Mozilla - CA Program

Case Information

Case Number	00000275	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Microsoft Corporation	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Microsoft Roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1448093

General information about CA's associated organization

CA Email Alias 1	certificateauthority@microsoft.com		
CA Email Alias 2			
Company Website	https://www.microsoft.com/pkiops /docs/repository.htm	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
Primary Market / Customer Base	End User Products, Enterprise Products and Services, Cloud Services	**Verified?**	Verified
Impact to Mozilla Users	Essential trust anchors for one of the major underlying operating systems.	**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	1. Publicly Available CP and CPS: CP/CPS section 1.5.4 1.1 Revision Table, updated annually: CP/CPS section 1.2.1 1.2 CAA Domains listed in CP/CPS: CPS section 4.2.4 microsoft.com 2. Audit Criteria: CPS section 8 3. Revocation of Compromised Certificates: CPS section 4.9.1 4. Verifying Domain Name Ownership: CPS section 3.2.2.4 5. Verifying Email Address Control: N/A 6. DNS names go in SAN: NEED: https://wiki.mozilla.org /CA/Required_or_Recommended_Practices#DNS_names_go_in_SAN CPS is not clear about this. section 3.1.1: "The Subject Alternative Name (SAN) MAY be used." and section 7.1.4.2.1. Subject Alternative Name Extension	**Verified?**	Need Response From CA

No Stipulation

7. OCSP: CPS section 4.9.9, 4.9.10
- OCSP SHALL NOT respond "Good" for unissued certs: CPS section 4.9.10
8. Network Security Controls: CPS section 6.7

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	1. Long-lived Certificates: CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS section 3.2.2.4 3. Issuing End Entity Certificates Directly From Roots: CP/CPS section 6.1.7 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: NEED: Update CPS to clarify what is/isn't allowed in regards to IP Addresses CPS currently says: "3.2.2.5 Authentication for an IP Address No Stipulation" Reference: https://wiki.mozilla.org /CA/Forbidden_or_Problematic_Practices#Certificates_Referencing_Local_Names_or_Private_IP_Addresses NEED: Also CPS currently says: "3.2.2.6 Wildcard Domain Validation No Stipulation" That is insufficient as well. Need to indicate if allowed, and what domain and other validation is performed for wildcard domains. (needs to be in line with BRs) 6. Issuing SSL Certificates for .int Domains: CPS section 3.2.2.4 7. OCSP Responses Signed by a Certificate Under a Different Root: CPS section 4.9.9 8. Issuance of SHA-1 Certificates: CPS section 6.1.5 9. Delegation of Domain / Email Validation to Third Parties: CPS 1.3.2	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Microsoft EV RSA Root Certificate Authority 2017	**Root Case No**	R00000541
Request Status	Information Verification In Process	**Case Number**	00000275

Certificate Data

Certificate Issuer Common Name	Microsoft EV RSA Root Certificate Authority 2017

O From Issuer Field	Microsoft Corporation
OU From Issuer Field	
Valid From	2017 Jul 26
Valid To	2042 Jul 26
Certificate Serial Number	19FCEB6DF7CF57844184BDD9E0228E98
Subject	CN=Microsoft EV RSA Root Certificate Authority 2017; OU=; O=Microsoft Corporation; C=US
Signature Hash Algorithm	SHA384WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	3AD38A39CE4E88DCDF46995E969FC339D0799858
SHA-256 Fingerprint	DFB3C314740596AD5FB97960EF62AD7C1FCCEEAD16E74054652D1032E6F140EF
Subject + SPKI SHA256	7EA74459FF5C26C9D622652B7624424A0B3BA61702495674DB178A92A3C5EEC6
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This "Microsoft EV RSA Root Certificate Authority 2017" is only used for EV TLS/SSL certs.	**Verified?**	Verified
Root Certificate Download URL	http://www.microsoft.com/pkiops/certs /Microsoft%20EV%20RSA%20Root%20Certificate%20Authority%202017.crt	**Verified?**	Verified
CRL URL(s)	http://www.microsoft.com/pkiops /crl/Microsoft%20EV%20RSA%20Root%20Certificate%20Authority%202017.crl http://www.microsoft.com/pkiops /crl/Microsoft%20TLS%20EV%20Issuing%20CA%2001.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.msocsp.com	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://actrsaevroot2017.pki.microsoft.com/	**Verified?**	Need Response From CA
Test Website - Expired	https://exprsaevroot2017.pki.microsoft.com/		
Test Website - Revoked	https://rvkrsaevroot2017.pki.microsoft.com/		
Example Cert			
Test Notes	NEED: SSL cert for the revoked test website needs to be revoked and in the CRL.		

