

# IIC TSA — Key Ceremony Record R1

**Publication notice.** This document is published by HTTPS CARD — INTERNET IDENTITY CARD LIMITED (England and Wales, company no. 09168431) for the IIC TSA time-stamping service at <https://tsa.internetidentitycard.com/tsa>. IIC TSA is designed to RFC 3161 / RFC 5816. It is **not** a qualified trust service under eIDAS or UK eIDAS, and it is not certified, accredited or recognised by any authority. IIC TSA and VerifBox ([verifbox.com](https://verifbox.com)) belong to the same company: for VerifBox users, IIC TSA is not an independent third party. Use of the service is subject to the [IIC TSA terms of use](#).

*Record 1 — ceremony of 10 October 2026. Published 11 October 2026. This record describes the generation of the production root key "IIC TSA Root R1" and the certification of the first TSA signing key generation, tsa-2026-a, as required by the IIC TSA Practice Statement (section 5). It contains only public material: certificates, fingerprints, identifiers and the hash of the script used. No private key, passphrase or private path appears in it.*

**What this record is.** The Practice Statement describes how keys are generated; this record states what was done, when, with which tool, and what came out of it, so that anyone can check that the root certificate they hold is the one produced that day. It is written by the operator about its own ceremony: there was no witness and no auditor (section 7). Operator: HTTPS CARD - INTERNET IDENTITY CARD LIMITED, company no. 09168431, 124 City Road, London EC1V 2NX, United Kingdom.

## 1. Summary

| Item        | Value                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ceremony    | R1, production root key and first TSA certificate                                                                                                                                                                                                  |
| Date        | 10 October 2026 (UTC), between the end of the test acceptance and 17:29 UTC                                                                                                                                                                        |
| Where       | Offline, on the operator's own computer; single operator, no witness                                                                                                                                                                               |
| Script      | <code>ceremony/hierarchy.sh</code> of the IIC TSA repository, commands <code>init</code> , <code>leaf</code> , <code>cr1</code> ; SHA-256 <code>0d9fdf025d55acd6af7376a05feae3bd8ae6227a164475f9b0b0966665804b19</code>                            |
| Environment | OpenSSL 3.4 or later (the script refuses to run otherwise); the reference environment is <code>ceremony/Dockerfile</code> (Debian trixie-slim with OpenSSL), SHA-256 <code>0e9c4b7103e2b7f97699941eb3d4be3f46d9265d0a52685bb1a1222533506ba8</code> |

| Item                   | Value                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Root certificate       | IIC TSA Root R1, SHA-256 86:52:E3:D1:3E:72:5F:7C:75:7C:FA:05:3D:64:13:60:AC:A4:43:CF:6C:09:D7:D6:DD:D4:4B:EA:85:1E:D3:B9    |
| TSA certificate        | IIC TSA tsa-2026-a, SHA-256 E4:F9:8E:7A:ED:CD:1A:07:D8:1C:A5:9D:1C:19:92:AB:E7:85:7A:2C:A1:CC:8D:F6:9F:72:05:FF:AD:34:FB:E8 |
| First root CRL         | number 1, issued 10 October 2026 17:29:19 UTC, next update 10 October 2027 17:29:19 UTC, no revoked certificate             |
| First production token | serial 0xD22448FD5AD33BD7A393BB6024B28126 , 10 October 2026 18:02:46 UTC                                                    |

## 2. The root key and certificate

| Field                          | Value                                                                                                                                                                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject                        | C=GB, O=HTTPS CARD - INTERNET IDENTITY CARD LIMITED, CN=IIC TSA Root R1                                                                                                                                                                   |
| Key                            | EC P-384 (secp384r1), generated with <code>openssl genpkey</code> during the ceremony                                                                                                                                                     |
| Serial                         | E6:4B:0C:EE:5C:28:B9:08:B9:03:A4:CE:5E:F0:F5:75 (16 random bytes)                                                                                                                                                                         |
| Validity                       | 10 October 2026 00:00:00 UTC to 9 October 2056 23:59:59 UTC (30 years)                                                                                                                                                                    |
| Signature                      | ECDSA with SHA-384, self-signed                                                                                                                                                                                                           |
| Extensions                     | basicConstraints critical CA:TRUE pathlen:0; keyUsage critical keyCertSign, cRLSign; subjectKeyIdentifier 44:1D:B9:C3:F4:6C:C4:20:C9:5A:84:F4:4F:32:6E:54:F5:0D:8F:88 (RFC 7093 method 1, leftmost 160 bits of SHA-256 of the public key) |
| SHA-256 of the DER certificate | 8652e3d13e725f7c757cfa053d641360aca443cf6c09d7d6ddd44bea851ed3b9                                                                                                                                                                          |

The private key was written only in encrypted form (PKCS#8, AES-256-CBC, scrypt), under a passphrase that exists on paper only and has never been typed into a networked system or written in any file or message. The key never left the ceremony computer: only `root.pem`, `root.crl` and the TSA certificate were carried to the cloud. Two USB backups of the ceremony folder were made and verified; the working copy was then deleted. The root key is used for two things only: to certify a TSA key generation, and to sign the root CRL.

