Original translations used for https://bugzilla.mozilla.org/show_bug.cgi?id=527419
The updates are highlighted in yellow

Organization Identity Verification	Translations from Security Communication RootCA Subordinate CA Certificate Pol (SCRootCP1) 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key It is proved that the applicant has the private key as follows. Certificate Signing Request, "CSR" submitted by the applicant and verify that the corresponding pu key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key. 3.2.2 Authentication of company Secom authorize the authentication of the applicant company as follows. By using the official documents from central or local government, database provided by QIIS or QG and another ways that the equal level of authorization possible. 3.2.3 Authentication of individual Secom authorize the authentication of the applicant individual as follows. By using the official documents from central or local government, database provided by QIIS or QG and another ways that the equal level of authorization possible. 3.2.4 Information of non verified certificate user Not described. 3.2.5 Confirmation of the authority to apply Secom confirm that the applicant has proper right to apply the certificate by the section 3.2 or 3.3 this CP. In the case if the application is made by third party, we request to give us the letter of attorney. * The third party application means that other than the company using the host name described or common name of the certificate that is described on the section 3.1.1. 4. Requirements for certificate life-cycle management 4.1 Certificate Application 4.1.1 The one who can apply certificate Application of issuance for certificates can be performed by representatives, employees or agents organizations or groups. 4.1.2 Registration procedures and responsibilities Applicant applies for the certificate in accordance with procedures notified by Secom in advance. Applicant who applies for the certificate accepts CP, CPS, and other contents of those documents disclosed by Secom. Applicant must ensure the accuracy of information on that application. 4.2 Certificate Application Procedures 4.2.1 Identification and authentication procedures Secom validates the application documents submit by the applicant and authenticity of CSR confor with this CP "3.2 initial identification and authentication". 4.2.2 Acceptance or rejection of certificate applications Secom notifies the applicant for the results whether accept or reject for the application after the validation in accordance with predetermined procedures. 4.2.3 Certificate Application Processing Time Secom issues the certificate immediately if the application is accepted. 4.3 Issuance of certificate 4.3.1 Procedures to issue certificate by CA Secom issues the certificate and prepares the certificate download site only available for the applic The applicant uses a client certificate or one time password along with access key to reach the download site. 4.3.2 Notification of certificate issuance to subscriber

	Secom notifies the applicant by the email that the certificate is ready and available at the downloa only for the applicant. 4.4 Confirmation for receipt of the certificate 4.4.1 Confirmation procedure for receipt of the certificate Secom realizes the acceptance of the certificate by the applicant when the applicant downloads an gets the certificate. 4.4.2 Publication of the certificate No publication. 4.4.3 Notification of certificate issuing by CA to other entities Secom does not notify the issuance of certificates for other entities. 4.5 Usage of key pair and certificate 4.5.1 Usage of the subscriber's private key and certificate The usage of the certificates issued by Secom root CA and private keys possessed by applicants are limited to services provided by Secom or services provided by subscribers of Secom root CA that is contractual relationship with Secom. The certificates issued by Secom root CA should not be used for any other purpose. 4.5.2 Usage of the user's public key and certificate Users are familiar with CP and CPS and agree to use root CA and verify the authenticity of the certificate issued by Secom root CA.
Domain Name Ownership / Control EV	Translations of sections 3.2, 3.3 and 3.4 of PfWEVCA-CP (https://bugzilla.mozilla.org/attachment.cgi?id=449589) 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key It is proved that the applicant has the private key as follows. Certificate Signing Request, "CSR" submitted by the applicant and verify that the corresponding public key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key 3.2.2 Authentication of company Secom authorize the authentication of the applicant company as follows. By using the official documents from central or local government, database provid by QIIS or QGIS, and another ways that the equal level of authorization possible. 3.2.3 Authentication of individual Secom authorize the authentication of the applicant individual as follows. By using the official documents from central or local government, database provid by QIIS or QGIS, and another ways that the equal level of authorization possible. 3.2.4 Information of non verified certificate user Not described. 3.2.5 Confirmation of the authority to apply Secom confirm that the applicant has proper right to apply the certificate by the section 3.2 or 3.3 on this CP. In the case if the application is made by third party, we request to give us the lette attorney. * The third party application means that other than the company using the host na described on common name of the certificate that is described on the section 3.1.1 3.2.6 This CA is issued one-way cross signing certificate from Security Communiat EV RootCA1. 3.3 Identification and authentication at renewal application 3.3.1 Identification and authentication at usual renewal application

	It is same as 3.2. 3.3.2 Identification and authentication at renewal application after revocation No renewal for revoked certificate. The application is treated as new and it is same as 3.2. Translations of Secom Passport for Web EV service verification procedures that w attached to the bug. https://bugzilla.mozilla.org/attachment.cgi?id=451885 2.3 procedure3. Physical existence of the applicant The below is the procedures to verify the physical existence of the applicant. (1) Current address is same with the QIIS/ QGIS and the one on the application. QIIS/QGIS(EDINET(https://info.edinet.go.jp/EdiHtml/main.htm)) (2) If we cannot verify by (1), RA or operation manager visits the current address verify the physical existence. (3) If we cannot verify by (1) or (2), we verify by lawyer opinion letter. We verify: The address for the current physical existence on the letter. (b) The real existence the lawyer who wrote the letter. 2.4 procedure 4. Domain/ CSR verification 4-1. The contents of (O) for CSR 4-1-1. Registered corporation We verify the (O) is same as the financial statements publicly available on the Wel site. If the financial statements is not available, it is verified by QIIS or QGIS. If it is not verified by the above, it is verified by certificate of incorporation or lawy opinion letter. And again, if it is not verified by the above, it should be roman alphabet of Hepbur system. For example, Secom CO.,LTD. => sekomu kabushikigaisya Wrong with the domain The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again. * For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-1-2. Government ministries and agencies and organization in country/local pub entity We verify the (O) is same as QIIS, QGIS and get the screen capture. If it is not verified by QIIS, QGIS, it should be roman alphabet of Hepburn system. For example, Yokohama city => Yokohamashi Government and municipal offices => Kankocho Wrong with the domain The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again.

	* For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-1-3. University/ National and public high school We verify the (O) is same as QIIS, QGIS and get the screen capture. If it is not verified by QIIS, QGIS, it should be roman alphabet of Hepburn system. For example, Tokyo university => Tokyo daigaku Wrong with the domain The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again. * For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-2 Verification of the domain owner By using Whois gateway(NIC domain reference function), we verify the applied company name on domain information (the contents included in CommonName) a the applicant (if the domain name use consent form is submitted, it is same as the domain owner). The two points to check for exclusive right to use. For example, the applied CN is "WWW.login.secom.co.jp" (1) Applied company or company that exists in parents/child relation with the applied company owns "secom.co.jp". (2) Applied company or company that exists in parents/child relation with the applied company owns "login.secom.co.jp". In order to check for parents/child relation, we use QIIS or QGIS(EDINET). If we cannot find it, we ask the applicant to change the owner as same as the appli company name for WHOIS. If we cannot refer the owner at Whois gateway, ask the applicant for registration. JP domain: http://whois.jprs.jp/ COM, NET, ORG domain: http://www.networksolutions.com/cgi-bin/whois/whoi 4-2-1. For the domain owner is different from the applicant company In order to verify the exclusive ownership, we check either document below if the domain owner is third party. Domain name use consent form Lawyer opinion letter Points to be checked on the lawyer opinion letter is below. (1) It is described that the domain (secondary domain) is exclusively owned by th applicant company. The domain name is described at item #5 on the lawyer opinion letter. (2) The lawyer who wrote the lawyer opinion letter is really existing that is check with 6. Check for the existence of the lawyer for supplementation.
Domain Name Ownership /	From SECOM: The procedure we verify of domain owner is same for EV and Non-E SSL.

Control non-EV	The only difference is that no lawyer opinion letter is used for Non-EV SSL. See translation of section 4.2 of the verification procedures above.
Email Address Ownership / Control	Translations of sections 3.2, 3.3 and 3.4 of CP at the URL below. https://repo1.secomtrust.net/spcpp/pfm20pub/PfM20PUB-CP.pdf 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key Secom confirm that Certificate Signing Request submitted by the applicant and verify that the corresponding public key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key. 3.2.2 Authentication of company Secom authorize the authentication of LRA or company as follows. By using the official documents from central or local government, database provided by QIIS or QGIS, and another ways that the equal level of authorization possible. In the case the official documents provided by central or local government, we request to give us Certificate of seal impression (issued within 3months) or equivalent as this. 3.2.3 Document to be submitted The documents provided to Secom is as follows. • The information described about the LRA or the company. • Another documents for verification required by Secom. If Secom judge the application is inappropriate after the verification, we return the all documents. We destroy the application form. 3.2.4 Authentication of applicant and certificate user Verification for applicant and certificate user is conducted by the method decided by LRA based on the operation standard. Translations of Mail Authentication Service Verification Procedure provided by SECOM 6. procedure4. Certificate information Verify for DN information Whether or not there is a mistake on DN information. - Not same for company name - Spelling mistake - Domain name mistake - The certificate was issued with the same DN before except the case of renewal or reissue. - Authentication by sending and receiving email. If it is not possible to send or receive the email, we verify the applied email address by making phone call or by another ways to the applicant company. 7. procedure5. Verification of the domain owner By using Whois gateway(NIC domain reference function), we verify the

	applied company name on domain information (the contents included in CommonName) and the applicant (if the domain name use consent form is submitted, it is same as the domain owner). JP domain: http://whois.jprs.jp/ COM, NET, ORG domain: http://www.networksolutions.com/cgi-bin/whois/whois 8. procedure6. Verification by phone call By making phone call to applicant company and make sure that the applicant belongs to the company and apply for the certificate.
Identity of Code Signing Subscriber	SECOM verifies the organization by QIIS or Certificate of the seal impression, and confirms the request of the certificate by making phone call to HRM of the organization. Possession of private key is confirmed as signing public key included in CSR by private key. It is described at section 3 “Identification and authentication” on CP.

Notes from the discussion of https://bugzilla.mozilla.org/show_bug.cgi?id=527419

1) Their typical CPS doesn't require an out-of-bands verification of the organization's existence. Instead they require that the applicant submit "information that shows the existence of the organization". This practices doesn't comply with Mozilla's revised policy which requires that the information be obtained from an independent source of information or an alternative communication channel.	1) There are 2 types of organizations. One is the organization registered in the QIIS, "Tokyo Shoko Research". The applicant information is obtained from the reliable independent source. I understand that this is much like an organizational credit reporting agency? Yes, it is. Tokyo Shoko Research (TSR) is a member of the D&B Worldwide Netw since 2005. http://www.tsr-net.co.jp/en/outline.html -- Another type is the organization not registered in the QIIS, "Tokyo Shok Rearch". This time, Secom require the organization to submit "Certificate of seal impression". "Certificate of seal impression" is the official document issued by the lo government and only available for the representative of the organizatio This is the proof of the real existence of the organization and there is nc identity theft. I believe that this is commonly referred to as a "chop". It be viewed as the same thing as what was formerly required in

	US for corporations before a lot of the corporate-procedure streamlining went into effect, the "embossed seal" which was only available to the corporate secretary. Yes, this is a "chop". This chop is used for a traditional tool of business contract in Japan. The proof of the chop is referred as "Certificate of seal impression". "Certificate of seal impression" is issued by the Legal Affairs Bureaus of Ministry of Justice. This official document is issued and available only to the representative the organization. This means that possessing this official document is the proof of the representative of the applicant's organization and there is no identity th The 'certificate of seal impression': Is it possible for any entity other than the organization to obtain a copy of the impression to compare against? No, it is impossible. Is it possible to send the certificate of registration to the issuing local government for authentication? No, it is impossible.
2) Their CP doesn't state how they validate the authority of the applicant's representative. This should also be an independent source of information or an alternative communication channel.	2) In order to validate the autority of the representative, make a phone cal the organization using the telephone number from the reliable independent source above 1), and ask switchboard for transfer to the applicant's representative. Out-of-band verification of authority to use the organizatior name, utilizing authoritative information (i.e., contact information from something much like Dun & Bradstreet)? I perceive this as acceptable. However, for those organizatior not registered in the QIIS, I cannot perceive this as an effective issuance control (there is no other reliable independent source described). If I am misunderstanding, ple would you correct me? In stead of getting the information ourselves from QIIS directly, howeve we get the Certificate of seal impression that is equally or more reliable information source from the Legal Affairs Bureaus of Ministry of Justice The certificate of seal impression is submitted to us by the representati because of the only available for the representative of the organization. Possessing this official document is the proof of the representative of th applicant's organization. Its watermarked surface of the official document makes us securely ver the original one and no copy or fraud made for the document.

With respect to code signing, I don't see a disclosure on how they link the applicant representative to the applicant organization. This verification is required under the updated Mozilla policy.	Same as the SSL certiifcate, making a phone call to the real existence organization using the reliable independent source and ask switchboar for transfer to the applicant's representative.
I've got a simple - hopefully not silly- question just for my general understanding: Due to the documentation provided "SECOM Passport for Web EV CA2" is not a Root-CA, although the CA Hirachy diagram says that it is cross-signed by "Security Communication EV RootCA2" (which is the one to be embedded). As "SECOM Passport for Web EV CA2" is not up to speed so far, why is it be cross-signed in this case? Thanks for any helpful clarification,	Dear Carsten-san, "SECOM Passport for Web EV CA2" is Subordinate CA. The certificate issued from Security Communication EV RootCA2 to SEC Passport for Web EV CA2 is "Subordinate CA Certificate". On the CA Hirarchy diagram, it is described as "Cross sign" should be "Subordinate CA Certificate". I applogize you if you confused at the description as "Cross sign". Sorry for confusion. The updated CA hierarchy diagram attached on bugzilla #1096205 describes the detail. Please refer it. https://bug1096205.bugzilla.mozilla.org/attachment.cgi?id=8519800