Valencia, July 31st, 2019

Independent Assurance Report

To the Certification and Electronic Signing Service of the Valencian Regional Ministry of Finance and Economic Model (hereinafter ACCV):

Scope

We have been engaged, in a reasonable assurance engagement, to report on ACCV management's assertion that for its Certification Authority (CA) operations at Valencia, SPAIN, throughout the period from May 1st,2018 to April 30th, 2019 for its CAs as enumerated in Appendix 1, ACCV has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - ACCV's Certification Practice Statement (CPS) – v4.0.5; and
  - Certification Policy (CP) for Qualified certs. for citizens on a secure device – v7.0
  - CP for Qualified certificates for citizens on software support – v6.0
  - Certification Policy (CP) for Qualified certificates for public employees – v5.0
  - CP for Qualified certificates for public employees – Intermediate level – v3.0
  - CP for Qualified certificates for Electronic Office on a secure device – v4.0.2
  - CP for Qualified certificates for Electronic Office on software support – v4.0.2
  - CP for Qualified Public Admin. eSeal Certificates on a secure device – v4.0
  - CP for Qualified Public Admin. eSeal Certificates on software support – v4.0
  - CP for Qualified certificates for Websites Authentication – v4.0.2
  - CP for Qualified eSeal certificates for entities on a secure device – v3.0
  - CP for Qualified eSeal certificates for entities on software support – v2.0
  - CP for Qualified certificates for employees belonging to a company on a secure device – v4.0
  - CP for Qualified certificates for employees belonging to a company on software support– v2.0
  - CP for Code Signing certificates – v3.0
  - CP for VPN Server certificates – v3.0
  - CP for Application certificates – v4.0
  - CP for Qualified certificates for public employees with pseudonym on a secure device – v3.0
  - CP for Qualified certificates for public employees with pseudonym on software support- v2.0
  - CP for Qualified certs. for legal representatives on a secure device – v1.0

    - CP for Qualified certs. for legal representatives on software support – v1.0
    - CP for Qualified certificates for legal representatives on a secure device for entities without legal personality – v1.0
    - CP for Qualified certificates for legal representatives on software support for entities without legal personality – v1.0
    - ACCV's TimeStamp Certification Policy – v2.0

- maintained effective controls to provide reasonable assurance that:
    - ACCV's Certification Practice Statement is consistent with its Certificate Policies.
    - ACCV provides its services in accordance with its Certificate Policies and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by ACCV); and
    - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1.

ACCV makes use of external registration authorities for specific subscriber registration activities as disclosed in ACCV's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

ACCV does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

ACCV'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 v2.1.

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.

Auren 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 ACCV's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle 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 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 ACCV 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, ACCV'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 from May 1st, 2018 to April 30th, 2019, ACCV 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 v2.1.

This report does not include any representation as to the quality of ACCV's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.1, nor the suitability of any of ACCV's services for any customer's intended purpose.

Use of the WebTrust seal

ACCV's use of the WebTrust for Certification Authorities 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.

F. Mondragon, Auditor
auren
Valencia, SPAIN
July 31st, 2019

APPENDIX 1 List of CAs in Scope

Root CAs
1. ACCVRAIZ1
OV SSL Issuing CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
EV SSL Issuing CAs
None
Private Trust Issuing CAs
None
Non-EV Code Signing Issuing CAs
3. ACCVCA-120
EV Code Signing Issuing CAs
None
Secure Email (S/MIME) CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
Document Signing CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
Adobe CAs
None
Timestamp CAs (TSU Issuer)
1. ACCVRAIZ1
Other CAs
None

