Bugzilla ID:1067887

BugZilla Summary: SAPO Trust Centre CA Root Certificates

# General Information about the CA’s associated organization

|  |  |
| --- | --- |
| **CA Company Name** | South African Post Office Limited |
| **Website URL** | [www.postoffice.co.za](http://www.postoffice.co.za) ; www.trustcentre.co.za |
| **Organizational Type** | Public Corporation |
| **Primary Market/Customer Base** | General Public |
| **Impact to Mozilla Users** | The SAPO Trust Centre CA has its own Roots and does not hang off any other Roots. The CA service is accredited to WebTrust and South African Accreditation Authority. All Mozilla users accessing secure web sites (https over ssl), sending and receiving emails, Signing documents using the advanced electronic signature as per ECT Act (South African Law). Sending and receiving encrypted email (S/MIME) will use the service. |
| **Inclusion in other major browsers** | Yes. Internet Explorer |
| **CA Primary Point of Contact** | POC 1  direct email:katekani.hlabathi@postoffice.co.za  direct email 2: katekani@trustcentre.co.za  Email alias:caadministrator@trustcentre.co.za  CA Phone number: +27 (21)8513853/4  Title/Department : Trust Centre  POC2:  Name: Thami Batyashe  email:thami.batyashe@postoffice.co.za  alias:gm@trustcentre.co.za |

# Technical information about each root certificate

## 2.1 SAPO CLASS 2 ROOT CA

|  |  |
| --- | --- |
| **Certificate Name** | SAPO Class 2 Root CA |
| **Certificate Issuer Field** | E = pkiadmin@trustcentre.co.za  CN = SAPO Class 2 Root CA  OU = SAPO Trust Centre  O = South African Post Office Limited  L = Somerset West  S = Western Cape  C = ZA |
| **Certificate Summary** | SAPO Class 2 Root Certificate signs the SAPO Class 2 CA (intermediate). This issuing CA issues Class 2 personal certificates used for email encryption and low level assurance, issued off the SAPO Trust Centre website. |
| **Mozilla Applied Constraints** | Not applicable |
| **Root Cert URL** | <https://www.trustcentre.co.za/ca_certs/c2rootcert2014-b64.cer> |
| **SHA1 Fingerprint** | ‎ed b3 cb 5f b4 19 a1 85 06 62 67 e5 79 15 54 e1 e2 8b 63 99 |
| **Valid From** | 15 September 2010 |
| **Valid To** | 14 September 2030 |
| **Certificate Version** | V3 |
| **Certificate Signature Algorithm** | SHA1RSA |
| **Signing Parameters** | RSA 2048 bits |
| **Example Certificate** | Attached: |
| **CRL URL** | <https://pki.trustcentre.co.za/crl/c2rootca.crl>  <https://pki.trustcentre.co.za/crl/sapo_c2ca.crl>  Section 20.6 (CRL Issuance Frequency) on the cps <https://www.trustcentre.co.za/docs/c2cacps.pdf>  CRL’s update frequency : 24 hours |
| **OCSP URL** | N/A |
| **Requested  Trust  Bits** | Client Authentication, Secure Email, Code Signing, Time Stamping |
| **SSL Validation Type** | N/A |
| **EV  Policy  OID(s)** | N/A |
| **Non-sequential serial numbers and entropy in cert** | 13 Bytes |
| **Response to CA Communications** |  |

**CA Hierarchy information**

|  |  |
| --- | --- |
| **CA  Hierarchy** | SAPO CLASS 2 ROOT CA  SAPO CLASS 2 CA  (Internally operated) |
| **Externally  Operated  SubCAs** | Not applicable |
| **Cross Signing** | Not applicable |
| **Technical  Constraints** | Not applicable. All certificates are issued within the SAPO Trust Centre hierarchy |