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

Revocation Tested	NEED: Fix errors listed here: https://certificate.revocationcheck.com /actrsaevroot2017.pki.microsoft.com	**Verified?**	Need Response From CA

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?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. And a list of all of the subordinate CAs that are signed by this root. Our preference is that this information be provided in the CPS.	**Verified?**	Need Response From CA
Externally Operated SubCAs	CPS 1.3.1 Certification Authorities: Microsoft PKI Services operates as the Root CA and administers all CA functions within its PKI hierarchy.	**Verified?**	Verified
Cross Signing	None, and none planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS 1.3.2 Registration Authorities: No RA functions are delegated to third parties by Microsoft PKI Services	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English. Microsoft's CP applies to both their external (publicly trusted) CA operations as well as their internal (not publicly trusted) CA operations. The Microsoft PKI Services CPS (Microsoft_PKI_Services_CPS) is for the external (publicly trusted) CA operations, so is the one governing this root certificate. The Microsoft PKI Services Corporate CPS (Microsoft_PKI_Services_Corporate-CPS) governs the private PKI of Microsoft PKI Services, so not relevant to this root certificate.	**Verified?**	Verified
CA Document Repository	https://www.microsoft.com/pkiops/docs/repository.htm	**Verified?**	Verified
CP Doc Language	English		
CP	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CP_v3.1.1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CPS_v3.1.1.pdf	**Verified?**	Need Response From CA

Other Relevant Documents	NEED: Update the Microsoft PKI Services CPS to bind that CPS to the root certificates that it applies to. Previous Audit Statements: Root Generation 7/26/2017 https://bug1448093.bmoattachments.org/attachment.cgi?id=8986854 WebTrust CA 8/4/2017 Audit Period: 5/1/2016 - 4/30/2017 www.cpacanada.ca/GenericHandlers/AptifyAttachmentHandler.ashx?AttachmentID=221185	**Verified?**	Need Response From CA
Auditor	BDO International Limited	**Verified?**	Verified
Auditor Location	United States	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=9009197	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/10/2018	**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	CP/CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8989260	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.4	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 6.5.1	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	Microsoft RSA Root Certificate Authority 2017	**Root Case No**	R00000631
Request Status	Information Verification In Process	**Case Number**	00000275

Certificate Data

Certificate Issuer Common Name	Microsoft RSA Root Certificate Authority 2017
O From Issuer Field	Microsoft Corporation
OU From Issuer Field	
Valid From	2017 Jul 26
Valid To	2042 Jul 26
Certificate Serial Number	29C87039F4DBFDB94DBCDA6CA792836B
Subject	CN=Microsoft RSA Root Certificate Authority 2017; OU=; O=Microsoft Corporation; C=US
Signature Hash Algorithm	SHA384WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	EE68C3E94AB5D55EB9395116424E25B0CADD9009
SHA-256 Fingerprint	ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1
Subject + SPKI SHA256	7904CC524E3A275B5B36C516E4C4507E92C0E93FA3382139279A064E25DE5D3F
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This "Microsoft RSA Root Certificate Authority 2017" is only used for non-EV TLS/SSL certs.	**Verified?**	Verified
Root Certificate Download URL	http://www.microsoft.com/pkiops/certs /Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt	**Verified?**	Verified
CRL URL(s)	http://www.microsoft.com/pkiops /crl/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crl http://www.microsoft.com/pkiops /crl/Microsoft%20TLS%20Issuing%20CA%2001.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.msocsp.com	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://actrsaroot2017.pki.microsoft.com/	**Verified?**	Need Response From CA
Test Website - Expired	https://exprsaroot2017.pki.microsoft.com/		
Test Website - Revoked	https://rvkrsaroot2017.pki.microsoft.com/		
Example Cert			
Test Notes	NEED: SSL cert for the revoked test website must be revoked and in CRL.		

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

Revocation Tested	NEED: Fix errors listed here:	**Verified?**	Need Response From CA