CA Identifying Information for in Scope CAs

CA#	Cert #	Subject	Issuer	serialNumber	Key Algorithm	Key Size	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	1	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	5EC3B7A6437FA4E0	rsaEncryption	4096 bit	sha1WithRSAEncryption	May 5 09:37:37 2011 GMT	Dec 31 09:37:37 2030 GMT	D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD	9A6EC012E1A7DA9DBE34194D478AD7C0DB1822FB071DF12981496ED104384113
2	1	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-110	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	337545D22DA86E4E	rsaEncryption	4096 bit	sha256WithRSAEncryption	May 7 12:25:39 2015 GMT	Dec 31 23:59:00 2026 GMT	92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E	E9327A347CBE1CB94CDC9AA54CB31B6E43D68968D17D09CE326A091BFC2F0B11
2	2	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-110	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	20DC654677BFC815	rsaEncryption	4096 bit	sha1WithRSAEncryption	Oct 13 11:22:04 2011 GMT	Dec 31 23:59:00 2026 GMT	92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E	1345C2D39AE4B65CCA71E88E9A2B29C71DC913F952E935A812B004DBA7AE7957
3	1	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-120	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	41F69CD2BD80C0B7	rsaEncryption	4096 bit	sha256WithRSAEncryption	Jan 27 14:06:42 2015 GMT	Dec 31 23:59:00 2026 GMT	E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5	2DE620F2D1200AA90B16C3CCF670FD7ED14379AB06FA8B031CFEF8DA051EA5A2
3	2	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-120	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	6482C4AB654B00A6	rsaEncryption	4096 bit	sha1WithRSAEncryption	Oct 13 14:55:04 2011 GMT	Dec 31 23:59:00 2026 GMT	E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5	3BC51856040AD7FF6683AA85A0D34F9EA680CD23C37CB8A0423B0F89A24405B9
4	1	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-130	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	5394E41746519E96	rsaEncryption	4096 bit	sha256WithRSAEncryption	Jan 15 10:23:24 2015 GMT	Dec 31 23:59:00 2026 GMT	E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2	572BF899FD774362DC19219625ECC157BB55434EA5166D5758DC4B4F890D6653
4	2	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVCA-130	C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1	51777CA6B938AF06	rsaEncryption	4096 bit	sha1WithRSAEncryption	Oct 14 10:07:28 2011 GMT	Dec 31 23:59:00 2026 GMT	E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2	8F7CC455E9A5507804120655D7139186253E43B00422E734263A0769D2F89F7D

ACCV MANAGEMENT'S ASSERTION

The Certification and Electronic Signing Service of the Valencian Regional Ministry of Finance and Economic Model (hereafter the ACCV) operates the Certification Authority (CA) services known as the Root Certification Authority **ACCVRAIZ1** and its subordinates **ACCVCA-110, ACCVCA-120** and **ACCVCA-130**, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management
- Certificate status information processing (using an online repository)

The management of ACCV is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 ACCV's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ACCV management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ACCV management's opinion, in providing its Certification Authority (CA) services at Valencia (Spain), throughout the period May 1, 2018 to April 30, 2019, ACCV has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - ACCV's Certification Practice Statement (CPS) – v4.0.5; and
  - Certification Policy (CP) for Qualified certs. for citizens on a secure device – v7.0
  - CP for Qualified certificates for citizens on software support – v6.0

- Certification Policy (CP) for Qualified certificates for public employees – v5.0
- CP for Qualified certificates for public employees – Intermediate level – v3.0
- CP for Qualified certificates for Electronic Office on a secure device – v4.0.2
- CP for Qualified certificates for Electronic Office on software support – v4.0.2
- CP for Qualified Public Admin. eSeal Certificates on a secure device - v4.0
- CP for Qualified Public Admin. eSeal Certificates on software support - v4.0
- CP for Qualified certificates for Websites Authentication – v4.0.2
- CP for Qualified eSeal certificates for entities on a secure device – v3.0
- CP for Qualified eSeal certificates for entities on software support – v2.0
- CP for Qualified certificates for employees belonging to a company on a secure device – v4.0
- CP for Qualified certificates for employees belonging to a company on software support– v2.0
- CP for Code Signing certificates – v3.0
- CP for VPN Server certificates – v3.0
- CP for Application certificates – v4.0
- CP for Qualified certificates for public employees with pseudonym on a secure device – v3.0
- CP for Qualified certificates for public employees with pseudonym on software support- v2.0
- CP for Qualified certs. for legal representatives on a secure device – v1.0
- CP for Qualified certs. for legal representatives on software support – v1.0
- CP for Qualified certificates for legal representatives on a secure device for entities without legal personality – v1.0
- CP for Qualified certificates for legal representatives on software support for entities without legal personality – v1.0
- ACCV's TimeStamp Certification Policy – v2.0

