Mozilla - CA Program

Case Information

Case Number	00000177 and Bug 1417041	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Swedish Government Root Authority v3	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include Example Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	i.	https://bug1330392.bmoattachments.org/attachment.cgi?id=8926629
	ii.	https://bugzilla.mozilla.org/attachment.cgi?id=8926630
	iii.	https://bugzilla.mozilla.org/attachment.cgi?id=8926631

General information about CA's associated organization

CA Email Alias 1			mca@forsakringskassan.se
CA Email Alias 2			magnus.enmarker@forsakringskassan.se
Company Website		**Verified?**	http://www.forsakringskassan.se/
Organizational Type		**Verified?**	http://www.myndighetsca.se/
Organizational Type (Others)		**Verified?**	Organization Type choices: - Government Agency
Geographic Focus		**Verified?**	Sweden
Primary Market / Customer Base		**Verified?**	- Public sector in Sweden

	geographic region?		
Impact to Mozilla Users		**Verified?**	In the public sector there are very many web servers the public should have access to in order to utilize the services that the public sector offers the public in Sweden

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	NEED: CAs response to each of the items listed in https://wiki.mozilla.org /CA/Required_or_Recommended_Practices	**Verified?**	Yes, we have read Required and Recommended Practices, and we follow those practices

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	NEED: CA's response to each of the items listed in https://wiki.mozilla.org /CA/Forbidden_or_Problematic_Practices	**Verified?**	Yes, we have read Forbidden and Potentially Problematic Practices, and we follow those practices

Root Case Record # 1

Root Case Information

Root Certificate Name	Swedish Government Root Authority v3	**Root Case No**	00000177
Request Status	Initial Request Received	**Case Number**	00000177

Certificate Data

see https://crt.sh/?id=12755488

Certificate Issuer Common Name	CN = Swedish Government Root Authority v3
O From Issuer Field	O = Swedish Social Insurance Agency
OU From Issuer Field	
Valid From	29 september 2015 12:32:32
Valid To	29 september 2040 12:42:09
Certificate Serial Number	32 69 a2 bf 40 6b 8d b4 47 83 64 3c 8b 0d c9 43
Subject	CN = Swedish Government Root Authority v3 O = Swedish Social Insurance Agency C = SE
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096
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	9c bc 01 e7 ab 64 35 f5 31 9b 8d b5 fb 17 99 88 02 cb 9b f2
Certificate Fingerprint	8F9ADB6D895DAB5ADF5C3D3FAB83927BE0FB64EF82485C62280D584E8BD55D22
Certificate Version	V3

Technical Information about Root Certificate

Certificate Summary	Verified?	
Root Certificate Download URL	Verified?	http://pki.myndighetsca.se/crl/SwedishGovernmentRootAuthorityv3.crt
CRL URL(s)	Verified?	http://pki.myndighetsca.se/crl/SwedishGovernmentRootAuthorityv3.crl
OCSP URL(s)	Verified?	Offline root
Mozilla Trust Bits	Verified?	Email; Websites
SSL Validation Type	Verified?	OV
Mozilla EV Policy OID(s)	Verified?	
Root Stores Included In	Verified?	

Mozilla Applied Constraints		**Verified?**	We need only *.gov and *.se.

Test Websites or Example Cert

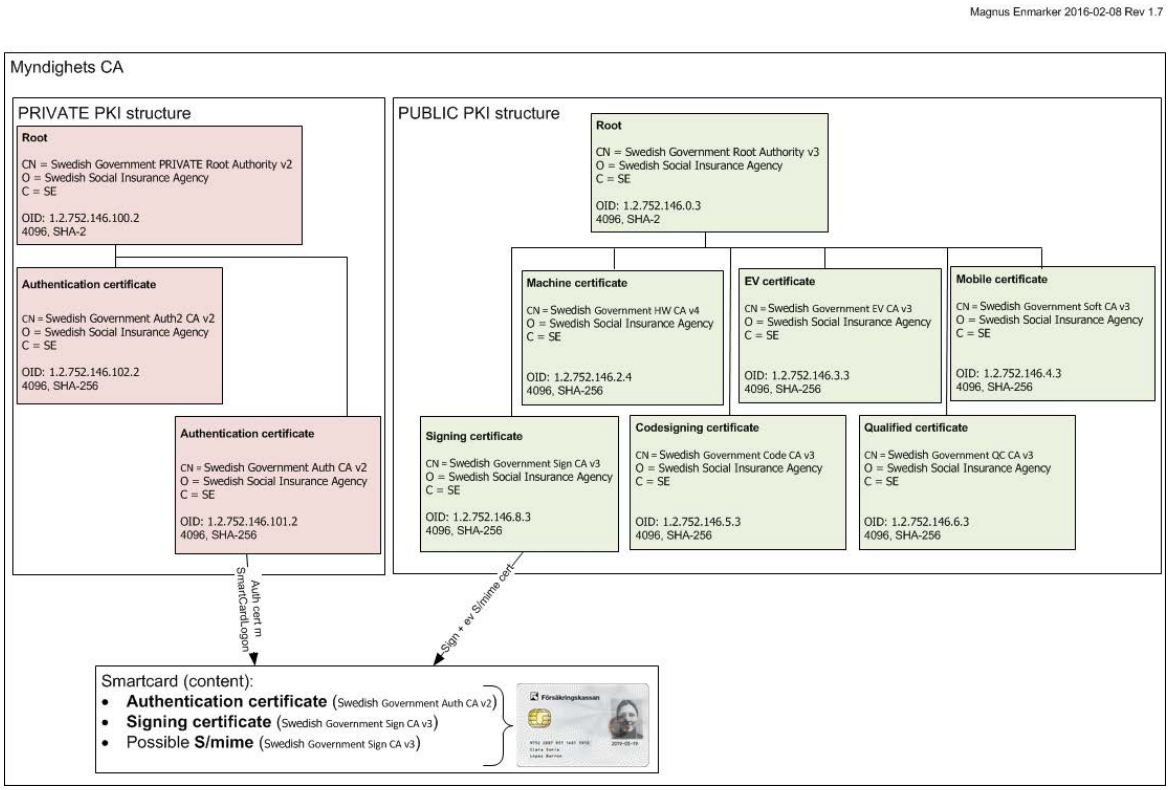
Test Website - Valid		**Verified?**	https://mcacert.myndighetsca.se/
Test Website - Expired			https://mcacertexpired.myndighetsca.se/
Test Website - Revoked			https://mcacertrevoked.myndighetsca.se/
Example Cert			See appendix
Test Notes			