## 2.2 SAPO CLASS 3 ROOT CA

|  |  |
| --- | --- |
| **Certificate Name** | SAPO Class 3 Root CA |
| **Certificate Issuer Field** | E = pkiadmin@trustcentre.co.za  CN = SAPO Class 3 Root CA  OU = SAPO Trust Centre  O = South African Post Office Limited  L = Somerset West  S = Western Cape  C = ZA |
| **Certificate Summary** | SAPO Class 3 Root CA is used to sign the SAPO Class 3 CA and SAPO SSL CA. The SAPO Class 3 CA is an issuing CA for end entity certificates used within closed user communities and also for applications accessed by similar entities. The collective users are general members of the public needing authentication to the same application. Even though the focus is on “closed user groups”, the audience is the general public. An example would be SAPO customers accessing the Electronic Bulk Mail Delivery platform that are issued with the certificates for authentication.  The SAPO SSL CA issues SSL certificates for website authentication. These are Standard SSL, Wildcard and SAN certificates. |
| **Mozilla Applied Constraints** | Not applicable |
| **Root Cert URL** | <https://www.trustcentre.co.za/ca_certs/c3rootcert2014-b64.cer> |
| **SHA1 Fingerprint** | ‎‎b1 b2 36 4f d4 d4 f5 2e 89 b2 d0 fa f3 3e 4d 62 bd 96 99 21 |
| **Valid From** | 15 September 2010 |
| **Valid To** | 14 September 2030 |
| **Certificate Version** | V3 |
| **Certificate Signature Algorithm** | SHA1RSA |
| **Signing Parameters** | RSA 4096 bits |
| **Example Certificate** | <https://www.trustcentre.co.za/> |
| **CRL URL** | <https://pki.trustcentre.co.za/crl/c3rootca.crl>  <https://pki.trustcentre.co.za/crl/sapo_c3ca.crl>  <https://pki.trustcentre.co.za/crl/sapo_sslca.crl>  Section 20.6 (CRL Issuance Frequency) on the cps <https://www.trustcentre.co.za/docs/c3cacps.pdf>  CRL’s update frequency : 24 hours |
| **OCSP URL** | N/A |
| **Requested  Trust  Bits** | Server Authentication  Client Authentication  Secure Email  Code Signing  Time Stamping  IP security tunnel termination  IP security user |
| **SSL Validation Type** | OV |
| **EV  Policy  OID(s)** | N/A |
| **Non-sequential serial numbers and entropy in cert** | 13 Bytes |
| **Response to CA Communications** |  |

**CA Hierarchy information**

|  |  |
| --- | --- |
| **CA  Hierarchy** | SAPO CLASS 3 ROOT CA  SAPO SSL CA  SAPO CLASS 3 CA  (Internally operated) |
| **Externally  Operated  SubCAs** | Not applicable |
| **Cross Signing** | Not applicable |
| **Technical  Constraints** | Not applicable. All certificates are issued within the SAPO Trust Centre hierarchy |

## 2.3 SAPO CLASS 4 ROOT CA

|  |  |
| --- | --- |
| **Certificate Name** | SAPO Class 4 Root CA |
| **Certificate Issuer Field** | E = pkiadmin@trustcentre.co.za  CN = SAPO Class 4 Root CA  OU = SAPO Trust Centre  O = South African Post Office Limited  L = Somerset West  S = Western Cape  C = ZA |
| **Certificate Summary** | SAPO Class 4 Root Certificate signs the SAPO Class 4 CA (intermediate). This issuing CA issues Class 4 personal certificates with a Face to Face Validation of the subscriber. The certificates issued under this CA are also accredited under the ECT Act by the South African Accreditation Authority (SAAA). <http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-28-29.html> |
| **Mozilla Applied Constraints** | Not applicable |
| **Root Cert URL** | <https://www.trustcentre.co.za/ca_certs/c4rootcert2014-b64.cer> |
| **SHA1 Fingerprint** | ‎‎cc 7e a2 92 af 87 15 d7 4c a4 b4 15 f3 20 15 4b 24 f5 65 fd |
| **Valid From** | 15 September 2010 |
| **Valid To** | 14 September 2030 |
| **Certificate Version** | V3 |
| **Certificate Signature Algorithm** | SHA1RSA |
| **Signing Parameters** | RSA 4096 bits |
| **Example Certificate** | Attached, filename KatekaniClass4.p7b |
| **CRL URL** | <https://pki.trustcentre.co.za/crl/c3rootca.crl>  <https://pki.trustcentre.co.za/crl/sapo_c4ca.crl>  Section 20.6 (CRL Issuance Frequency) on the cps <https://www.trustcentre.co.za/docs/c4cacps.pdf>  CRL’s update frequency : 24 hours |
| **OCSP URL** | N/A |
| **Requested  Trust  Bits** | Server Authentication  Client Authentication  Secure Email  Code Signing  Time Stamping  IP security tunnel termination  IP security user |
| **SSL Validation Type** | N/A |
| **EV  Policy  OID(s)** | N/A |
| **Non-sequential serial numbers and entropy in cert** | 13 Bytes |
| **Response to CA Communications** |  |

**CA Hierarchy information**

|  |  |
| --- | --- |
| **CA  Hierarchy** | SAPO CLASS 4 ROOT CA  SAPO CLASS 4 CA  (Internally operated) |
| **Externally  Operated  SubCAs** | Not applicable |
| **Cross Signing** | Not applicable |
| **Technical  Constraints** | Not applicable. All certificates are issued within the SAPO Trust Centre hierarchy |

