Validation

- When Geant provisions the Trusted Certificate Service to an NREN, an NREN 'division' is created. Simultaneously, a first administrator for the NREN division is invited by the DigiCert service. The NREN division just serves as a container for the subdivisions of its customers. It doesn't do much more. As soon as the NREN decides that a Subscriber (like University X) can start using the service, the NREN creates a sub-divisions for that Subscriber. Such a subscriber division is intended for a single legal entity (like a foundation or inc). Within a subsciber division, its administrator creates one or more organisation names (like 'SURFnet B.V.') belonging to the legal entity, as well as domains (like 'surfnet.nl'). By introducing organisations and domains in the portal, the subscriber applies for validation by the DigiCert Validation department. Preferably first get your organisation name validated and only when that is done start with domains.

- Some NREN customers consists of more than one legal entity, for example when an academic hospital is another legal entity than its university. In that case the customer should apply for a separate division. So one customer can have more than one division.

- For many customers of an NREN a single Organisation suffices. However, some legal entities have very recognisable institutes which present themselves with their own organisation names. A faculty of a university does not qualify for a separate organisation name: that is an Organisational Unit. An example where more than one separate organisation belongs to one legal entity is the Foundation for Fundamental Research on Matter in the Netherlands. Its Nikhef institute belongs to the foundation, but it is widely known under its own name. In such a case the mother-foundation can try to get DigiCert validation for its daughter. That example worked, but your mileage may vary.

- Another reason for validating more that an organisation name within a division is the existence of more than one commonly used name or abbreviation. This certainly works when secondary names are formally registered. For example DigiCert Validation will accept 'Tilburg University' as an alias of 'Universiteit van Tilburg' because both names appear in its Chamber of Commerce file. DigiCert also accepts reasonable presentations in ASCII as organisation names in addition to their real names that contain diacritic characters, like the never to be forgotten (Kent!) Linköping Universitet with alternative name Linkoping Universitet,

- A domain can be validated for use with more than one organization name. So for example tilburguniversity.edu can be validated for O=Tilburg University as well as O=Universiteit van Tilburg.

- Organisations participating in the eScience Grid have another important reason to be careful when setting up their organisation names. In the eScience grid, ownership of datasets is assigned to the full Distinguished Name of end users. The O=Organisation is part of the DN. If a TCS subscriber sets up its first organisation name to satisfy the needs of their Communications and Marketing department, it should also set up an Organisation name for eScience if another spelling was historically in use in the grid. The grid always uses 7-bit ASCII organisation names. It is specifically important that the **NAME** of the eSciense-specific organisation is **EXACTLY the SAME** as the name that was set in the Comodo service in the Confusa eScience Personal portal(s) - including the same capitalisation.

- Immediately after entering an Organization you submit the types of certificates you want to be validated. The wiki page Account mentions in the bullit Users that the administrator who wants to handle Extended Validation will first need to fill in his phone number and his job tiltle. Once that is done, open the organisation and click the 'submit for validation' button. Entering all five (Organization Validated, eScience Grid, Extended Validation, Code Signing, Document Signing) at once is most useful, unless you have defined a separate eScience Organisation as described above; you of course request 'Grid' validation only for the eScience organisation.

- After Organization validation you start requesting domain validations. Only ask domain validation for domains that you own, for which you are the legal 'registrant'. You want to have a good reputation in the eyes of DigiCert Validation; so before requesting validation verify your ownership of domains, for example in these whois services:
    - http://net.educause.edu/edudomain/ for .edu
    - http://www.eurid.eu/ for .eu
    - http://pir.org/ for .org
    - http://www.iana.org/domains/root/db fo more authoritative whois resources

- Domains play no role in Code Signing, Document Signing and Client certificates. So domain validation is about Organisation Validation (OV), Grid Validation (Grid) and Extended Validation (EV). For most domains validate only OV and Grid. The principal domains that you use to present yourself to the world are fine candidates for EV. Don't go for EV validation of domains that are in use at secondary departments not representing the organisation. Don't get EV in the hands of people refusing to read legal texts, especially the TCS Terms of Use. You don't want these people to get you into liability fights with American lawyers.

- Domain validation is currently in principle valid for 36 months; so there is no Domain Control Validation mail per certificate. That's very nice as DCV handling and spam filtering at participants occasionally goes wrong and generally sucks.

- DigiCert does its single shot domain validation using mail to (part of) the infamous 7 adresses admin, administrator, hostmaster, postmaster, webmaster, whois technical contact and WHOIS administrative contact. DigiCert DNS based DCV is available but as yet poorly understood.