# Instructions for automatic certificate release
# Server.ID Standard (Wildcard) and Server.ID Multidomain

## Explanation:

In order to speed up the processing of Server.ID Standard (Wildcard) and Multidomain certificate orders, the processes for automatic certificate release have been adapted.

In order for certificates to be released automatically, the following conditions must be met:

- The customer data check, which is valid for 13 months, must not have expired yet. The customer check is carried out by us as a Trusted Service Provider (TSP) in the course of manual order processing.
- If you order OV and EV certificates, use separate accounts/organizations for the OV and EV certificates if possible, because the powers of attorney required for EV can hinder the automatic certificate release.
- Since the last certificate release, no changes must have been made to the customer data or contact persons. Changes must first be confirmed by the TSP.
- The certificate data (information in the CSR) must match the customer data stored in the service portal exactly. Upper and lower case must match; However, umlauts must be replaced in the CSR; e.g. Ä by AE, ü by ue, etc.
- For all domains included in the order, the domain validation must have been successfully completed **in advance**.

## Tips:

- In the customer data (data on the organization), enter the organization name according to the proof of identity (e.g. excerpt from the commercial register) in unabridged notation so that it is unique, comprehensible and verifiable. If the organization name is longer than 64 characters, please coordinate the abbreviation with us in advance.
- If a certificate order cannot be released automatically due to customer data changes or an expired customer data check (unfortunately this is not recognizable by you as a customer), then please send us the associated order form signed first. Do not place any further orders in the service portal until this certificate has been approved by us. Only then is there a chance of an automated certificate release again.
- If you are a service provider for other companies, please create separate organizations for your "own" certificates and those of your customers.
- Please also use separate organizations for OV and EV certificates (use the alias function in the customer data to differentiate).
- For customer data and in the certificate request (CSR), use the company's registered office according to the proof of identity and **not** a server location.
- Make sure that there are no double spaces or different special characters (e.g. "-" is not the same as "–") in the customer or CSR information.
- If, during a renewal, you find that any of the above points are not met, then please refrain from renewing and instead post a new order with a corrected CSR. No changes are possible in the course of the renewal.

- Before requesting a certificate, check the status of your domain validations in the "**My Domains**" menu.
    - Update an expired domain validation using the "New" button or start the validation for a new domain using the "Add" button.
    - If possible, always validate the 2nd-level domain. In this case, all subdomains are automatically validated in the DNS and E-Mail validation procedures.
    - Complete domain validation before ordering a certificate or renewal.
    - If you are asked to validate one or more domains in the course of an order, this order cannot be released automatically under any circumstances. We recommend canceling the order, starting and completing the domain validation via the "My Domains" menu (green status) and then restarting the certificate request.