Audit Attestation

AKD d.o.o. ETSI Assessment 2020

Date: 15.06.2020

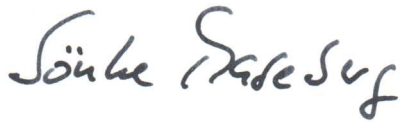
Provider: AKD d.o.o.
Service(s): Trust Service Provider Issuing EU Qualified Certificates

Registration Number: DSC.871

Conformity Assessment Body
Contact:
datenschutz cert GmbH
Konsul-Smidt-Straße 88a
28217 Bremen, Germany
office@datenschutz-cert.de

Accreditation Information: http://www.dakks.de/as/ast/d/D-ZE-16077-01-00.pdf

Bremen, 15.06.2020



Dr. Sönke Maserberg
Reviewer

Klaus-Werner Schröder
Lead Auditor

datenschutz cert

Conformity Assessment Body

1 Name: datenschutz cert GmbH

VAT No.: DE 260 557 462

Address: Konsul-Smidt-Str. 88a, 28217 Bremen, Germany

Internet: www.datenschutz-cert.de

The Certificate of Accreditation is available at

http://www.dakks.de/as/ast/d/D-ZE-16077-01-00.pdf

Head of Conformity Assessment Body: Klaus-Werner Schröder

Inquiries shall be sent to office@datenschutz-cert.de

National Accreditation Body

2 Name: Deutsche Akkreditierungsstelle GmbH

Address: Spittelmarkt 10, 10117 Berlin, Germany

Internet: www.dakks.de

Trust Service Provider Assessed

3 Name: AKD d.o.o.

Address: Savska cesta 31, HR-10000 Zagreb, Croatia

www.akd.hr

Audit Details

4 Requirements: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2

5 Kind of audit: stage 1 audit, stage 2 audit

6 Goal of audit: assessment of conformity

7 The full annual audit (stages 1 and 2) is based on

- documentation provided by the organization assessed,
- interviews with employees and management,
- remote audit.

Summary

8 The audit was performed as a full annual audit of the trust service provider AKD d.o.o., HR-10000 Zagreb, Croatia. The stage 2 audit was conducted after successful completion of stage 1 audit. The audit (stage 1 and stage 2) took place from 31.03.2020 to 30.05.2020 and covered the period from 30.05.2019 to 30.05.2020.

9 Due to travel restrictions because of the Covid-19 pandemic the audit was carried out as a remote audit supported by live transmission of video streams. The possible impact on the audit results was assessed in advance by the auditor to be low or very low.

10 The audit was performed according to the European Standards ETSI EN 319 401 (C), ETSI EN 319 411-1 (B), and ETSI EN 319 411-2 (A).

11 The trust services audited are described in the following policy and practice documents of the trust service provider:

[1] AKD d.o.o., AKD PKI, Certificate Policy, Edition 2.4, Status: May 1, 2020

[2] AKD d.o.o., HRIDCA Certification Practice Statement, Edition 2.2, Status: May 1, 2020

[3] AKD d.o.o., eOI PKI Disclosure Statement, Version 1.1, Status: 20.04.2018

[4] AKD d.o.o., KIDCA Certification Practice Statement, Edition 1.4, Status: May 1, 2020

[5] AKD d.o.o., kIDCA Policy Disclosure Statement (n), Edition 1.3, Status: 15.07.2019

[6] AKD d.o.o., kIDCA Policy Disclosure Statement (l), Edition 1.1, Status: 15.07.2019

Issuing Certificates signed by AKDCA Root

12 The full annual audit covered the service provided under the CA certificate:

Issuer: CN = AKDCA Root; O = AKD d.o.o.; C = HR

Serial No.: 46 1f a5 41 93 fa 83 52 (hex); 5052939008007111506 (dec)

Valid from: June 1, 2015, 17:08:08 (CET)

Valid to: June 1, 2030, 17:08:08 (CET)

Certification Authority: CN = HRIDCA; O = AKD d.o.o.; C = HR

Information on Algorithm: SHA256RSA; Length of RSA modulus: 4096 bits

Public key (ASN.1-notation):