- maintained effective controls to provide reasonable assurance that:
  - ACCV's Certification Practice Statement is consistent with its Certificate Policies
  - ACCV provides its services in accordance with its Certificate Policies and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by ACCV); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

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

CA Key Lifecycle 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 Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services

- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

ACCV does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

GENERALITAT
VALENCIANA
Conselleria d'Hisenda
i Model Econòmic

Enrique Valls Muñoz
Deputy Director General for ICT
Planning and Coordination

July 30, 2019

ATTACHMENT A1
LIST OF CAs IN SCOPE

Root CAs
1. ACCVRAIZ1
OV SSL Issuing CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
EV SSL Issuing CAs
None
Private Trust Issuing CAs
None
Non-EV Code Signing Issuing CAs
3. ACCVCA-120
EV Code Signing Issuing CAs
None
Secure Email (S/MIME) CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
Document Signing CAs
2. ACCVCA-110 3. ACCVCA-120 4. ACCVCA-130
Adobe CAs
None
Timestamp CAs (TSU issuer)
1. ACCVRAIZ1
Other CAs
None

ATTACHMENT A2

CA IDENTIFYING INFORMATION FOR IN SCOPE CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	5EC3B7A6437FA4E0	rsaEncryption	(4096 bit)	sha1WithRSAEncryption	May 5 09:37:37 2011 GMT	Dec 31 09:37:37 2030 GMT	D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD	9A:6E:C0:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:13
2	1	CN=ACCVCA-110, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	337545D22DA86E4E	rsaEncryption	(4096 bit)	sha256WithRSAEncryption	May 7 12:25:39 2015 GMT	Dec 31 23:59:00 2026 GMT	92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E	E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11
2	2	CN=ACCVCA-110, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	20DC654677BFC815	rsaEncryption	(4096 bit)	sha1WithRSAEncryption	Oct 13 11:22:04 2011 GMT	Dec 31 23:59:00 2026 GMT	92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E	13:45:C2:D3:9A:E4:B6:5C:CA:71:E8:8E:9A:2B:29:C7:1D:C9:13:F9:52:E9:35:A8:12:B0:04:DB:A7:AE:79:57
3	1	CN=ACCVCA-120, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	41F69CD2BD80C0B7	rsaEncryption	(4096 bit)	sha256WithRSAEncryption	Jan 27 14:06:42 2015 GMT	Dec 31 23:59:00 2026 GMT	E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5	2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2
3	2	CN=ACCVCA-120, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	6482C4AB654B00A6	rsaEncryption	(4096 bit)	sha1WithRSAEncryption	Oct 13 14:55:04 2011 GMT	Dec 31 23:59:00 2026 GMT	E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5	3B:C5:18:56:04:0A:D7:FF:66:83:AA:85:A0:D3:4F:9E:A6:80:CD:23:C3:7C:B8:A0:42:3B:0F:89:A2:44:05:B9
4	1	CN=ACCVCA-130, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	5394E41746519E96	rsaEncryption	(4096 bit)	sha256WithRSAEncryption	Jan 15 10:23:24 2015 GMT	Dec 31 23:59:00 2026 GMT	E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2	57:2B:F8:99:FD:77:43:62:DC:19:21:96:25:EC:C1:57:BB:55:43:4E:A5:16:6D:57:58:DC:4B:4F:89:0D:66:53
4	2	CN=ACCVCA-130, OU=PKIACCV, O=ACCV, C=ES	CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES	51777CA6B938AF06	rsaEncryption	(4096 bit)	sha1WithRSAEncryption	Oct 14 10:07:28 2011 GMT	Dec 31 23:59:00 2026 GMT	E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2	8F:7C:C4:55:E9:A5:50:78:04:12:06:55:D7:13:91:86:25:3E:43:B0:04:22:E7:34:26:3A:07:69:D2:F8:9F:7D