Bugzilla ID: 1067887
Bugzilla Summary: SAPO Trust Centre CA Root certificates

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	South African Post Office Limited (SAPO)
Website URL	http://www.postoffice.co.za/
Organizational type	Public Corporation
Primark 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 browsers	Yes. Internet Explorer
CA Primary Point of Contact (POC)	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

Certificate Name	SAPO Class 2 Root CA	SAPO Class 3 Root CA	SAPO Class 4 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
	ST = Western Cape
	C = ZA
		E = pkiadmin@trustcentre.co.za
		CN = SAPO Class 3 Root CA
		OU = SAPO Trust Centre
		O = South African Post Office Limited
		L = Somerset West
		ST = Western Cape
		C = ZA
			E = pkiadmin@trustcentre.co.za
			CN = SAPO Class 4 Root CA
			OU = SAPO Trust Centre
			O = South African Post Office Limited
			L = Somerset West
			ST = 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.	**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.	**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
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8505789	https://bugzilla.mozilla.org/attachment.cgi?id=8505790	https://bugzilla.mozilla.org/attachment.cgi?id=8505792
SHA1 Fingerprint	E4:55:01:60:8A:A1:EF:89:E2:7B:8C:D3:C3:B3:4C:03:B0:38:E6:D7	38:DD:76:59:C7:35:10:0B:00:A2:37:E4:91:B7:BC:0F:FC:D2:31:6C	20:A8:F5:FF:C4:3A:F4:A9:BC:89:88:1E:BF:99:20:FF:91:E9:FD:0A
Valid From	2010-09-15	2010-09-15	2010-09-15
Valid To	2030-09-14	2030-09-14	2030-09-14
Cert Version	3	3	3
Cert Signature Algorithm	SHA-1	SHA-1	SHA-1
Signing key parameters	2048	4096	4096
Test Website or Example Cert	Example cert provided in doc	https://www.trustcentre.co.za/	Example cert provided in doc
CRL URL	https://pki.trustcentre.co.za/crl/c2rootca.crl https://pki.trustcentre.co.za/crl/sapo_c2ca.crl	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	https://pki.trustcentre.co.za/crl/c3rootca.crl https://pki.trustcentre.co.za/crl/sapo_c4ca.crl

	CPS Section 20.6: CRLs for Certificates shall be issued at least once per day. CRL's update frequency: 24 hours	CPS Section 20.6: CRLs for Certificates shall be issued at least once per day. CRL's update frequency: 24 hours	CPS Section 20.6: CRLs for Certificates shall be issued at least once per day. CRL's update frequency: 24 hours
OCSP URL (Required for SSL certs)	None	None OCSP is required for SSL certs, according to the CA/Browser Forum's Baseline Requirements	None
Requested Trust Bits	Email (S/MIME)	Websites (SSL/TLS) Email (S/MIME)	Email (S/MIME)
SSL Validation Type	N/A	DV and OV	N/A
EV Policy OID(s)	N/A	N/A	N/A
Non-sequential serial numbers and entropy in cert	13 Bytes	13 Bytes	13 Bytes

CA Hierarchy information for each root certificate

CA Hierarchy	SAPO Class 2 Root CA has signed one internally-operated subordinate CA.	SAPO Class 3 Root CA has signed two internally-operated subordinate CAs. One for issuing SSL certificates, and one for issuing certificates for email and code signing.	SAPO Class 4 Root CA has signed one internally-operated subordinate CA.
Externally Operated SubCAs	https://www.trustcentre.co.za/ca_ra_issuing.php "… can offer you fully SAPO-hosted and customer-hosted certification authorities (CA) and registration authorities (RA) that are available in all the certificate classes." So, also have to provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	https://www.trustcentre.co.za/ca_ra_issuing.php "… can offer you fully SAPO-hosted and customer-hosted certification authorities (CA) and registration authorities (RA) that are available in all the certificate classes." So, also have to provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	https://www.trustcentre.co.za/ca_ra_issuing.php "… can offer you fully SAPO-hosted and customer-hosted certification authorities (CA) and registration authorities (RA) that are available in all the certificate classes." So, also have to provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist

	CPS section 6.1: Self Hosted CA's who perform all or some of the back-end functions to a point in the Certificate issuance chain, where the Certificate is ultimately issued by the Self Hosted CA. The RA function may be outsourced to Policy Authority approved entities.		
Cross-Signing	Currently None. CPS section 6.1: Cross-certification with other CAs is being considered for the future, but is not covered by this version of the CPS.	Currently None.	Currently None
Technical Constraints on Third-party Issuers	Registration Authorities are third-party issuers. What constraints are put on them? Customer-hosted CAs are third-party issuers. What constraints are put on them? CPS section 9.1.3: Issuing CA and Self Hosted CA Obligations CPS section 9.1.4: RA Obligations	Registration Authorities are third-party issuers. What constraints are put on them? Can they issue SSL certs? Customer-hosted CAs are third-party issuers. What constraints are put on them? **Can they issue SSL certs?** CPS section 18.1: Certificate applicants should submit their applications and credentials to the Post Office Trust Centre Root CA, Issuing CA or an approved RA. CPS section 18.2.3: SSL Server Certificates issued by the Post Office Trust Centre **or an Issuing CA** …	Registration Authorities are third-party issuers. What constraints are put on them? Customer-hosted CAs are third-party issuers. What constraints are put on them? CPS section 14: The Post Office Trust Centre and Issuing CAs will undergo at least an annual audit to demonstrate compliance with this CPS.

