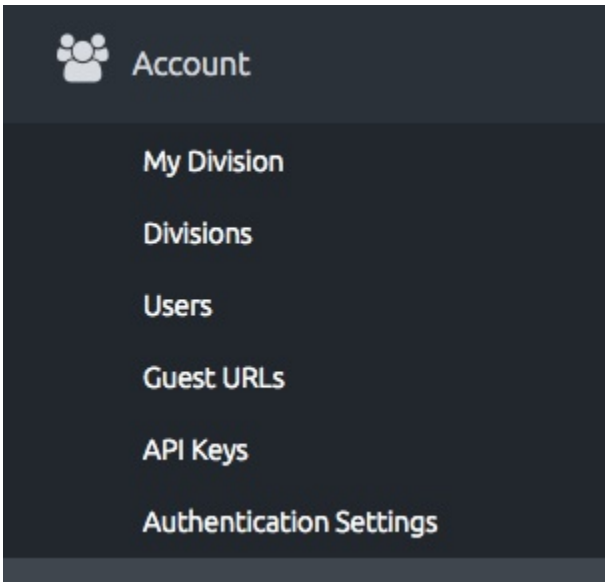
Account



- **My Division:** you find naming data about your NREN if you use an NREN account; and about your subscriber if you are logged into a subscriber account. You can update naming and upload your logo. The info you find here is mainly descriptive. The much more important naming of organisations is handled in Validation.
- **Divisions:** an NREN administrator can create and manage new subscriber divisions. From here you can also inactivate a division that you no longer want to remain valid; for example when a subscriber ceases to exist or terminates his contract with an NREN.
- **Users:** From here administrators can create new users and manage the already existing ones. The new users will receive an email from DigiCert with the link to the page where to set their own password and data. Note that all administrators can approve or reject certificate requests and revocation requests. User accounts can only submit requests. If a username should be allowed to treat Extended Validation SSL certificates make sure that both the fields Phone (phone number) and Title (function name) are correctly filled. If either field is empty, the user cannot do EV work.
    - The regular procedure to validate such a user for EV includes a phone call from DigiCert. This call goes to the formal number of the Institution and commonly via to Human Resource department). DigiCert Validation will ask confirmation whether there is indeed an employee with that name that works under that Title. Make sure that the function name you provide is the correct one.
    - Suggestions: Give to somebody an administrator account only if it is a trusted expert. Give to as few people as possible EV admin rights. Make sure that the click-through 'TCS Terms of Use' has been thoroughly read by everybody.
    - Requesting EV validation for an administrator is done from the Validation menu:
      Validation Organizations Manage Submit for Validation.
- We strongly recommend to **not** make use of
    - **Guest URLs** that anyone can use to issue certificates. Any form of check is completely bypassed when using Guest URLs.
    - **API keys** unless you want to program your own interface.
- Under **Authentication Settings** you can enable the two factors of authentication for login (2FA). Both client certificates and One Time Passwords (OTP) are available. Refer to the DigiCert Two-Factor Authentication section in the user guide (Documentation section in this wiki) for more info. Switch on 2FA by individual user, not for your entire division or entire account; and also one by one. So if one admin locks himself out of the service, another admin can solve the problem. You can click '30 day' caching of a two factor authentication for the computer you are logging into. If its IP address changes or cookies get lost you need re-authentication.