

FACTSHEET

Your solution for an automated and full lifecycle management of TLS/SSL certificates

Joined Solution Sheet



The joined solution between Venafi and D-Trust, allows the integration of D-Trust TLS/SSL certificates into Venafis platform for quick, easy setup and full lifecycle management, allowing a smooth management of certificates from a Trust Service Provider.

Automated certificate lifecycle

Machine identities – keys and certificates – must be properly managed enterprise-wide in order to avoid costly process or system outages. The biggest barrier to efficient machine identity management: decentralized control of TLS/SSL certificates. Machine identity management platforms such as Venafi make it possible to automate the certificate lifecycle across multiple certificate authorities (CAs), auto-install across multiple endpoints, and provide end-to-end management. If you are using Venafi to help solve this problem, the next step is partnering with a reliable, reputable Trust Service Provider that offers not only a service that you can integrate with, but also a wide range of certificate types to suit any use case.

Venafi and D-Trust

Due to the rapid rise in enterprise encryption, the need for certificate authority agility and machine identity management continues to escalate. D-Trust has years of experience providing managed Public Key Infrastructure (PKI) services to international companies and organizations. D-Trust's PKI products and services take the pain out of deploying digital certificates. Venafi's visibility and automation protects machine identities that are integrated with trusted D-Trust digital certificates, enabling organizations to focus on their core business applications.

D-Trust Certificate Service Manager

D-Trust Certificate Service Manager (CSM) is a web-based certificate management platform used to process certificate requests and to manage verification data and certificates in a one stop shop. Using the CSM, all request and verification data for all certificates required in the future can already be sent before the actual request is made. The required verification and the purchase process take place in advance. This means direct access is available to many different types of certificates, for example SSL/TLS certificates securing data transmissions, S/MIME certificates for digital signing and encryption of e-mails and machine certificates for securing communication between machines or objects with organizational affiliation.

Key benefits

- Automate the full certificate lifecycle from issuance to revocation
- Gain full visibility into the demand, usage and workflow of certificate services
- Enforce policies with automated workflow and detailed logging
- Easily track workflow approvals, authorization, and authentication

About Venafi

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. Learn more at www.venafi.com

About D-Trust

D-Trust GmbH is part of the Bundesdruckerei Group and is regarded as one of the pioneers in the field of secure digital identities. Since 2016, D-Trust has been listed with the Federal Network Agency as a qualified trusted service provider in accordance with the European eIDAS regulation. We issue qualified digital certificates for electronic signatures, seals and the qualified remote signature, and also offer other PKI products and services such as the ID card IDent service. For more information please visit: www.d-trust.net