# Verification Policies and Practices

|  |  |
| --- | --- |
| **Policy Documentation** | Language that documents are in : **English**  CP: https://www.trustcentre.co.za/docs/cp.pdf  CPS: https://www.trustcentre.co.za/docs/cps.pdf  Relying Party Agreement: https://www.trustcentre.co.za/docs/RPA2014.pdf |
| **Audits** | WebTrust audits: <https://cert.webtrust.org/ViewSeal?id=1739> |
| **Baseline Requirements (SSL)** | Compliance to Baseline Requirements stated in CPS section 37.2.2 page 59 |
| **SSL Verification Procedures** | CPS: https://www.trustcentre.co.za/docs/cps.pdf  **Section 4.4 and 19.1** |
| **Organization Verification Procedures** | CPS: https://www.trustcentre.co.za/docs/cps.pdf  **Section 4.4 and 19.1** |
| **Email Verification Procedures** | A challenge-response mechanism is used to verify email addresses for all subscribers before they are added to the system. For Class 4 certificates and additional check using biometrics is checked against the National Identity System to ensure the user is who they say they are (Face to face identification).  CPS: https://www.trustcentre.co.za/docs/cps.pdf  **Section 4.4 and 19.1** |
| **Code Signing Subscriber Verification Procedures** | **No code signing certificates are issued at present.** |
| **Multi-factor Authentication** | Username/password with Biometrics is used for accounts that can cause the issuance of certificates. All activity is logged in a protected database. |
| **Network Security** | SAPO Trust Centre confirm that it has used Security best practices to design and protect the network used for Certificate Issuance. There is also Monitoring of all network activity, PKI issuance systems. All SSL certificate requests are approved by Internal trained operators following a documented procedure. Access reviews are done regularly and all systems are patched regularly. All certificate issuance can be shut down quickly by disabling (and also revoking) Certificate Authority Systems. We also confirm that we check for mis-issuance of certificates on a daily basis. |

# Response to Mozilla’s CA Recommended Practices

|  |  |
| --- | --- |
| **Publicly Available CP and CPS** | Comply with practice.  <https://www.trustcentre.co.za/docs/cps.pdf>  <https://www.trustcentre.co.za/docs/cp.pdf>  Revocation requirements : In CPS document, section 19.5  Online repository (CRL) : In CPS document, section 20.6, 20.7 |
| **CA Hierarchy** | One Root is used to sign the Class 2 and Class 4 Issuing CAs. The exception is the Class 3 Root that signs both the Class 3 Issuing CA and the SSL CA. The hierarchy is shown in section 2 above. |
| **Audit Criteria** | CA has being audited according to the WebTrust Services Principles and Criteria for Certification Authorities (version 2) |
| **Document Handling of IDNs in CP/CPS** | IDNs not supported |
| **Revocation of Compromised Certificates** | Revocation is supported and done as per CPS, section 20.4 |
| **Verifying Domain Name Ownership** | Domain Validation is performed against public databases (such as whois, CIPC in South Africa). We also send an email to the following list for verification:   * admin@domain * administrator@domain * hostmaster@domain * webmaster@domain * postmaster@domain |
| **Verifying Email Address Control** | A challenge response mechanism is used for all email address validations performed. Section 4.4.4 of cps (<https://www.trustcentre.co.za/docs/cps.pdf>) describes verification done for all classes of certificates. The actual procedure is listed in the CA certificate management procedures. |
| **Verifying Identity of Code Signing Certificate Subscriber** | **Code signing certificates not issued yet.** |
| **DNS names go in SAN** | **Subject Alternative Name** extension is a mandatory field, usually containing the **dns name** = |
| **Domain owned by a Natural Person** | We haven’t issued Domains owned by natural persons yet. However the recommendation will be followed. |

# Response to Mozilla’s List of Potentially Problematic Practices

|  |  |
| --- | --- |
| **Long-lived DV certificates** | DV certificates are valid for a period up to 24 months. All certificates requests are treated as new and checks are redone. All previous certificates are revoked. |
| **Wildcard DV SLL certificates** | All SSL certificates (including wildcard) are validated with domain ownership and subscriber validation. |
| **Email Address Prefixes for DV Certs** | Domain Validation is performed against public databases (such as whois, CIPC in South Africa). We also send an email to the following list for verification:   * admin@domain * administrator@domain * hostmaster@domain * webmaster@domain * postmaster@domain |
| **Delegation of Domain / Email validation to third parties** | All SSL certificate issuance are approved by internal SAPO Trust Centre personnel. External RA’s can submit certificate requests, but no certificate will be signed without the SAPO personnel approving (after validation) the documentation submitted. |
| **Issuing end entity certificates directly from roots** | No end entity certificates are issued directly from offline Roots. All end entity certificates are issued from the Intermediate CAs (see hierarchy provided) |
| **Allowing external entities to operate subordinate CAs** | No external entities operate CAs under the original CA’s root. |
| **Distributing generated private keys in PKCS#12 files** | We DO NOT generate Private Keys for SSL certificates. Subscribers generate these and paste the CSR during the application processes. |
| **Certificates referencing hostnames or private IP addresses** | We do not accept certificates for private IP addresses as these cannot be tied to the applying entity or individual. Only publicly registered FQDNs are allowed. |
| **Issuing SSL certificates for internal domains** | This does not happen as we thoroughly check the validity of the domain ownership |
| **OCSP Responses signed by a certificate under a different root** | OCSP is not currently activated. However we will ensure that this is signed by the Root in the same chain. |
| **SHA-1 Certificates** | Noted. We will ensure the end entity certificates expires before 2017 |
| **Generic names for CAs** | No generic names are used on the CN of our CA’s |
| **Lack of communication with end users** | We are contactable via telephone, email and via the web |
| **Backdating the notBefore date** | Backdating certificates is not performed. |