Transitioning SSL Validation from WHOIS to DNS

Recent vulnerabilities in the domain name WHOIS system have highlighted the WHOIS-based domain-validation method as a weakness in the process of validating publicly-trusted digital certificates. As a result, Sectigo and all other public Certificate Authorities have announced that WHOIS-listed email addresses are no longer acceptable for domain validation, nor can historic domain validations based on WHOIS email addresses be reused. You can read more information about this change here.

Renewal or Re-issue of SSL orders that currently use WHOIS email address will fail with error "**CA request failed**" due to this. To ensure continued successful validation and issuance of your SSL certificates, at Openprovider we will be proactively switching the validation method from WHOIS to DNS validation for affected orders. This change will apply automatically before the next renewal or issuance. After the certificate is issued, you will still have the option to change the validation method (e.g., to email or HTTP) if preferred. You ca find available validation methods here.

Revision #2
Created 2026-08-07 14:54:43 UTC by Sarath
Updated 2026-08-07 16:03:35 UTC by Sarath