Print this page

Mozilla - CA Program

Case Information

Case Number	00000228	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Sweden (Försäkringskassan)	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Include Swedish Government Root Authority v3	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1417041

General information about CA's associated organization

CA Email Alias 1	mca@forsakringskassan.se		
CA Email Alias 2			
Company Website	http://www.forsakringskassan.se/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Verified
Geographic Focus	Sweden	**Verified?**	Verified
Primary Market / Customer Base	Public sector in Sweden	**Verified?**	Verified
Impact to Mozilla Users	CA for Swedish Government authorities. Employees from 8 government organizations are using this root. We are adding Health care in Sweden in a few months and some more government organization.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended

			Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	https://bugzilla.mozilla.org/attachment.cgi?id=8937421 Yes, we have read Required and Recommended Practices, and we follow those practices	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	https://bugzilla.mozilla.org/attachment.cgi?id=8937421 Yes, we have read Forbidden and Potentially Problematic Practices.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Swedish Government Root Authority v3	**Root Case No**	R00000412
Request Status	In Detailed CP/CPS Review	**Case Number**	00000228

Certificate Data

Certificate Issuer Common Name	Swedish Government Root Authority v3
O From Issuer Field	Swedish Social Insurance Agency
OU From Issuer Field	
Valid From	2015 Sep 29
Valid To	2040 Sep 29
Certificate Serial Number	3269a2bf406b8db44783643c8b0dc943

Subject	CN=Swedish Government Root Authority v3, OU=null, O=Swedish Social Insurance Agency, C=SE
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	74:6F:88:F9:AC:16:3C:53:00:9E:EF:92:0C:40:67:75:6A:15:71:7E
SHA-256 Fingerprint	8F:9A:DB:6D:89:5D:AB:5A:DF:5C:3D:3F:AB:83:92:7B:E0:FB:64:EF:82:48:5C:62:28:0D:58:4E:8B:D5:5D:22
Certificate ID	D2:F9:1A:57:52:5B:43:2B:57:54:F2:55:7C:04:41:C4:5B:70:D2:71:47:76:71:31:02:DA:F3:30:F1:D9:20:3A
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This request is to include the 'Swedish Government Root Authority v3' root certificate and turn on the Email and Websites trust bit. This root and its subCAs are operated by the Swedish Social Insurance Agency (SSIA).	**Verified?**	Verified
Root Certificate Download URL	http://pki.myndighetsca.se/crl/SwedishGovernmentRootAuthorityv3.crt	**Verified?**	Verified
CRL URL(s)	http://pki.myndighetsca.se/crl/SwedishGovernmentRootAuthorityv3.crl http://pki.myndighetsca.se/crl/SwedishGovernmentHWCAv4.crl CP section 4.9.7: The SSIA CA shall publish CRLs at least every 24 hours and within 18 hours of notice of a key compromise.	**Verified?**	Verified
OCSP URL(s)	http://ocsp.myndighetsca.se/ocsp	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	We need only *.gov and *.se	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://mcacert.myndighetsca.se/	**Verified?**	Verified

Test Website - Expired	https://mcacertexpired.myndighetsca.se/
Test Website - Revoked	https://mcacertrevoked.myndighetsca.se/
Example Cert	
Test Notes	

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/mcacert.myndighetsca.se OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=14608&opt=cablint,zlint,x509lint&minNotBefore=2015-01-01 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
EV Tested	Not EV	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	The root and subordinate CAs are operated by the Swedish Social Insurance Agency (SSIA).	**Verified?**	Verified
Externally Operated SubCAs	Not allowed. SwedishGovernmentRootAuthority_CP_Ver0100.pdf section 1.1.3.	**Verified?**	Verified
Cross Signing	Not allowed. SwedishGovernmentRootAuthority_CP_Ver0100.pdf section 1.1.3.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	SwedishGovernmentRootAuthority_CP_Ver0100.pdf section 1.1.3: Certificates issued pursuant to this CP are intended for use solely within the Swedish government and its agencies, and their contracted service providers (hereafter assumed to be included within any reference to the government or its agencies), and there are no provisions within this CP for cross-certification or other forms of recognition or usage of certificates issued under this CP by or with certificates issued by other governments, other CAs or under any other PKIs.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents provided in English.	**Verified?**	Verified
CA Document Repository	http://www.myndighetsca.se/cps/	**Verified?**	Verified

CP Doc Language	English		
CP	http://www.myndighetsca.se /cps/SwedishGovernmentRootAuthority_CP_Ver0100.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.myndighetsca.se /cps/SwedishGovernmentRootAuthority_CPS_Ver0100.pdf	**Verified?**	Verified
Other Relevant Documents	http://www.myndighetsca.se /cps/SSIA_HWCA_v4_CP_Ver420.pdf http://www.myndighetsca.se /cps/SSIA_HWCA_v4_CPS_Ver430.pdf http://www.myndighetsca.se /cps/SSIA_Sign_CA_v3_CP_Ver320.pdf http://www.myndighetsca.se /cps/SSIA_Sign_CA_v3_CPS_Ver330.pdf http://www.myndighetsca.se /cps/SSIA_Soft_CA_v3_CP_Ver311.pdf http://www.myndighetsca.se /cps/SSIA_Soft_CA_v3_CPS_Ver311.pdf http://www.myndighetsca.se /cps/SSIA_QC_CA_v3_CP_Ver310.pdf http://www.myndighetsca.se /cps/SSIA_QC_CA_v3_CPS_Ver310.pdf	**Verified?**	Verified
Auditor (New)	Deloitte	**Verified?**	Verified
Auditor Location (New)	Sweden	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2383&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	10/31/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2384&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	10/31/2017	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	SwedishGovernmentRootAuthority_CP_Ver0100.pdf section 1.1.3. SwedishGovernmentRootAuthority_CPS_Ver0100.pdf section 1.1.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8937420	**Verified?**	Verified

SSL Verification Procedures	SwedishGovernmentRootAuthority_CPS_Ver0100.pdf sections 3.2.2, 4.1.2 (ssia-HWCA) SSIA_HWCA_v4_CPS_Ver430.pdf section 4.1.2.	**Verified?**	Verified
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	SwedishGovernmentRootAuthority_CP_Ver0100.pdf sections 3.2.2, 3.2.3, 3.2.5. SwedishGovernmentRootAuthority_CPS_Ver0100.pdf section 3.2.2, 3.2.3, 3.2.5.	**Verified?**	Verified
Email Address Verification Procedures	SwedishGovernmentRootAuthority_CPS_Ver0100.pdf sections 3.2.5, 4.1.1, 4.1.2 and 4.3.1 (ssia-SignCA). SSIA_Sign_CA_v3_CPS_Ver330.pdf section 4.1.2. Users from all Agencies can request an S/mime certificate on a self-service page at the Portal if they have a valid certificate from “Swedish Government User CA” or “Swedish Government Auth CA”. The s/mime certificate is stored at the Applicants smart card.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	SwedishGovernmentRootAuthority_CPS_Ver0100.pdf section 4.2.1. All end-user have certificate at smart card and use them to certificate issuance	**Verified?**	Verified
Network Security	SwedishGovernmentRootAuthority_CPS_Ver0100.pdf section 6.7	**Verified?**	Verified