Whitepaper

essendi xc ACME-Adapter

Automatisiertes Zertifikatsmanagement mit ACME

essendi xc ist ein vollumfängliches Management-System mit einem unternehmensweiten Repository für verschiedene Zertifikate und Zertifikatstypen. Es deckt den kompletten Zertifikate-Life-Cycle von der Beantragung bis zur Installation ab. Somit bleiben jederzeit sämtliche Zertifikatsbestände im Blick, auch solche die automatisch per ACME ausgestellt und verteilt werden (Details s.u.). essendi xc erleichtert Zertifikatsprozesse und ermöglicht eine individuell definierbare Automatisierung der Abläufe, z.B. für Validierung, Ausstellung, Erneuerung von Zertifikaten.

TLS, ACME und Let's Encrypt

Für den Aufbau einer verschlüsselten Verbindung zu einer Webseite haben sich digitale Zertifikate in Verbindung mit SSL/TLS durchgesetzt. Für die einfache und kostenlose Ausstellung von SSL/TLS-Zertifikaten hat sich die Zertifizierungsstelle Let's Encrypt in Verbindung mit ACME etabliert.

Um es Let's Encrypt zu ermöglichen, die Inhaberschaft einer Domain schnell und automatisiert abzuprüfen, wurde das ACME Protokoll (Automatic Certificate Management Environment RFC8555) geschaffen. **ACME reduziert den Aufwand für die Ausstellung eines Zertifikats sowohl für den Endanwender, als auch für die Zertifizierungsstelle.** Die zugehörigen Tools sind weit verbreitet und meistens open source. Sie unterstützen bei der Automatisierung der Domainvalidierung und darüber hinaus auch bei der Installation der Zertifikate im Webserver.

Automatisiertes Zertifikatsmanagement in Unternehmen

Mit zunehmender Anzahl digitaler Zertifikate bei immer kürzerer Laufzeit steigt in Unternehmen der administrative Aufwand. Ungeregelte Prozesse und Zuständigkeiten erhöhen das Risiko, dass ungewollt ablaufende Zertifikate zu Betriebsstörungen oder Systemausfällen führen.

Zertifikatsmanagement-Lösungen und Automation bieten folgende Vorteile:

- Zentrale Übersicht und Kontrolle der im Unternehmen befindlichen Zertifikate
- Sicherstellen von Compliance-Anforderungen
- Verwalten und Abrechnen mehrerer CAs
- Schnelles und einfaches Ausstellen, Installieren und Erneuern von SSL/TLS-Zertifikaten
- Sichere Aufbewahrung des sensiblen Schlüsselmaterials

Diesen Herausforderungen hat sich die essendi it gestellt und eine innovative und mächtige Plattform zum Management digitaler Zertifikate entwickelt: **essendi xc**.

ACME-basierte Client-Tools wie Certbot erlauben eine vollständige Automatisierung der Ausstellung von SSL/TLS-Zertifikaten für einen Webserver. Damit wird es möglich, erhaltene Zertifikate voll automatisiert in die bekannten Webserver wie z.B. nginx, Apache sowie IIS installieren zu können. Administratoren schätzen besonders den weiteren Vorteil, dass auch bei Erneuerung eines Zertifikats keine manuellen Eingriffe mehr nötig sind.

Die Grenzen der Zertifizierungsstelle Let's Encrypt

Gehen die Anforderungen für TSL-Zertifikate über die Domainvalidierung hinaus, sind Zertifikate von Let's Encrypt nicht geeignet. Weder Organisationsvalidierung noch weitere Zertifikatstypen, wie sie z.B. für die Signatur von E-Mails, Dokumenten und Code notwendig sind, sind verfügbar. Hierfür müssen also weitere CAs hinzugezogen werden.

Wie behält man nun den Überblick und die Kontrolle über diese weitgehend automatisiert und ohne Beteiligung der PKI-/Security-Administration verwalteten Zertifikate? Wie verbindet man das Handling der verschiedenen CAs dahinter?

Höhere Reichweite von ACME und Let's Encrypt mit dem essendi xc ACME-Adapter

Durch den ACME-Adapter von essendi xc werden die Möglichkeiten von ACME umfänglich erweitert.
Der xc ACME Adapter kombiniert sämtliche Vorteile eines ACME Clients wie Certbot (Automation, Erneuerung von Zertifikaten und Verteilung in diverse Zielumgebungen etc.) mit dem Nutzen der professionellen Zertifikatsmanagement-Plattform essendi xc (Erweiterung des Spektrums an Zertifizierungsstellen und Zertifikatstypen aller Art etc.).

ACME Clients wie Certbot können in Kombination mit dem essendi xc ACME Adapter und essendi xc Webserverzertifikate vollautomatisiert anfordern und verwalten. Der essendi xc ACME Adapter unterstützt die Challenge-Typen DNS und HTTP.

Neben den Funktionalitäten von essendi xc zur Überwachung und Verwaltung von Zertifikaten sind diverse Zertifizierungsstellen anbindbar. **Diese Multi-CA-Fähigkeit von essendi xc bietet die Möglichkeit über das ACME Protokoll Zertifikate bei beliebigen Zertifizierungsstellen zu beantragen.** An den xc ist bereits eine Vielzahl öffentlicher und privater Zertifikatsanbieter angebunden. Beispiele sind D-Trust, DigiCert, GlobalSign, PSW-Group, SwissSign sowie die Microsoft PKI. Die Integration weiterer Zertifizierungsstellen ist möglich.

Viele Server und Komponenten im internen Netzwerk dürfen keine Verbindung zum freien Internet aufbauen. Die Konnektivität von einem ACME-Client mit der Let's Encrypt-CA ist damit nicht gegeben. Mit dem essendi xc-ACME-Adapter als internem ACME-Server können Sie auch interne ACME-Clients mit Zertifikaten versorgen.

Ihre Vorteile auf einen Blick

ACME und essendi xc sind in Kombination noch leistungsfähiger und bieten folgende Features:

- **Hoher Automatisierungsgrad** und Nutzung bekannter und akzeptierter Verfahren zur Zertifikatsbeantragung
- Alle Zertifikate in essendi xc werden **überwacht** und stehen unter **zentraler Kontrolle** im Repository.
- Zertifikate können aus essendi xc heraus **revoziert** (gesperrt) werden.
- Zertifizierungsstellen können aufgrund der **Multi-CA-Fähigkeit** von essendi xc frei gewählt werden. Bei Bedarf ist ein Wechsel der Zertifizierungsstelle einfach möglich.
- Das Nutzungsprofil von Zertifikaten kann durch **zusätzliche Attribute**, z.B. im Subject, erweitert werden.
- Derart angereicherte Zertifikate ermöglichen die **organisatorische Zuordnung, Gruppierung und Validierung**.
- essendi xc stellt sicher, dass die digitalen Zertifikate **Ihren Compliance-Vorgaben** entsprechen.

Über ACME hinaus sind mögliche Anwendungsbereiche von essendi xc, neben der Automatisierung von Webserverzertifikaten, im gesamten Umfeld Internet of Things, in Cloud Umgebungen (z.B. in Zusammenspiel mit Docker) und in der E-Mail-Kommunikation.

Für eine LiveDemo sprechen Sie uns an.

+49 89 944 697 71 **info@essendi.de**

essendi it GmbH, Dolanallee 19
DE-74523 Schwäbisch Hall