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

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Correct. Only one error, and it´s correct behavior since root is offline.
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI	**Verified?**	Need Response From CA



Externally Operated SubCAs		**Verified?**	This root has subordinate CA. Root and Sub CA are operated by Försäkringskassan (Swedish Social Insurance Agency)
Policy Documentation		**Verified?**	see http://www.myndighetsca.se/cps/
CA Document Repository		**Verified?**	-http://www.myndighetsca.se/cps/
CP Doc Language			English
CP		**Verified?**	
CP Doc Language			
Cross Signing		**Verified?**	We don´t issued cross-signing certificates.
Other Relevant Documents		**Verified?**	
Auditor Name		**Verified?**	Deloitte AB
Auditor Website		**Verified?**	https://www2.deloitte.com/se/sv.html
Auditor Qualifications		**Verified?**	
Standard Audit		**Verified?**	Audit report WebTrust for CA Audit report WebTrust Principles for CA_SSL

	Store Policy.		
Standard Audit Type		**Verified?**	i. https://bug1330392.bmoattachments.org/attachment.cgi?id=8926629 ii. https://bugzilla.mozilla.org/attachment.cgi?id=8926630 iii. https://bugzilla.mozilla.org/attachment.cgi?id=8926631
Standard Audit Statement Date		**Verified?**	
BR Audit		**Verified?**	
BR Audit Type		**Verified?**	
BR Audit Statement Date		**Verified?**	
EV SSL Audit		**Verified?**	
EV SSL Audit Type		**Verified?**	
EV SSL Audit Statement Date		**Verified?**	
BR Commitment to Comply	NEED: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**Verified?**	See SwedishGovernmentRootAuthority_BRSelfAssessment.xlsx
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of	**Verified?**	

	the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.		
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	See "SwedishGovernmentRootAuthority_CPS_Ver0100.pdf" chapter 3.2.2.1.1
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	See "SwedishGovernmentRootAuthority_CPS_Ver0100.pdf" chapter 3.2.5, 4.1.2 and 4.3.1 (ssia-SignCA).
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	See "SwedishGovernmentRootAuthority_CPS_Ver0100.pdf" chapter 4.2.1. Applications for certificates are authenticated using multi factor authentication.
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	See "SwedishGovernmentRootAuthority_CPS_Ver0100.pdf" chapter 6.7

