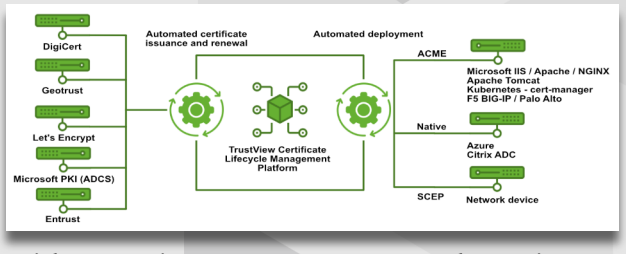
TrustView: Automation Module

Change certificates and fix vulnerabilities with one click directly in TrustView. If you already have the TrustView SSL module, you can manage your entire certificate flow in one place with the Automation module. Ordering, storage, deployment and renewal are no longer a cumbersome task. With TrustView, you can handle it all yourself or let the automation help you

Automation with TrustView

The validity period for certificates will change from the current level of 398 days to just 47 days by 2029. The first change will take place as early as March 2026, when the validity period will be halved. Furthermore, the validity for DNS TXT records will decrease to just 10 days, which is why DNS integration is a necessity to be able to establish an automated process.

TrustView already supports the most popular DNS services such as Cloudflare, EBRAND, MS Azure and many more.

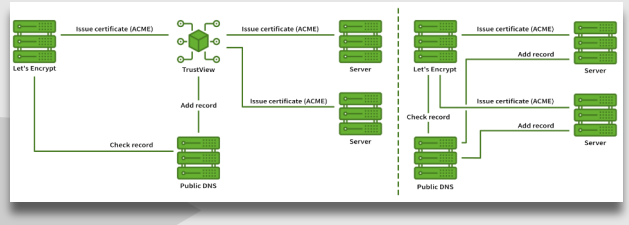


With TrustView, you can automate the entire workflow from ordering and issuing certificates to deployment and renewal of certificates on the individual device on which the certificate is in use.

The automation is thus two-part, with the first part automating the issuing and renewal of the certificates, while the second part automates the installation and ongoing updating of the renewed certificate on the individual devices.

Support for certificate issuance and renewal

TrustView's automation module supports automated issuance of TLS/SSL certificates from the leading providers such as DigiCert, Geotrust, Let's Encrypt and Entrust as well as an internal ADCS. In addition, automated issuance and renewal of MitID company and function certificates is supported directly in TrustView.



Support of clients

TrustView exposes an ACME-based server, so that all clients that support the ACME protocol are automatically supported by TrustView. In addition, TrustView exhibits an API through which you can access certificates and possibly Private keys that are stored in TrustView if needed.

In both cases, the individual client communicates exclusively with TrustView, and in this way it is avoided that the individual client communicates directly with, for example, Let's Encrypt or other certificate suppliers. At the same time, in TrustView you have an overview of any clients who do not renew a certificate as expected, so that you can react before the certificate expires.

The diagram at the bottom left shows the communication between the servers on which the certificate is issued, both with (left side) and without (right side) the use of TrustView. Note that when TrustView is used, all servers do not need access to add DNS records, as this is done from TrustView on behalf of all servers.

We help you get started

To give a good introduction to this module, the installation includes a get-started workshop for your managers. We show you how to connect to your servers, changes certificates and repairs vulnerabilities with one click, and then we help of course with the initial setup.

TrustSkills A/S

Aarhus
Inge Lehmanns Gade 10
DK-8000 Aarhus C

København
Rosenørns Allé 31
DK-1970 Frederiksberg C

Tel. +45 70 60 50 24
sales@trustskills.com
trustskills.com
linkedin.com/company/trustskills