### 3. The TSA signing key and certificate

The TSA signing key is not generated in the ceremony: it is the Cloud KMS key `tsa-2026-a` of the production project (EC P-256, SOFTWARE protection level, created on 10 October 2026), whose public key, SHA-256 `3d11b2af1f9a52d960e79c5aae3553c087a8627e32628a0ab51c0cb83a8a0d02`, was exported from Cloud KMS and brought to the ceremony computer. The script checks that it is a P-256 public key before certifying it ( `leaf tsa-2026-a` ).

| Field                        | Value                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject                      | C=GB, O=HTTPS CARD - INTERNET IDENTITY CARD LIMITED, CN=IIC TSA tsa-2026-a                                                                                                                                                                                                                                               |
| Issuer                       | IIC TSA Root R1                                                                                                                                                                                                                                                                                                          |
| Key                          | EC P-256, the public key of Cloud KMS key version tsa-2026-a                                                                                                                                                                                                                                                             |
| Serial                       | F3:DB:B1:C3:E9:99:37:F5:3B:10:22:06:19:55:7B:34                                                                                                                                                                                                                                                                          |
| Validity                     | 10 October 2026 00:00:00 UTC to 9 January 2038 23:59:59 UTC (135 months)                                                                                                                                                                                                                                                 |
| Signature                    | ECDSA with SHA-384, by the root                                                                                                                                                                                                                                                                                          |
| Extensions                   | extendedKeyUsage critical timeStamping only; subjectKeyIdentifier 92:98:6A:23:D0:63:9A:26:9D:87:B1:10:76:55:3D:D4:81:F0:0D:E2 ; authorityKeyIdentifier = the root's subjectKeyIdentifier; CRL distribution point <a href="https://tsa.internetidentitycard.com/tsa/crl">https://tsa.internetidentitycard.com/tsa/crl</a> |
| Verification at the ceremony | <code>openssl verify -x509_strict -purpose time stampsign -CAfile root.pem tsa-tsa-2026-a.pem</code> : OK                                                                                                                                                                                                                |

The certificate is valid for 135 months so that tokens can be validated long after issuance; under the policy the key signs for at most 15 months before the next generation is certified at a further ceremony, recorded as R1 is here.

### 4. The first CRL

The root CRL number 1 was issued at the end of the ceremony ( `crl` ): last update 10 October 2026 17:29:19 UTC, next update 10 October 2027 17:29:19 UTC, signed ECDSA with SHA-384, no revoked certificate. It is published at <https://tsa.internetidentitycard.com/tsa/crl> and mirrored by VerifBox at <https://verifbox.com/.well-known/iic-tsa-racine.crl>. It is re-issued at least yearly, and immediately after any revocation, in a ceremony of the same kind ( `crl` only ).

## 5. Steps as performed

1. Test acceptance passed on the test project (43 of 43 checks) with a separate test hierarchy ("IIC TSA Test Root R1", test policy 1.3.6.1.4.1.67100.1.1.9.1); the test root is distinct from the production root and is never installed in a production trust store.
2. Cloud KMS key tsa-2026-a created in the production project; its public key exported.
3. Ceremony computer offline. hierarchy.sh init : root key generated and encrypted, root certificate issued (section 2), CRL files initialised.
4. hierarchy.sh leaf tsa-2026-a <public key> : TSA certificate issued and verified (section 3).
5. hierarchy.sh crl : CRL number 1 issued (section 4).
6. Fingerprints of the root and TSA certificates read on screen and recorded in the Practice Statement; two USB backups of the ceremony folder made and verified; working copy deleted.
7. root.pem, root.crl and tsa-tsa-2026-a.pem carried to Cloud Shell and installed in the production service; production acceptance passed at 18:22 UTC (40 of 40 checks); first production token at 18:02:46 UTC.

## 6. How to check this record

- Fetch the root at <https://tsa.internetidentitycard.com/tsa/root.pem> or from <https://verifbox.com/.well-known/iic-tsa.json>, and compare `openssl x509 -noout -fingerprint -sha256` with section 2. The same fingerprint is printed on <https://www.internetidentitycard.com/tsa> and in the Practice Statement.
- Any IIC TSA token carries the TSA certificate (requests are sent with certReq TRUE): `openssl ts -reply -in token.tsr -token_out | openssl pkcs7 -inform DER -print_certs` shows the certificate of section 3; `openssl ts -verify -CAfile root.pem` validates the chain.
- The script and Dockerfile hashes identify the exact tool used; the script is part of the IIC TSA repository published by the operator.

## 7. Limits

This is the operator's own record, with no witness, no auditor and no hardware security module: the root is a software key on an offline computer, held by one person, with the compensating controls described in the Practice Statement (sections 3 and 10). IIC TSA is designed to RFC 3161 / RFC 5816; it is not a qualified trust service and nothing here is a certification.

## History

| Record | Date       | Content                                                                |
|--------|------------|------------------------------------------------------------------------|
| R1     | 2026-10-11 | First publication: ceremony of 10 October 2026, root R1 and tsa-2026-a |

---

© 2026 Htpps Card — Internet Identity Card Ltd, 124 City Road, London EC1V 2NX, United Kingdom. UK Company No. 09168431. Governed by the laws of England and Wales.