30 82 02 0a 02 82 02 01 00 e3 bf f7 20 3b 3d 5f 41 7f d1 f6 21 77 bc f3 73 2e dd 6c bb e9 1f f2 9a e8 a8 50 a2 50 29 be 90 5f 5c 5a 5a 80 89 43 4e 1b da e7 a6 3c a3 1b 3b 90 d5 09 f4 c9 6f 4b ff 35 76 1e b2 22 6e 43 b4 b9 b1 d9 28 74 4e bc 9e 68 52 13

88 af 15 e4 a4 a5 3e a4 77 7a 45 29 07 bb 84 18 62 a5 f0 b0 ff 78 c4 62 e6 ff cc bd 4e 3e db 53 48 a2 c1 b3 66 8f 6e d1 81 5b 58 0a 34 49 46 20 48 d1 e6 e5 51 20 78 db ba 2c 85 6b 59 9f 34 16 20 ab 02 57 09 2b 80 ba 59 e6 14 cc 96 2b ea 99 2d b2 00 eb fc 7e a9 2e 1d 7c 24 c7 5b 59 25 b9 a7 a1 36 04 ba 9a 86 f6 c4 e0 60 a2 71 13 88 29 5e 34 46 9c 02 40 aa f9 4b cd 77 8b b7 d9 ce 40 5d 53 bf 30 87 e9 e4 26 ec d8 0a 4d 02 95 bd 55 5e cb 46 2a dd 1c 8b b1 9e 4a ef aa b1 cc ad 78 aa bb bc 1c 65 a7 52 fa f9 9f d1 1d fc 12 9a 49 b8 8d 2f 41 7d 65 ed 3e ab 75 34 25 c0 45 0c 29 4d 72 85 04 17 0d 37 e1 25 33 c9 43 9c fb d8 b2 67 90 29 f5 90 44 58 3e ff f8 59 b4 4e cd 4c bd d5 6c aa 57 73 5f f0 c7 eb 93 c3 12 c4 de c7 83 39 fd 4b ae 9f be 6d 95 34 b3 d8 91 00 ec 79 1e 44 32 8c ba 22 30 e5 c5 44 08 7e 22 86 f1 3a 4d 88 db a5 59 fa bd 3e 6e c5 10 a7 76 59 e9 20 66 e5 e5 b6 1d 0b c7 96 51 b2 fa 58 59 d5 51 05 7a 38 09 f8 57 46 ed ad 12 df 40 b6 0d 67 9d a5 0c 0c 82 da ee 72 c4 7f 8e 31 8e 05 02 ea ed 04 4b 77 d9 3a f0 5e 61 1d 0a f7 cb d7 db 0f 64 e5 85 45 72 85 0c c8 fd d9 eb 73 90 a9 a9 6b d7 73 ae 3d 48 d7 7d 8e ae 17 61 57 90 3a b5 48 16 fe 69 47 dd ee ee a8 b7 d9 98 4e 25 33 04 69 61 fa e5 8b 71 9f 9c e9 b9 99 30 83 9a 4e fe 27 17 4b 43 94 2b 3c 94 9c e4 a1 f0 88 9d 69 1a 5e e0 98 fc 86 4c 9a 2f 0b 02 03 01 00 01

Thumbprint of the certificate (SHA256):

558f46ff83b6dd3ccd0ceba5db7bb1803c830ba74c3c8d7db41e1218e8834ab4

13 This service is referred to as “HR electronic IDentity”. The service issues certificates for nonrepudiation and authentication where the private signing keys reside in a secure signature creation device (Croatian electronic identity card). Furthermore, the service issues certificates for electronic identification. The documents governing the service are identified above, cf. [1], [2], and [3].

14 The full annual audit covered the service provided under the CA certificate:

Issuer: CN = AKDCA Root; O = AKD d.o.o.; C = HR

Serial No.: 34 7a 05 b5 f8 c0 2d 94 (hex), 3781341116251516308 (dec)

Valid from: December 28, 2016, 15:28:53

Valid to: December 28, 2031, 15:28:53

Certification Authority: CN = KIDCA; O = AKD d.o.o.; C = HR

Information on Algorithm: SHA256RSA; Length of RSA modulus: 4096 bits

Public key (ASN.1-notation):