Appendix

-----BEGIN CERTIFICATE-----
MIIHRzCCBS+gAwIBAgITQgAAANTz/ydyBDxFjAAAAAAA1DANBgkqhkiG9w0BAQsF
ADBfMQswCQYDVQQGEwJTRTEoMCYGA1UEChMfU3dlZGlzaCBTb2NpYWwgSW5zdXJh
bmNlIEFnZW5jeTEmMCQGA1UEAxMdU3dlZGlzaCBHb3Zlcm5tZW50IFNpZ24gQ0Eg
djMwHhcNMTYwMzAxMTIxNDI5WhcNMjEwMjE3MTAwODQyWjCBijELMAkGA1UEBhMC
U0UxHDAaBgNVBAoME0bDtnJzw6RrcmluZ3NrYXNzYW4xEzARBgNVBAsTCjIwMjEw
MDU1MjExHjAcBgNVBAMTFUVybnN0IE1hZ251cyBFbm1hcmtlcjERMA8GA1UEBBMI
RW5tYXJrZXIxFTATBgNVBCoTDEVybnN0IE1hZ251czCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALc1BpR/3RzKxSMP7BEUe6KaBX9O1diN7O7SJmFagG/b
zrpgfFDcb3L3Ryn1W0LLlhBqCPTJw7b5eFngu0FLcmJhYBEw4kbcLQVC7TI7kyx5
FXB8vZN3UClkXiS6ieMhpLk6q0c8GiiYAq07MAImrr+9tB5f4fZjyywWJMlcJ4eH
CRa4KDEaVTQNLmioTjSlkgMUhVToRg9lwROOfS7JBZTP4JN9A1T4rrweSJWz61g0
efsEFRBZ5nsO6mqwgeIXx2KaM35bMm14eK52NrGJmyhGnUceo+ixO3P6PXHQcGYa
4SJw4IDf1yp/CA8uxhi06wDmc3GAMHHhFu246iv+43ECAwEAAaOCAs4wggLKMA4G
A1UdDwEB/wQEAwIFoDAdBgNVHQ4EFgQU4UDChTJ/TzxTyZ5/2Ol/xOTwcUQwHwYD
VR0jBBgwFoAUbh8i4WbXQW2GziS1koZJdMtnQX4wgZUGA1UdHwSBjTCBijCBh6CB
hKCBgYY8aHR0cDovL3BraS5teW5kaWdoZXRzY2Euc2UvY3JsL1N3ZWRpc2hHb3Zl
cm5tZW50U2lnbkNBdjMuY3JshkFodHRwOi8vcGtpLmZvcnNha3Jpbmdza2Fzc2Fu
LnNlL2NybC9Td2VkaXNoR292ZXJubWVudFNpZ25DQXYzLmNybDCB1wYIKwYBBQUH
AQEEgcowgccwSAYIKwYBBQUHMAKGPGh0dHA6Ly9wa2kubXluZGlnaGV0c2NhLnNl
L2NybC9Td2VkaXNoR292ZXJubWVudFNpZ25DQXYzLmNydDBNBggrBgEFBQcwAoZB
aHR0cDovL3BraS5mb3JzYWtyaW5nc2thc3Nhbi5zZS9jcmwvU3dlZGlzaEdvdmVy
bm1lbnRTaWduQ0F2My5jcnQwLAYIKwYBBQUHMAGGIGh0dHA6Ly9vY3NwLm15bmRp
Z2hldHNjYS5zZS9vY3NwMDwGCSsGAQQBgjcVBwQvMC0GJSsGAQQBgjcVCIK74T74
+2iBhYssgvCUTYaJxneBZMayTYTrik8CAWQCAQ4wEwYDVR0lBAwwCgYIKwYBBQUH
AwQwGwYJKwYBBAGCNxUKBA4wDDAKBggrBgEFBQcDBDBEBgNVHSAEPTA7MDkGByqF
cIESCAMwLjAsBggrBgEFBQcCARYgaHR0cDovL3d3dy5teW5kaWdoZXRzY2Euc2Uv
Y3BzLwAwHwYGKoVwIgIBBBUWEzk3NTIyNzU4OTU3MTgyNjA3MjAwLwYDVR0RBCgw
JoEkbWFnbnVzLmVubWFya2VyQGZvcnNha3Jpbmdza2Fzc2FuLnNlMA0GCSqGSIb3
DQEBCwUAA4ICAQBx3GQma0twAGJaYSgbLUvkH67zoxRaMJZKFgHJmLn1hyIHeBGw
ayn7G/Uhi8yQHgnGbtwxKPV3bLAEDw/NExlSnmUk1t3IOzgYPbui+KOBjrT84gUr
flouVqEnYwCqeO/wEz2mH745RqOJr8kwBku//zQgTnFzQ/nygh1fuZXCSohVSPjg
yKi27H0yh6tB5WI0M0ODk3KpJ+2i8Ta83sz4g3jv3zJkGKMOgcGP48n8LqodqIqz
S0KG1mpvx7mPpuf9Q0FFcnKhBAyBJUXxPXIJy9/lIce16qIzuZcNlDb9w3mDjbui
ItKPv6Pj+cXYNE127p8fXgow6iCIRkWQueQppukVTmnQFIuumYYjHJOORExXcRXTV
lX/q25qeBO2+hETvKGwPnjBPajkfWRMcoRC94+HCfvzpxpbBMstt6Lc+AwJJO1A3
nEHTxzn9ywbgOfkTgodynhD7XPRRMmkcSSofq9YC1ILysLyOrNllHn2QCKzk8Efv
V0Gqc40SpGMm4e5KHYQ73P+TPsac6Z21HshHECW3PiUri1OrlERqFiTOYTJDoOkg
f9sbjjlVe5s2mLZtUNLCzrTlok6we91QVGYqmXCjDVsXhilSU9roZ25+oX2szpKc
hEkYSrucb/eEAlP3JMNLBihGJdnZtlOVmexO9QlSwzwmnCxN1LzdcXLsrg==
-----END CERTIFICATE-----