Certificates ready2go – EaSy

Weil Sicherheit Erfahrung braucht.

Automatisiertes Zertifikats-management für interne Server

Im World Wide Web hat sich das Sicherheitsprotokoll TLS fest etabliert. Moderne Browser warnen vor unverschlüsselten Verbindungen und viele Webdienste wären ohne HTTPS gar nicht möglich. Auch in internen Netzen wird immer häufiger TLS eingesetzt. Zentrales Element dabei sind die benötigten TLS-Serverzertifikate.

Mit **Certificates ready2go – EaSy** können TLS-Zertifikate für interne Server vollautomatisiert bezogen und und erneuert werden. So steht ohne manuelles Zutun stets ein gültiges Serverzertifikat zur Verfügung - und das ohne Kompromisse bei der Sicherheit, auf dem Niveau öffentlich gültiger Zertifikate und abhängig vom Trustcenter sogar kostenfrei.

Einzige Voraussetzung ist, dass im internen Netz öffentlich registrierte Domainnamen verwendet werden. Dann übernimmt **Certificates ready2go – EaSy** als Proxy für das ACME Zertifikatsmanagement-Protokoll die Antrags-Validierung bei einem externen Trustcenter wie z. B. Let's Encrypt.

Damit gehören auch für interne Server aufwändige, manuelle Beantragungsprozesse, Verbindungsfehler aufgrund abgelaufener Zertifikate und Browser-Warnungen vor nicht vertrauenswürdigen Zertifikaten der Vergangenheit an.

Ihr Ansprechpartner

Hans-Joachim Knobloch
Diplom-Informatiker,
35 Jahre PKI-Erfahrung

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe

Telefon +49 721 255171-0
hans-joachim.knobloch@secorvo.de
www.secorvo.de

Über Secorvo

Die Secorvo Security Consulting GmbH ist ein auf Informationssicherheit und Datenschutz spezialisiertes und bereits mehrfach ausgezeichnetes Beratungsunternehmen. Alle Mitarbeiter sind ausgewiesene Experten mit vieljähriger Erfahrung.

Seit 2007 ist Secorvo anerkannter Schulungsanbieter für die Qualifizierung zum „TeleTrusT Information Security Professional (T.I.S.P.)". Im September 2019 erscheint das Begleitbuch zur T.I.S.P.-Schulung im dpunkt-Verlag in dritter Auflage.

Automatisieren Sie Ihr Zertifikats-management für interne Server

Ersparen Sie sich komplexe Beantragungsverfahren, abgelaufene Zertifikate und Zertifikatswarnungen im Browser. **EaSy** automatisiert Ihr Zertifikatsmanagement für interne Server und befreit Sie von manuellen Prozessen.