	https://certificate.revocationcheck.com/actrsaroot2017.pki.microsoft.com		
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	N/A	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. And a list of all of the subordinate CAs that are signed by this root. Our preference is that this information be provided in the CPS.	**Verified?**	Need Response From CA
Externally Operated SubCAs	CPS 1.3.1 Certification Authorities: Microsoft PKI Services operates as the Root CA and administers all CA functions within its PKI hierarchy.	**Verified?**	Verified
Cross Signing	None, and none planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS 1.3.2 Registration Authorities: No RA functions are delegated to third parties by Microsoft PKI Services	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English. Microsoft's CP applies to both their external (publicly trusted) CA operations as well as their internal (not publicly trusted) CA operations. The Microsoft PKI Services CPS (Microsoft_PKI_Services_CPS) is for the external (publicly trusted) CA operations, so is the one governing this root certificate. The Microsoft PKI Services Corporate CPS (Microsoft_PKI_Services_Corporate-CPS) governs the private PKI of Microsoft PKI Services, so not relevant to this root certificate.	**Verified?**	Verified
CA Document Repository	https://www.microsoft.com/pkiops/docs/repository.htm	**Verified?**	Verified
CP Doc Language	English		
CP	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CP_v3.1.1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CPS_v3.1.1.pdf	**Verified?**	Need Response From CA
Other Relevant Documents	NEED: Update the Microsoft PKI Services CPS to bind that CPS to the root certificates that it applies to.	**Verified?**	Need Response From CA

	Previous Audit Statements: Root Generation 7/26/2017 https://bug1448093.bmoattachments.org /attachment.cgi?id=8986854 WebTrust CA 8/4/2017 Audit Period: 5/1/2016 - 4/30/2017 www.cpacanada.ca/GenericHandlers /AptifyAttachmentHandler.ashx?AttachmentID=221185		
Auditor	BDO International Limited	**Verified?**	Verified
Auditor Location	United States	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=9009197	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/10/2018	**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
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	CP/CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8989260	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.4	**Verified?**	Verified
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 6.5.1	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 3

Root Case Information

Root Certificate Name	Microsoft EV ECC Root Certificate Authority 2017	**Root Case No**	R00000632
Request Status	Information Verification In Process	**Case Number**	00000275

Certificate Data

Certificate Issuer	Microsoft EV ECC Root Certificate Authority 2017

Common Name	
O From Issuer Field	Microsoft Corporation
OU From Issuer Field	
Valid From	2017 Jul 26
Valid To	2042 Jul 26
Certificate Serial Number	3FDCCC3B5BDCD29844CADF59D1D2EB1C
Subject	CN=Microsoft EV ECC Root Certificate Authority 2017; OU=; O=Microsoft Corporation; C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	B8095F5A89FB47A7017ED794DD4F611E27830E27
SHA-256 Fingerprint	6AEA30BC02CA85AFCFEC2F65F60881893C926925FD0704BD8ADA3F0F6EDDB699
Subject + SPKI SHA256	4AA5CBF2A4CA58965C469BBC7376DEB08AAB1A00EFAA96733B9F669801B3D7C9
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This "Microsoft EV ECC Root Certificate Authority 2017" is only used for EV TLS/SSL certs.	**Verified?**	Verified
Root Certificate Download URL	http://www.microsoft.com/pkiops/certs /Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt	**Verified?**	Verified
CRL URL(s)	http://www.microsoft.com/pkiops /crl/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crl http://www.microsoft.com/pkiops /crl/Microsoft%20TLS%20ECC%20EV%20Issuing%20CA%2001.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.msocsp.com	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://acteccevroot2017.pki.microsoft.com/	**Verified?**	Need Response From CA
Test Website - Expired	https://expeccevroot2017.pki.microsoft.com/		
Test Website - Revoked	https://rvkeccevroot2017.pki.microsoft.com/		
Example Cert			
Test Notes	NEED: SSL cert for the revoked test website needs to be revoked and in the CRL.		

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

Revocation Tested	NEED: Fix errors listed here: https://certificate.revocationcheck.com /acteccevroot2017.pki.microsoft.com	**Verified?**	Need Response From CA

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?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. And a list of all of the subordinate CAs that are signed by this root. Our preference is that this information be provided in the CPS.	**Verified?**	Need Response From CA
Externally Operated SubCAs	CPS 1.3.1 Certification Authorities: Microsoft PKI Services operates as the Root CA and administers all CA functions within its PKI hierarchy.	**Verified?**	Verified
Cross Signing	None, and none planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS 1.3.2 Registration Authorities: No RA functions are delegated to third parties by Microsoft PKI Services	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English. Microsoft's CP applies to both their external (publicly trusted) CA operations as well as their internal (not publicly trusted) CA operations. The Microsoft PKI Services CPS (Microsoft_PKI_Services_CPS) is for the external (publicly trusted) CA operations, so is the one governing this root certificate. The Microsoft PKI Services Corporate CPS (Microsoft_PKI_Services_Corporate-CPS) governs the private PKI of Microsoft PKI Services, so not relevant to this root certificate.	**Verified?**	Verified
CA Document Repository	https://www.microsoft.com/pkiops/docs/repository.htm	**Verified?**	Verified
CP Doc Language	English		
CP	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CP_v3.1.1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CPS_v3.1.1.pdf	**Verified?**	Need Response From CA

