Whitepaper
essendi xc ACME-Adapter

Automatisiertes Zertifikatsmanagement in Unternehmen

Je größer die Anzahl von digitalen Zertifikaten im Unternehmen, desto höher auch die damit verbundenen administrativen Aufwände. Ungeregelte Prozesse und Zuständigkeiten erhöhen das Risiko ungewollt ablaufender Zertifikate, die Funktionsstörungen im Betrieb sowie ganze Systemausfälle zur Folge haben können. Die steigende Anzahl von Zertifikaten bei gleichzeitig immer kürzeren Laufzeiten erfordern Managementlösungen und Automation.

Zu den Herausforderungen steigender Zertifikatsbestände zählen unter anderem:

- Zentrale Übersicht und Kontrolle der im Unternehmen befindlichen Zertifikate, wie deren Anzahl, Ablaufdaten, Installationsorte etc.
- Definition von Prozessen und Vorgehensweisen für alle am Zertifikateprozess Beteiligten
- Sicherstellen von Compliance Auflagen, wie z.B. Zertifikate-Policies
- Verwalten und Abrechnen mehrerer CAs
- Unabsichtliches Ablaufen von SSL Zertifikaten
- Schnelles und einfaches Ausstellen, Installieren und Erneuern von SSL Zertifikaten
- Sichere Aufbewahrung des sensiblen Schlüsselmaterials

Diesen Herausforderungen haben sich die Entwickler von essendi it gestellt und mit essendi xc eine innovative und mächtige Plattform zum Management digitaler Zertifikate entwickelt.

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 sichere Datenübertragung haben sich mittlerweile digitale Zertifikate in Verbindung mit TLS (Transport Layer Security) durchgesetzt. Für die einfache und kostenlose Ausstellung von TLS-Zertifikaten hat sich u.a. 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, unterstützen bei der Automatisierung der Domainvalidierung und darüber hinaus auch bei der Installation der Zertifikate im Webserver.

ACME-basierte Clients wie Certbot erlauben eine vollständige Automatisierung der Ausstellung von TLS-Zertifikaten (x.509) 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? Und wie verbindet man das Handling der verschiedenen CA's 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 Zertifikatstypen aller Art anfordern. Der essendi xc ACME Adapter unterstützt die Challenges DNS und HTTP standardmäßig. Weitere Validierungsregeln können in essendi xc hinterlegt und automatisch geprüft werden.

Neben den Funktionalitäten von essendi xc zur Überwachung und Verwaltung von Zertifikaten sind diverse Zeritifizierungsstellen anbindbar. Diese Multi-CA-Fähigkeit von essendi xc bietet die

Möglichkeit über das ACME Protokoll Zertifikate bei beliebigen Zertifizierungsstellen zu beantragen. Dies beinhaltet öffentliche Zertifizierungsstellen, wie z.B. SwissSign, QuoVadis oder D-Trust, aber auch private CAs, wie z.B. die Microsoft PKI und andere.

Ihre Vorteile auf einen Blick

Mit essendi xc wird ACME noch leistungsfähiger und um folgende weitere Features erweitert:

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

Mögliche Anwendungsbereiche neben der Automatisierung von Webserverzertifikaten finden sich beispielsweise 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 oder über info@essendi.de