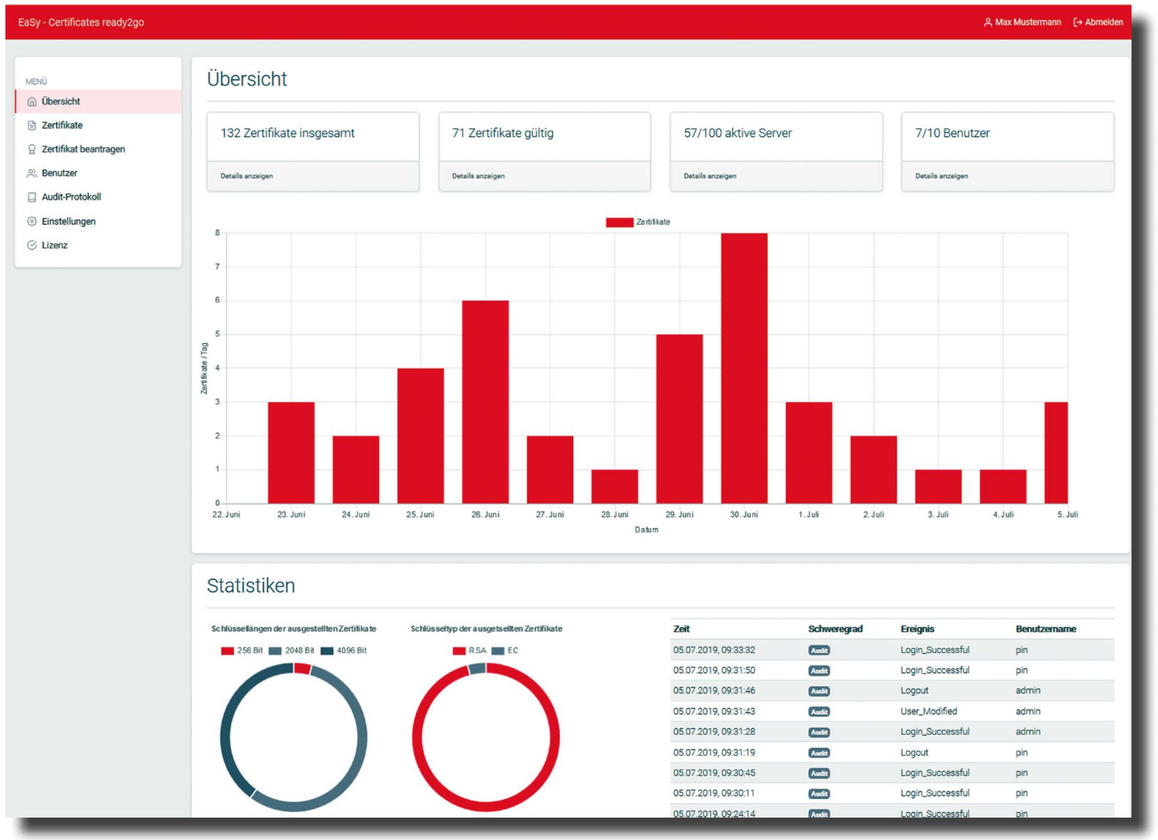
Das ermöglicht EaSy Ihnen

- Automatisierte Domain-Validierung beim Bezug von Serverzertifikaten
- Automatische Erneuerung der Serverzertifikate vor dem Ablaufdatum
- Integriertes Sperrmanagement
- Clientsoftware für praktisch alle gängigen Serverplattformen
- Unterstützt Let's Encrypt und andere öffentliche Trustcenter

Ihr Mehrwert

- Mit **Easy** nutzen Sie die Vorteile des ACME-Protokolls für Ihre internen Server.
- Sie profitieren von kostenlosen, öffentlich gültigen TLS-Zertifikaten für Ihre interne Infrastruktur.
- **EaSy** bietet ein übersichtliches Dashboard für das Monitoring der ausgestellten Zertifikate, der Laufzeiten und der Vorgänge auf dem Enrollment-Gateway.
- Das integrierte Audit-Log protokolliert jeden Zertifikatsbezug und jede Zertifikatserneuerung.
- Zertifikate sperren Sie bei Bedarf direkt über die Weboberfläche.

EaSy-Dashboard



Certificates ready2go – EaSy

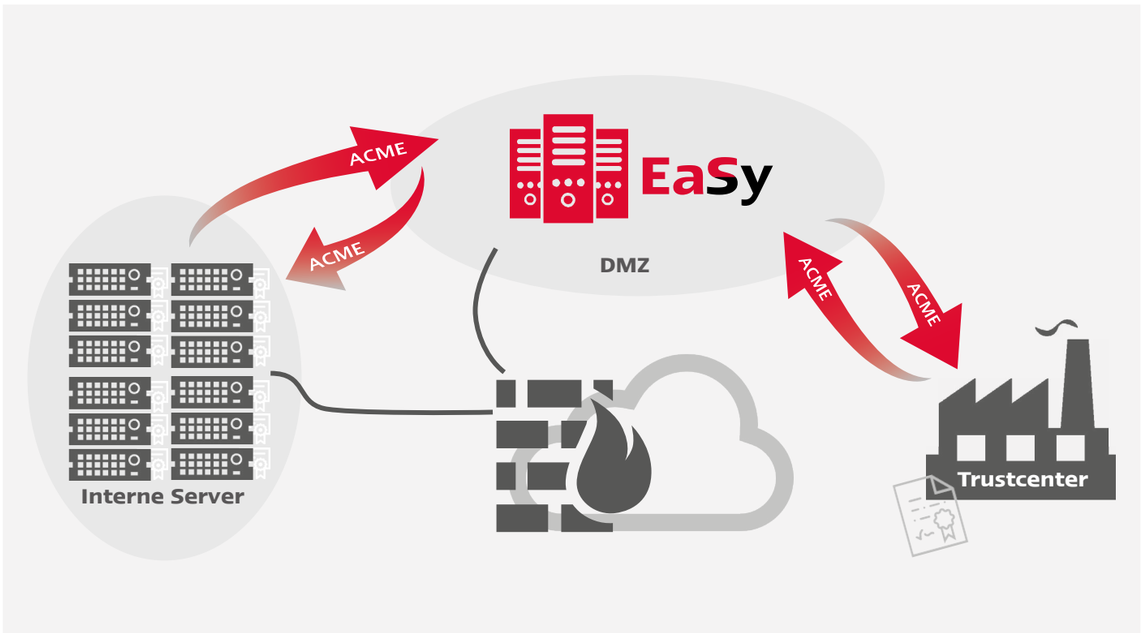
	Enrollment Gateway
Zertifikats-Management	Zertifikate für interne Server über ACME beziehen und erneuern
	Kompatibel mit Certbot und anderen etablierten ACME-Clients
	Anbindung an Let's Encrypt und Buypass Go integriert
	Weitere ACME-Zertifizierungsstellen ergänzbar
Dashboard	Komfortable Zertifikatssperrung
	Übersichtliche Weboberfläche für die EaSy-Administration
	Detaillierte Statistiken und Audit-Logs
	Zertifikatsanfrage (PKCS#10) über Weboberfläche

Funktionsweise

- EaSy agiert als Proxy zwischen dem ACME-Client Ihres internen Servers und öffentlichen Zertifizierungsstellen wie Let's Encrypt.
- Das Enrollment Gateway ist sowohl aus Ihrem internen Netz als auch über das Internet erreichbar und führt stellvertretend Domain-Validierungen für Ihre internen Server durch.

Voraussetzungen

- Verwendung öffentlich registrierter Domainnamen im internen Netz
- Nutzung von Split-DNS, bei dem die internen Servernamen bei Abfragen von extern auf das Enrollment Gateway aufgelöst werden
- Red Hat, SUSE oder Ubuntu Linux Server mit Docker als Systemplattform für das Enrollment Gateway



Icons designed by Freepik and Madebyoliver