30 82 02 0a 02 82 02 01 00 c6 71 2e 36 c1 22 13 08 bc a6 b0 a1 d7 93 3b 2e 5f 64 3a b9 ca 73 27 1a 27 2f c7 f3 31 0e c3 f7 53 98 e4 28 d9 e8 20 ab 13 43 67 03 15 83 7e b1 62 80 8f d2 e6 48 68 91 6a 0e 7d 29 a5 6e 0d f1 3f 00 b4 e6 cb 40 cc 26 9c e6 a0 e1 65 5c 17 6f cc 08 65 fa 0e 22 72 3a 8d dc f5 3e 2e 6e d0 ec 27 7e cf 65 80 e3 14 94 6a 53 43 06 fb 7b 2c 4b b6 c1 d9 2a 35 2a 42 e5 89 2f 09 2f 06 c2 5e 90 eb d7 6f 46 aa 68 6a ab 80 69 77 4b 85 14 c7 26 cc 2f 63 81 5a f8 02 39 7f 6f ba f8 85 24 ef 2a d2 8e 25 87 da 31 6d a4 b1 37 c1 53 f3 20 c1 e7 d2 cf 95 34 7c ba bd e3 2e 6e 6a ea e6 c8 22 6d 4d 4c 74 5e d9 d2 1e 4e cb 4e fe 4e 9e 07 f5 3b a1 64 9f 7a ca fe 83 ce 6d 32 a6 c1 c8 f8 6e 41 17 29 47 84 c6 54 b5 72 8d 1e fd 78 18 bb a3 71 5a 46 c9

a7 15 f9 11 c0 3e 55 9a 1e a3 2c 17 f0 0c b3 89 d7 5d e8 20 2f e8 7c 65 36 60 88 28 ba 82 47 32 c9 c1 5e 1e 73 48 c8 3d c2 1a 4d 66 c8 2a c2 d0 34 89 7d b6 91 e1 23 01 0b 28 ce 76 b1 45 9d d9 8f 43 2f 79 10 5a 93 04 6f 0c 68 59 cd 77 53 63 28 69 0e 29 5b a9 69 4b 0c fc 34 ff 43 25 67 fd de 2f a4 cc 6e 23 bf 29 b8 4f f5 00 90 c9 54 bd 06 e8 3a e4 58 e1 16 29 71 80 57 9d 29 9d fd 8f fc c0 c5 56 7e 1e 36 49 79 49 82 96 f9 91 bc a7 63 39 ff 7d 46 82 74 ab b5 f1 b0 e0 24 4a cf e6 a5 ba 5b a0 8e 1f c8 cb ec 33 90 82 6c ba 13 0a 1d 3c 07 f7 f7 38 61 51 39 15 9b 41 70 15 d6 68 a1 82 9d f9 06 58 53 e5 fa 49 6d 38 98 e5 4c 88 2e 3f 19 18 ea c8 3f 55 d5 15 b0 e3 0d 31 a3 24 03 b4 4f 17 86 52 6e 70 5a ad fb 0d 2c dd d3 59 61 08 77 61 3b bf 56 ef 77 32 44 40 f0 1a 38 17 77 49 06 d8 c5 d2 2a 3f 42 a9 b8 4f 0b 02 03 01 00 01

Thumbprint of the certificate (SHA256):

2086b14325b7f2260e2829f8380b0c48b4136c204a877aced69aaca5d8ad8fde

15 This service is referred to as “HR commercial IDentity”. The service issues certificates for nonrepudiation and authentication for natural as well as legal persons where the private signing keys reside in a secure signature or seal creation device (AKD-eID-Card 1.0). Furthermore, the service issues certificates for electronic identification. In addition, the service issues certificates for nonrepudiation and authentication for natural as well as legal persons where the private signing keys is generated and managed by a qualified trust service provider (i. e. AKD d.o.o.). Those keys are applied when residing in a qualified signature or seal creation device, respectively. The service is referred to as “KIDCA remote services”. The documents governing the services are identified above, cf. [1], [4], [5], and [6].