Other Relevant Documents	NEED: Update the Microsoft PKI Services CPS to bind that CPS to the root certificates that it applies to. Previous Audit Statements: Root Generation 7/26/2017 https://bug1448093.bmoattachments.org/attachment.cgi?id=8986854 WebTrust CA 8/4/2017 Audit Period: 5/1/2016 - 4/30/2017 www.cpacanada.ca/GenericHandlers/AptifyAttachmentHandler.ashx?AttachmentID=221185	**Verified?**	Need Response From CA
Auditor	BDO International Limited	**Verified?**	Verified
Auditor Location	United States	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=9009197	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/10/2018	**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	CP/CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8989260	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.4	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 6.5.1	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 4

Root Case Information

Root Certificate Name	Microsoft ECC Root Certificate Authority 2017	**Root Case No**	R00000633
Request Status	Information Verification In Process	**Case Number**	00000275

Certificate Data

Certificate Issuer Common Name	Microsoft ECC Root Certificate Authority 2017
O From Issuer Field	Microsoft Corporation
OU From Issuer Field	
Valid From	2017 Jul 26
Valid To	2042 Jul 26
Certificate Serial Number	71767E8D58E4FC9649C63EFBCF3ABDA7
Subject	CN=Microsoft ECC Root Certificate Authority 2017; OU=; O=Microsoft Corporation; C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	7CA9013D43721551E987380B3EAE4B442DC037EA
SHA-256 Fingerprint	FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2
Subject + SPKI SHA256	1638A5943D83C3B0FF3C2D17DAA93034408105E29B4F6D74735A7BE95497860A
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This "Microsoft ECC Root Certificate Authority 2017" is only used for non-EV TLS/SSL certs.	**Verified?**	Verified
Root Certificate Download URL	http://www.microsoft.com/pkiops/certs /Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt	**Verified?**	Verified
CRL URL(s)	http://www.microsoft.com/pkiops /crl/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crl http://www.microsoft.com/pkiops /crl/Microsoft%20TLS%20ECC%20Issuing%20CA%2001.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.msocsp.com	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://acteccroot2017.pki.microsoft.com/	**Verified?**	Need Response From CA
Test Website - Expired	https://expeccroot2017.pki.microsoft.com/		
Test Website - Revoked	https://rvkeccroot2017.pki.microsoft.com/		
Example Cert			
Test Notes	NEED: SSL cert for the revoked test website must be revoked and in CRL.		

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

Revocation Tested	NEED: Fix errors listed here:	**Verified?**	Need Response From CA

	https://certificate.revocationcheck.com/actecccroot2017.pki.microsoft.com		
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	N/A	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. And a list of all of the subordinate CAs that are signed by this root. Our preference is that this information be provided in the CPS.	**Verified?**	Need Response From CA
Externally Operated SubCAs	CPS 1.3.1 Certification Authorities: Microsoft PKI Services operates as the Root CA and administers all CA functions within its PKI hierarchy.	**Verified?**	Verified
Cross Signing	None, and none planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS 1.3.2 Registration Authorities: No RA functions are delegated to third parties by Microsoft PKI Services	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English. Microsoft's CP applies to both their external (publicly trusted) CA operations as well as their internal (not publicly trusted) CA operations. The Microsoft PKI Services CPS (Microsoft_PKI_Services_CPS) is for the external (publicly trusted) CA operations, so is the one governing this root certificate. The Microsoft PKI Services Corporate CPS (Microsoft_PKI_Services_Corporate-CPS) governs the private PKI of Microsoft PKI Services, so not relevant to this root certificate.	**Verified?**	Verified
CA Document Repository	https://www.microsoft.com/pkiops/docs/repository.htm	**Verified?**	Verified
CP Doc Language	English		
CP	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CP_v3.1.1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pkirepositorysite.azurewebsites.net/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CPS_v3.1.1.pdf	**Verified?**	Need Response From CA
Other Relevant Documents	NEED: Update the Microsoft PKI Services CPS to bind that CPS to the root certificates that it applies to.	**Verified?**	Need Response From CA

	Previous Audit Statements: Root Generation 7/26/2017 https://bug1448093.bmoattachments.org /attachment.cgi?id=8986854 WebTrust CA 8/4/2017 Audit Period: 5/1/2016 - 4/30/2017 www.cpacanada.ca/GenericHandlers /AptifyAttachmentHandler.ashx?AttachmentID=221185		
Auditor	BDO International Limited	**Verified?**	Verified
Auditor Location	United States	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=9009197	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/10/2018	**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
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	CP/CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8989260	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.4	**Verified?**	Verified
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 6.5.1	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified