Expert	Date	Subject	Comment
Kent Engstrom (SUNET)	2014-12-02	CREATING A NEW DIVISION ADMINISTRATOR LOG IN ADDING NEW USERS ADDING A NEW ORGANISATION VALIDATION ORDERING A CERTIFICATE CREATING A USER	• Accessed www.digicert.com/account using my SUNET NREN-level Administrator account I setup last Friday. • Created a New Division of type Participant for Linköpings universitet, setting U.H. as Administrator. • U.H. got email with username (= the email I entered for him) and link with secrets in it. • U.H. followed the link and got to a form for setting password (min 8 chars, must have at least on capital letter and one number or special), also security question + answer, and a click-through license called **NREN Participant Agreement** • U.H. got to the login page and could login at once with the username (email) and newly set password. • U.H. selected New User and added his colleague J.H. For him, he could also add phone number and job title. • U.H. found himself and did Edit User to add phone number and email address. • U.H. selected New Division and it seems that he would be able to fill out the form for a new Participant. Is that right? We did not follow through... • U.H. went to New Organization and added Linköpings universitet. He tries to use himself as Validation Contact, with his direct number as phone number and no extension. • U.H. selected to Manage the Organization and added OV validation, and submitted for authorization. • U.H. selected New Domain, selected the Linköpings universitet organization, typed liu.se as domain and marked OV, submitted. • At that point, the clock was 14:51 CET. We are now waiting for any validation contact (phone, email, carrier pidgeon, ...) to take place. • An email was sent 15:35 CET (arrived same minute) to domainmaster@liu.se for domain control validation. • U.H. saw it later and followed the link-with-secrets found in the email. • U.H. got a form where he had to promise that he was authorized to approve certificates for the domain etc. There was also a link to a **Subscriber Agreement**, not the same as the **NREN Participant Agreement**. • U.H. accepted the terms and submitted, and got a "thank you" page. • At that point, the clock was 16:24 CET • U.H. now created a New Division called "Side Order University" of type participant. It seemed to be a subdivision of the Linköpings universitet participant. See the issues page. • At 17:17 CET, U.H. got two emails about "Linköpings universitet Approved" and "liu.se Approved" • At 17:41 CET, U.H. ordered an SSL Plus certificate for ceres.nsc.liu.se. Had to accept **Digital Certificate Subscriber Agreement** • Got to "SSL Plus Certificate Request" where he could immediately Approve or Reject. Approved at 17:48 CET. • Got email 17:50 CET with certificate and intermediate in a ZIP file. • At 18:09 created a user at level User for kent+digicertuser@nsc.liu.se. • Kent did the password setting. As before (password, security question), but no clickthrough. • When Kent logged in as that user, could just access Dashboard and Tools. No Cert Request possible.
Kent Engstrom (SUNET)	2014-12-03	REQUESTING A CERTIFICATE	kent+digicertuser requested a certificate (using URL, as the is nothing in the menu). U.H. approved. Got certificate in a few minutes. OK.
Kent Engstrom (SUNET)	2014-12-04	CREATING DIVISIONS	Created divisions for "Karlstads universitet" and "Kungliga Tekniska Högskolan" after talking to a person each there about taking part in the test. They will validate organizations and domains and request certificates.
Pascal		*Usage's report from scratch:*	• added our entity "Le reseau telematique belge de la recherche, Belnet" as new organisation

Panneels (Belnet)		ADDING A NEW ORGANISATION ORDERING CERTIFICATES VALIDATION	• added me as administrator user for that organisation • asked each of the 3 personal certificates (Digital Signature Plus, Email Security Plus and Premium); after having filled the form, I've received an email with a link to Digicert to create the certificate; at that moment, the certificates were installed in my browser (Firefox 34.0 under Linux Mint 17, amd64 bits version); I've exported them in PKCS12 files and then imported them in Thunderbird (31.3.0, same machine, same OS); there seems to be a problem in Thunderbird when you have to choose which certificate to associate with an identity (only the first 2 certificates are shown); I had 4 in thunderbird's certificates manager which causes a problem... I guess this is maybe a bug in Thunderbird, but didn't find which one yet. Anyway, it worked to sign a mail, with a certificate signed by TERENA Personal CA 3. • I have asked to validate for OV,Grid,EV,CS at 15:00; it is now 15:30 and I see that the OV has already been validated in the portal; I've also received an email to tell me that validation is ok for OV; validated for Grid at 15:51. • I have asked to validate a bunch of domains at 15:30, since 15:40 I've received an email per domain sent to "hostmaster@belnet.be"; fortunately, I receive the emails sent to that alias; there is link to click, a checkmark and your name to put on a form; the validation is still pending as mentioned on the web page after having approved the ownership of the domains.
Pascal Panneels (Belnet)		BUGS	minor: visual : Tools -> Tools Overview : there is a text for "SHA-1 Sunset Tool" and the icon as well; for the others, only the icon
Pascal Panneels (Belnet)		PENDING ORDERS EXPIRY DATE	In the pending orders, the expires date is weird... 620234 2015-01-23 10:53 AM idpstaff.belnet.be Processing 3 years SSL Plus 1970-01-01 1:00 AM
Pascal Panneels (Belnet)	2015-03-02	*Other remarks:* REQUESTING CERTIFICATES	• minor UI : in the "Request a certificate -> SSL Certificates" section, there are several mentions of "at no extra cost", "for free"; is it worth to give these cost relative terms in the descriptions ? • minor UI : in the "Request a certificate -> Document Signing" section, is it worth to have 2 different variants, either for signing 2000 or 5000 documents ? • major UI : when you request a Client Certificate -> Premium as a user with "simple user" privilege (not administrator) you get a page with a message "you are not authorized to get such certificate" (not sure of the correct message) after having filled all the fields and pressed to button "Apply for a certificate", BUT you receive well an email (saying that "You have been approved to create a DigiCert Personal ID Certificate (Premium)") with the link to generate your certificate that you successfully get anyway afterwards. Thus the message on the web page after the request is annoying because user think its request has failed...
Kurt Bauer (ACOnet)	2014-12-04	CREATING A NEW DIVISION VALIDATION	added ORG ACOnet/VIX to Division Universität Wien with myself as contact selected validation for OV only added aco.net and vix.at for domain-validation (appr. 13:30 cet)
Kurt Bauer (ACOnet)	2014-12-04	*Legal name question:* VALIDATION	As neither ACOnet nor VIX are a legal entity, but both are run by the Vienna University Computer Center, I wonder how the validation goes. DV mails came at 13:38 cet for both domains Org validated mail at 13:44 cet the name of the Org was silently changed for *ACOnet/VIX* to *ACOnet* would be interesting how the approval process works, ie. what is validated and on which basis they change org-names vix.at approved mail at 13:46 cet aco.net approved mail at 13:52 cet
			To my surprise and joy, the organisation "Nikhef", being a "samenwerkingsverband" between the (legally KvK registered) Foundation FOM and

David Groep (Nikhef)		OV, GRID VALIDATION	four universities, got instantly approved for at least OV and Grid. Submitted data has the "Legal Name" set to "Nikhef", the address and provide as per the telephone directory, and myself (in the "Identity Management Coordinator" job description) as the validation contact. For the OV and Grid validation, I did not actually get called (also our switchboard never got a call). The telephone directory has "Fom Institute Nikhef" as the name, so that was close enough. No additional documentation was needed to get this far. Process initiated at 09.25 CET, OV cert (for sso.nikhef.nl) issued 09.50 CET.
David Groep (Nikhef)		EV VALIDATION	Request for the EV validation was put in at 13:32 CET, I got the approval at 17:23 CET, so: 4 hours. And doing the upgrade to EV (once validated) actually triggered the 'system error' bug in the portal, so after validation I could not immediately approve the cert - probably the reason customer support called me later. Interestingly, I did not yet get any direct phone call, nor did the FOM foundation headquarters in Utrecht, on the validation of the Organisation. I did not have to send any document. The only actions on my side: • Under validation -> Organisation, I checked the "EV" (and "CS") and pressed "request authorization" • I put in a single EV Multi-domain SSL request and waited. Interestingly, I just got the request for sign&approval. Digicert has independently found out that the "Jurisdiction of Incorporation" for Nikhef is.... NWO: Our top-level organisation two levels removed from Nikhef, the "Netherlands Organisation for Scientific Research; Reg. #: Government Entity; Country: Netherlands" – which is true, since NWO is the mother-organisation of FOM, but I'm surprised that DigiCert found that link. Even more so since the legal document that actually creates "Nikhef" is the "Samenwerkingsovereenkomst NIKHEF Fase III" of which I have a copy, but which is not on-line. And that one mentions FOM, not NWO. But then Nikhef is listed as an NWO Institute on the official NWO web pages and in all NWO documents. And now (18.20 CET which I missed while driving, then 19:20 CET) I just got the call from DigiCert validation and said "yes". They apparently do a lot of issuance in the Netherlands, so maybe that's why they know NWO. Anyway, I've pressed Sign&Approve in the portal once the 'system error' was fixed, and now got an EV cert!
David Groep (Nikhef)		ADDITIONAL DOMAIN NAMES TO AN ORGANISATION	2 December, 20.00 CET: Once Nikhef was validated, added 5 additional domains to it, and requested pre-approval for OV, Grid, and EV for: igtf.net, eugridpma.org, eugridpma.info, gridpma.org, and gridpma.net. Their WHOIS info all lists "Stichting voor Fundamenteel Onderzoek der Materie, Nikhef" as the registrant. You get one mail or each domain to validate ownership, sent to the whois admin contact. This you sign as usual with a checkbox and your full name. At 20.10 CET, submitted a multi-domain EV request with www.eugridpma.org, www.igtf.net , www.eugridpma.info , www.gridpma.org , www.gridpma.net , dist.igtf.net , igtf.net , eugridpma.org, with the last two domains added by hand, the rest taken from the CSR. At 20.29 CET, I got a whole bunch of domain EV approvals, and all the requested domains (linked to organisation Nikhef) are now approved for OV, EV, and Grid. Again signed for the fact that Nikhef is under the NWO umbrella. At 20.36 CET, I got the certificate issued. All cert bundles are actually called "Digicert_certs.zip" if you have them in apache format, so there's no hint about which cert is inside. May be confusing in you are requesting O(100) certs.
David Groep (Nikhef)		REPEATED EV VALIDATION	Once the org and domain have received validation once, you still have to respond to the email challenge and click "Sign & Approve". But the turn-around time gets shorter. Two samples: • Request: 11.26 - validation request mail to admin: 11.31 - issued: 12.51. Total time: 1h25 • Request: 13.58 - validation request mail to admin: 14.05 - issued: 14.29. Total time: 31min

			This was all for actually the same domain name (sso.nikhef.nl). But that coincidence wasn't noticed. Also of interest: you can submit two requests with the SAME key pair. This does not get noticed, you just get a cert twice, with different product names if you so choose.
David Groep (Nikhef)		CODE SIGNING ADDING NEW USERS	Used a colleague of mine (Dennis van Dok) as the tester, having a User role. Invited, and set the contact data for the user with email and phone number (the phone number is visible to me as an admin, but not to the user), and job title "Software Engineer". With the **direct request** URL he requested the CS cert on 2014-12-02 10:42 AM (users don't have a request option in the web panel, see issues #2 and #13) The 'approve' button became available to me (as admin) after validation of the org Nikhef for CS, which took 30 hours (for some unknown reason, since in parallel EV went through in ~1 hr). Pressed the approve button as admin on Dec 3, 20.30 CET, got an email with request for confirmation at 20.32CET. Certificate issued to Dennis van Dok on Dec 3, ~20.50 CET! Subject is rather generic and does not have the requester name in it: Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=Nikhef, CN=Nikhef
David Groep (Nikhef)		DOCUMENT SIGNING	I already had. Nikhef is pre-approved for OV,EV,CS,Grid. Started the process *without* the token connected. Using eToken software 8.1SP1 on Win8.1Pro 64-bit. • Request pre-validation for DS (Document Signing). This came round in less than 1 minute - no further interactions (09.37 CET) • Request a cert using the pre-existing token option. You get a mail to approve the request. Clicked through and waited 2 minutes. (09.41 CET) • Then got a plain-text mail (as the Verfiied User for the Organisation) to allow issuance, with request mail for approval sent to the Verified User again. Clicked "Approve" there. • After 5 minutes, got yet another mail for approval which looked like the EV validation ones (html). Again clicked on a button called "Sign & Approve". (09.47 CET) • After 10 minutes, got yet another mail for approval which looked like the EV validation ones (html). Again clicked on a button called "Sign & Approve". (09.56 CET) • After 5 minutes, got yet another mail for approval which looked like the EV validation ones (html). Again clicked on a button called "Sign & Approve". (10.01 CET) Then after final sign & approve, waited for 3 minutes and the order was approved at 10.04 CET! Dear **David Groep**, Your Document Signing - Organization (5000) certificate for Nikhef has been issued. It is now ready to create on your hardware token. If you have your hardware token ready, you can start the initialization process by downloading the DigiCert Document Signing Installer using this link: https://www.digicert.com/util/DigiCertDocumentSigningInstaller.zip After running the installer, you will need to enter your Initialization Code for this order. You can find the Initialization Code by visiting this link and logging into your DigiCert account: https://www.digicert.com/secure/certificates/XXXXXXXX You need a DigiCert account to request one, as you will need to login to get the initialization code. The ZIP file contains a ".exe" windows executable, even though I had never specified Windows as the plaform. If you do not run windows, you probably should have a token sent to you. But that does not matter, since only Adobe Acobat actually can use the certificate or process signatures... Having clicked the link to install the certificate, having obtained the secret key and having installed the certificate on the token, you can no longer obtain the secret key from CertCentral. So you can only install the cert on a single eToken (which is fine). See attached PDF for screenshots One MUST update the Adobe trust anchors via the "Preferences->Trust" settings for the Assured ID Root to be recognised
David Groep (Nikhef)		API USAGE	The use of the DigiCert API for requesting (and approving, if you are so privileged) in bulk, and later on retrieving the issued certs in a nicely-named way is fairly straightforward. Attached a minimalistic (and rather ugly, sorry) perl script that does the job, with one subdirectory per certificate, support for SAN, and either request or installation support. Will resolve organisation name in case your division has multiple ones.

			https://ndpfsvn.nikhef.nl/repos/pdpsoft/nl.nikhef.pdp.tcs/nl.nikhef.pdp.tcs.dctcs-cli/trunk/dctcs-cli Enjoy, no guarantees, and "-h" gives help: **dctcs-cli**
Teun Nijssen (UVT)		SSL CA 3	CN=TERENA SSL CA 3 DigiCert 'TERENA SSL CA 3' looks **okay**. Comparing it to the comodo 'TERENA SSL CA 2': 1. DigiCert does not include an Extended Key Usage while Comodo contains OID's for TLS Web Server Authentication, TLS Web Client Authentication 2. As discussed, DigiCert 'X509v3 Certificate Policies' contains Policy: X509v3 Any Policy instead of an explicit list 3. DigiCert CRL Distribution Points contain two Full Name URIs
Teun Nijssen (UVT)		SSL PLUS	CN=test-cn-only-2048_tilburguniversity_edu.crt Regular DigiCert SSL Plus cert (2048 bit, sha256WithRSAEncryption) look **okay**. Comparing with Comodo/djangora server certs: 1. Like before the present CN is copied into a not requested subjAltName 2. DigiCert uses two CRL Distribution Point URIs 3. DigiCert includes one Policy OID: 2.16.840.1.114412.1.1 which is the DigiCert OV OID (https://cabforum.org/object-registry/)
Teun Nijssen (UVT)		SSL PLUS	test-cn-only-4096_uvt_nl.crt Beware: 1. the order form for **SSL Plus** states: 'Protect your web or email traffic with strong **2048**-bit SSL encryption using a DigiCert SSL Plus Certificate.' 2. it means really 2048 and **not 4096** bit 3. **order 4096 bit as Unified Communications** 4. Unified Communications 4096 is **okay**; profile remarks like comment above for test-cn-only-2048_tilburguniversity_edu
Teun Nijssen (UVT)		ORDERING SAME CERTIFICATE FOR MULTIPLE NAMES	25 SANs and test-99sans_tilburguniversity_edu.crt 1. Unified Communications order form: 'DigiCert UC Certificates use Subject Alternative Names to let you secure up to 25 server names with one certificate' 2. ordering a CN with 25 subjAltNames produces 26 SANS; the copied CN and the 25 requested 3. X509v3 Subject Alternative Name: DNS:test-25sans.tilburguniversity.edu, DNS:nr00.uvt.nl, DNS:nr01.uvt.nl, DNS:nr02.uvt.nl, DNS:nr03.uvt.nl, DNS:nr04.uvt.nl, DNS:nr05.uvt.nl, DNS:nr06.uvt.nl, DNS:nr07.uvt.nl, DNS:nr08.uvt.nl, DNS:nr09.uvt.nl, DNS:nr10.uvt.nl, DNS:nr11.uvt.nl, DNS:nr12.uvt.nl, DNS:nr13.uvt.nl, DNS:nr14.uvt.nl, DNS:nr15.uvt.nl, DNS:nr16.uvt.nl, DNS:nr17.uvt.nl, DNS:nr18.uvt.nl, DNS:nr19.uvt.nl, DNS:nr20.uvt.nl, DNS:nr21.uvt.nl, DNS:nr22.uvt.nl, DNS:nr23.uvt.nl, DNS:nr24.uvt.nl 4. bt the Comodo limit of 99 or 100 also works as promised in the webex conference. **Okay** 5. X509v3 Subject Alternative Name: DNS:test-99sans.tilburguniversity.edu, DNS:x00.uvt.nl, DNS:x01.uvt.nl, DNS:x02.uvt.nl, DNS:x03.uvt.nl, DNS:x04.uvt.nl, DNS:x05.uvt.nl, DNS:x06.uvt.nl, DNS:x07.uvt.nl, DNS:x08.uvt.nl, DNS:x09.uvt.nl, DNS:x10.uvt.nl, DNS:x11.uvt.nl, DNS:x12.uvt.nl, DNS:x13.uvt.nl, DNS:x14.uvt.nl, DNS:x15.uvt.nl, DNS:x16.uvt.nl, DNS:x17.uvt.nl, DNS:x18.uvt.nl, DNS:x19.uvt.nl, DNS:x20.uvt.nl,

			DNS:x21.uvt.nl, DNS:x22.uvt.nl, DNS:x23.uvt.nl, DNS:x24.uvt.nl, DNS:x25.uvt.nl, DNS:x26.uvt.nl, DNS:x27.uvt.nl, DNS:x28.uvt.nl, DNS:x29.uvt.nl, DNS:x30.uvt.nl, DNS:x31.uvt.nl, DNS:x32.uvt.nl, DNS:x33.uvt.nl, DNS:x34.uvt.nl, DNS:x35.uvt.nl, DNS:x36.uvt.nl, DNS:x37.uvt.nl, DNS:x38.uvt.nl, DNS:x39.uvt.nl, DNS:x40.uvt.nl, DNS:x41.uvt.nl, DNS:x42.uvt.nl, DNS:x43.uvt.nl, DNS:x44.uvt.nl, DNS:x45.uvt.nl, DNS:x46.uvt.nl, DNS:x47.uvt.nl, DNS:x48.uvt.nl, DNS:x49.uvt.nl, DNS:x50.uvt.nl, DNS:x51.uvt.nl, DNS:x52.uvt.nl, DNS:x53.uvt.nl, DNS:x54.uvt.nl, DNS:x55.uvt.nl, DNS:x56.uvt.nl, DNS:x57.uvt.nl, DNS:x58.uvt.nl, DNS:x59.uvt.nl, DNS:x60.uvt.nl, DNS:x61.uvt.nl, DNS:x62.uvt.nl, DNS:x63.uvt.nl, DNS:x64.uvt.nl, DNS:x65.uvt.nl, DNS:x66.uvt.nl, DNS:x67.uvt.nl, DNS:x68.uvt.nl, DNS:x69.uvt.nl, DNS:x70.uvt.nl, DNS:x71.uvt.nl, DNS:x72.uvt.nl, DNS:x73.uvt.nl, DNS:x74.uvt.nl, DNS:x75.uvt.nl, DNS:x76.uvt.nl, DNS:x77.uvt.nl, DNS:x78.uvt.nl, DNS:x79.uvt.nl, DNS:x80.uvt.nl, DNS:x81.uvt.nl, DNS:x82.uvt.nl, DNS:x83.uvt.nl, DNS:x84.uvt.nl, DNS:x85.uvt.nl, DNS:x86.uvt.nl, DNS:x87.uvt.nl, DNS:x88.uvt.nl, DNS:x89.uvt.nl, DNS:x90.uvt.nl, DNS:x91.uvt.nl, DNS:x92.uvt.nl, DNS:x93.uvt.nl, DNS:x94.uvt.nl, DNS:x95.uvt.nl, DNS:x96.uvt.nl, DNS:x97.uvt.nl, DNS:x98.uvt.nl
Teun Nijssen (UVT)		NO COMMON NAME	1. CABform Baseline_Requirements_V1.2.3 states in paragraph 9.2.2 that subject:commonName (OID 2.5.4.3) is Deprecated (Discouraged, but not prohibited) 2. The ordering GUI of both SSL Plus and Unified Communications enforces CN content 3. **okay** for me; commonName will take some time before being overridden.
Teun Nijssen (UVT)		DUAL COMMON NAME	requesting multiple commonNames [req_distinguished_name] C = NL ST = Noord Brabant L = Tilburg O = Tilburg University 0.CN = test-dual-CN-noOU-2048.tilburguniversity.edu 1.CN = test-dual-CN-noOU-2048.uvt.nl 1. requesting it as an SSL Plus cert uses the first CN and omits the second; **should refuse** 2. requesting it as a Unified Communications cert uses the first as the CN and copies both into the subjAltNames; **okay**

Teun Nijssen
(UVT)
		DOUBLE subAltName	requesting a subjectAltName twice
			[req_distinguished_name]
			C = NL
			ST = Noord Brabant
			L = Tilburg
			O = Tilburg University
			OU = Library and IT Services
			CN = test-doubleSAN.tilburguniversity.edu
			[v3_req]

			subjectAltName = DNS:blabla.uvt.nl,DNS:blabla.uvt.nl 1. resulting cert contains CN=test-doublesan.tilburguniversity.edu 2. and subjAltName DNS:test-doublesan.tilburguniversity.edu, DNS:blabla.uvt.nl (so the double blabla is corrected) **okay**
Teun Nijssen (UVT)		DEPRECATED WILDCARD subAltName	the format blabla*.uvt.nl is forbidden; wildcards must start with an asterisk CN = test-CN-wildSAN.tilburguniversity.edu [v3_req] subjectAltName = DNS:blabla*.uvt.nl 1. produces CN=test-cn-wildsan.tilburguniversity.edu with SAN DNS:test-cn-wildsan.tilburguniversity.edu 2. so the CN is copied as normal and the erroneus SAN is omitted without errormessage; **bug**
Teun Nijssen (UVT)		CODESIGNING	**Codesigning cert CN=Nikhef** comparing profile with a Tilburg University codesigning cert issued by Comodo issuer CN=TERENA Code Signing CA looks **okay** 1. DigiCert does not include postalCode, nor street, nor OU but only C, ST, L, O and CN. I would **like to have OU**, 2. CN equals O as we were used to have with Comodo **okay** 3. Comodo CS contained an extension Netscape Cert Type: Object Signing which is very old fasioned; Digicert omits it **okay** 4. X509v3 Extended Key Usage: Code Signing is present of course; **okay** 5. DigiCert uses its Policy OID 2.16.840.1.114412.3.1 which means OV Code Signing **okay**: this is issued by the OV CA, not EV 6. Digicert did not incude an email subject alternative name for the requester or contact **Codesigning cert CN=Tilburg University** 1. The (non EV) Code Signing profile allows 4096 bit keys 2. the OU is indeed omitted, even if the CSR contains an OU. **CN=TERENA Code Signing CA 3** 1. Key Usage: critical Digital Signature, Certificate Sign, CRL Sign 2. Extended Key Usage: Code Signing 3. Policy: X509v3 Any Policy nothing unexpected **okay**
Teun Nijssen (UVT)		DigiCert EV MULTI-DOMAIN	**DigiCert EV Multi-Domain www.tilburguniversity.edu versus www.sidn.nl by Verisign** 1. DigiCert neatly uses sha256WithRSAEncryption 2. two year certs like from the other intermediates means 2 years plus a few days https://cabforum.org/wp-content/uploads/EV-V1_5_2Libre.pdf say: 3. The validity period for an EV Certificate SHALL NOT exceed twenty seven months. It is RECOMMENDED that EV 4. Subscriber Certificates have a maximum validity period of twelve months

			5. 1.3.6.1.4.1.311.60.2.1.3 in a different order than Verisign and includes street and postalCode businessCategory=Private Organization/1.3.6.1.4.1.311.60.2.1.3=NL/serialNumber=41095855/street=Warandelaan 2/postalCode=5037AB the serial number is the Chamber of Commerce dossiernumber used in validating the organisation 6. Verisign uses a set of own values for three OUs; OU=Terms of use at www.verisign.ch/rpa (c)05, OU=Authenticated by VeriSign, OU=Member, VeriSign Trust Network DigiCert omits the OU= 7. the EV Multi-Domain profile supports 4096 bit keys 8. DigiCert AKI, SKI, SAN. KU, CRLDP, AIA and BC as expected 9. DigiCert EKU = TLS Web Server Authentication, TLS Web Client Authentication while Verisign still also includes deprecated 'Netscape Server Gated Crypto' 10. DigiCert CP includes Policy: 2.16.840.1.114412.2.1 (see https://cabforum.org/object-registry/) all looks **okay**, but I need to better read the EV-V1_5_2Libre.pdf (adopted by Ballot 123 on 16 October 2014)