Root Certificate AKDCA Root

16 The full annual audit covered the root CA certificate, which issued the aforementioned subordinate CA certificates. It is identified by

Issuer: CN = AKDCA Root; O = AKD d.o.o.; C = HR

Serial No.: 3c 72 d6 29 d0 83 c1 83 (hex), 37813411162515163 08 (dec)

Valid from: May 25, 2015, 14:59:36

Valid to: January 19, 2038, 05:14:07

Certification Authority: CN = AKDCA Root; O = AKD d.o.o.; C = HR

Information on Algorithm: SHA256RSA; Length of RSA modulus: 4096 bits

Public key (ASN.1-notation):

30 82 02 0a 02 82 02 01 00 b5 1c 1f b3 92 80 7c 0f 20 99 be ec 7e 35 c6 6d 1e 74 33 6c 13 76 ba b5 3d 22 b6 9f 8a 05 40 65 19 56 3c 8f f5 1d 59 f4 6e 7f b6 00 1a 00 ac 4a 35 ed a7 7d 1a 7e d5 14 3b 2f 2e d8 3f d3 67 10 ef 26 e0 50 9e e9 3f 66 15 90 eb 2c b5 87 6a 09 de a4 38 f8 98 aa e5 a3 37 96 c2 e7 b9 f1 0b 9c d6 8a 34 e3 f1 26 3b ff 47 55 4c 08 b8 3d c7 9a f5 6a 96 2f 9d d5 c1 67 9a 53 0d 00 e8 f9 f1 f9 21 9e 4c 86 ed db 1c 02 bf 24 03 25 35 fe d2 01 f6 87 c4 5d 27 97 14 f1 66 86 e1 c8 79 ea 29 90 26 9a 4b d7 08 71 dc 3c 08 e1 cf 2a 99 ad 56 78 c8 d4 55 fe 36 bd 45 2c 0b 60

65 bb 8b a1 8e 14 35 64 49 9b f4 f1 39 48 ba 11 a7 07 58 5c b0 fd 1c e2 80 21 eb a7
78 2d 5c 7d ad 34 cc f6 46 0f 52 8a 33 21 1b a5 3e dd c7 aa c1 1f a8 f2 25 75 57 1c 60
f7 5b f7 69 67 b4 64 65 1b c7 18 39 5f 3f c4 e7 7f a3 ce 5f f7 af 89 bc ee fc ff 19 d7
00 b6 16 c3 db b2 27 2e 3a 06 50 0f 4e c4 d1 ca 7f 1b 6d 2b 7d a5 51 04 f6 2d 7a 9a
b6 96 66 da ec 49 e3 7b 9b 7f 0d 50 b3 98 68 f5 f2 f4 59 a6 fb fc 7c ec 58 37 0f 72
87 46 dc 81 2b 58 f8 1b 9f be e0 76 8d bf 32 28 26 f9 ff 4a cc 61 8b 4e 9a 98 81 a8
d6 d5 fa aa 67 2a d2 f5 1b 21 da ff d1 49 9e 29 32 82 30 26 17 1f 69 c4 8c 73 88 6d
af d2 19 32 73 c7 63 92 38 8e e7 13 bd 0c 64 09 ae a3 22 36 4f a4 c2 0c 94 bb b6 8a
01 ea 4b 45 8a 62 fa 6b 95 94 fc 24 07 46 35 82 62 37 8f 96 32 c7 03 82 22 59 6e 58
61 51 35 47 28 d3 27 89 cf 14 36 2c 10 5a 97 ef 39 2f 85 ec 8d 88 e7 a8 d4 05 7e ab
36 16 2d 3f 10 d9 e8 61 db 19 c9 55 ed c3 d8 b4 95 1d e5 dd 2e 2d 5c 75 a8 7b 6b 95
d0 2e da 26 8e 1f a2 53 0c a3 fb 98 59 50 1e 71 02 03 01 00 01

Thumbprint of the certificate (SHA256):

2b923b061c4d8d413922829 0c5c660979233a52deb1307f908f583c5a5c5063c

17 The audit was completed successfully without critical findings.

18 For contact information, see page 2.

References

(A) ETSI EN 319 411-2 V2.2.2 (2018-04): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

(B) ETSI EN 319 411-1 V1.2.2 (2018-04): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

(C) ETSI EN 319 401 V2.2.1 (2018-04): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

(D) DIN EN ISO/IEC 17065:2013-01 „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“

(E) ETSI EN 319 403 V2.2.2 (2015-08): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers, Version 2.2.2, 2015-08, European Telecommunications Standards Institute

(F) ETSI EN 319 421 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

End of Audit Attestation