Verification Policies and Practices

Policy Documentation	Language that documents are in: English Document Repository: https://www.trustcentre.co.za/links.php CPS: https://www.trustcentre.co.za/docs/cps.pdf Relying Party Agreement: https://www.trustcentre.co.za/docs/RPA2014.pdf
Response to Recent CA Communication(s)	https://wiki.mozilla.org/CA:Communications Please review and provide your response to these CA Communications: https://wiki.mozilla.org/CA:Communications#May_13.2C_2014 https://wiki.mozilla.org/CA:Communications#January_10.2C_2013

Audits	Audit Type: WebTrust for CA version 2.0 Auditor: KPMG Auditor Website: http://www.kpmg.co.za Audit Report: https://cert.webtrust.org/SealFile?seal=1739&file=pdf (2014.08.28)
Baseline Requirements Audit Statement (SSL)	URL to BR audit statement: Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements (also have your auditor carefully review this wiki page) And provide a BR Audit Statement. How can we be sure that all of the Issuing CAs are also compliant with the Baseline Requirements, and get regular BR Audits?
Baseline Requirements Commitment to Comply (SSL)	The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. >> Compliance to Baseline Requirements stated in CPS section 37.2.2 page 59 I looked in the CPS, but I could not find reference to the Baseline Requirements.
Organization Verification Procedures	CPS section 4.4.1: Class 2 Certificates provide assurance that the subscribers' public key is associated with the email address supplied by the subscriber and that the distinguished name of the subscriber is unique and unambiguous within the Database of the CA. CPS section 4.4.2: Class 3 Certificates provide high level assurance and require validation of affiliation from the organisation that they are affiliated to. CPS section 4.4.3: Class 4 Certificates provide assurance of the identity of the Subscriber or Juristic Person based on the Subscriber or Authorised Representative of the Juristic Person having physically confirmed his/her identity to the CA or RA and validation of the Juristic Person by a third party validation check. CPS section 19.1: Valid authentication methods for a Juristic Person shall include, but not be limited to, a subset or a superset of the following: ... The Issuing CA confirms the identity of an applicant for a Class 3 SSL Server or Code Signing Certificate by conducting an independent investigation in order to determine whether: i. the applicant exists and conducts business at the address listed in the application; ii. the application was signed by a signatory who was a duly authorized representative of the applicant named therein. iii. the information contained in the application corresponds to the Juristic Persons registration details as published by CIPRO or the Master of the High Court. iv. If the Juristic Person applying is not a native entity to the Republic of South Africa special assessment will be made of the validity of the documents and particulars.

	CPS section 19.2.1. 19.2.2, and 19.2.3 describe authentication of Natural Persons for personal certificates.
SSL Verification Procedures	CPS section 4.4.4: Check of third-party database or other documentation showing proof of right to be linked to Juristic Person. Verification check by telephone (or comparable procedure) to confirm information in, and authorization of, the application. In the case of web server Certificates, confirmation that the applicant has the right to use the domain name to be placed in the Certificate. What does the following mean in section 18.2.5? CPS section 18.2.5: The authenticated common name value included in the subject distinguished name of a Class 3 SSL Certificate, however, is the generally accepted personal name of the affiliated natural person authorised to use the Juristic Person's private key, and the Juristic Person component is the registered name of the Juristic Person. CP section 19.1: Additional procedures are performed for SSL Server Certificates: The Issuing CA verifies that the applicant is the record owner of the domain name of the server that is the subject of the Certificate or is otherwise authorised to use the domain by the domain owner. Where in the CP/CPS is the following documented? 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
Email Address Verification Procedures	Where in the CP/CPS is this documented? A challenge response mechanism is used for all email address validations performed. CPS section 4.4.4: Class 2 -- Name and e-mail address search within the CA to ensure that the distinguished name is unique and unambiguous. Ensure that the Subscriber has access to given email address. Class 4 -- Distinguished Name, Affiliation and e- mail address search to ensure that the distinguished name is unique and unambiguous, plus personal presence, plus validation of non-South African Citizens ID credentials and capture of applicant's biometric data for validation with DHA in the case of South African Citizens. Juristic Persons credentials will be checked by a search at an appropriate third Party to ensure its existence. E-mail unique URL check to ensure that the Subscriber has control over the email address.
Code Signing Subscriber Verification Procedures	Not requesting the Code Signing trust bit, because 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.

	What about RAs and Issuing CAs? Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
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. What about Issuing CAs who operate their own subordinate CA?

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	IDNs not supported
Revocation of Compromised Certificates	CPS section 20.4
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	Where is this documented? 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.
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Where is this documented? 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 SSL certificates	All SSL certificates (including wildcard) are validated with domain ownership and subscriber validation.
Email Address Prefixes for DV Certs	See above.
Delegation of Domain / Email validation to third parties	Where in the CPS is this stated? 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
Allowing external entities to operate subordinate CAs	See above. No external entities operate CAs under the original CA's root. I get the impression from reading the CPS that external entities may operate subordinate CAs. Please clarify.
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	See above
SHA-1 Certificates	Noted. We will ensure the SHA-1 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.