auditors.	25.06.2024	04.09.2024	BR 7.1.4.2.
1917571	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** An incident occurred where 4 S/MIME certificates were issued incorrectly due to discrepancies between the OrganizationIdentifier and Country field. This was discovered during a scan that identified similar issues in 6 certificates, 2 of which had already been revoked. The root causes included initial validator limitations and confusion over country names. To address this, linting for S/MIME certificates was implemented, and the process for generating OrganizationIdentifiers was improved. Future plans include adding ISO Country Codes next to country names in user interface to prevent recurrence. After Certum's first mis-issuance of S/MIME certificates that had a wrong OrganizationIdentifier, Certum had planned to solve the problem in two steps. The first step was to improve the validator of that field in Certum's system, ensuring that it checks for basic data integrity and compliance with the required format, reducing the chance of human errors when entering the number. The second step was to implement a mechanism that would fill the OrganizationIdentifier number and reduce the need to enter a number by hand.	09.09.2024	06.11.2024	BR 7.1.4.2.

	This incident is a result of multiple contributing factors: Initial Validator Limitations: The initial validator, implemented in December, did not verify if the Country in the OrganizationIdentifier matched the Country code. This oversight allowed the validation officer to mistakenly use "PL" instead of "CZ" for one of the certificates. Similar Country Names: Three out of four mis-issued certificates had incorrect country fields due to selection of the wrong country from the list. The confusion between "People's Republic of China (Chińska Republika Ludowa)" and "Republic of China (Republika Chińska)" contributed to the mis-issuance. Despite the names being similar, they represent different countries according to ISO-3166 standard. The validation officer did not catch this error, leading to the issuance of certificates with incorrect country information. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** Improvement completed in June, involved implementing a mechanism that fills the correct OrganizationIdentifier number based on the data provided by the client, and effectively reduced human errors and improved the accuracy of the information.			
1935393	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** On December 3, 2024, a Certum employee reviewed the CCADB and identified errors that appeared after a recent website update. During the review of new features Certum found that the current Certification Policy is older than 365 days. According to Section 2.3 of the Baseline Requirements, the CA is required to annually update a Certificate Policy and/or Certification Practice Statement. Additionally, Section 4 of the Mozilla Root Store Policy requires updates to the CP and CPS at least once every 365 days. This requirement was not met. The root cause of the incident was a gap in internal procedures and the reliance on individual methods for handling the annual update of non-audit documents. Both the CP and CPS updates were manually managed by a single individual. The previous person responsible for the updates had their own approach, which was not standardized. As a result, while the CPS update was completed, the CP update was overlooked due to a lack of clarity in the process. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** The procedure for documentation update was revised, specifying that the CP and CPS must be updated at least once every 365 days. An internal tracker for CP and CPS updates for employees responsible for the task was created. Update in the procedure for updating the CP and CPS. Creation of internal tracker for CP and CPS updates for employees responsible for the task. Implementation of the script which compares the list of CP and CPS from CCADB public report and alerts if they are about to expire.	05.12.2024	28.01.2025	EV BR 9.3.4 BR 7.1.6.3

1909203	**Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.** During scheduled network maintenance on 2024-07-21, Certum's infrastructure experienced a disruption that caused the unavailability. The scope of network maintenance concerned the replacement of network interfaces for networks within the organisation (part one of the work) and for public networks (part two of the work). The problem occurred during the second part of the network maintenance and was related to the incorrect setting of the route in the configuration. As a result, the following services were not available from the internet. The problem affected the following services which according to BR must be available 24x7: CP/CPS respond to revocation requests and Certificate Problem Report CRL OCSP The failure was resolved within about 1-2 hours, and since then all the services mentioned are working correctly. This incident did not affect the issuance of certificates. **List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.** Implement additional monitoring controls for network devices and traffic. Implement additional monitoring controls for services. Changing the configuration of CDN to automate traffic switching between Primary Origins Server and Secondary Origin Server. Add external monitoring for Certificate Problem Report. Improvements were implemented on time and strengthened controls which were insufficient to prevent this incident.	22.07.2024	04.09.2024	BR 7.1.