Sicherung der Vertraulichkeit, Authentizität und Integrität der internen Unternehmenskommunikation

Migration der Public-Key-Infrastructure

Kunde
RheinEnergie AG

Branche
Wasser- & Energieversorgung

Für Interessenten an:
Enterprise-PKIs auf Basis Active Directory Certificate Services (ADCS).

Aufgabe
Die bestehende Public-Key-Infrastruktur der RheinEnergie AG soll auf eine neue Version aktualisiert werden. Dabei soll die bestehende Infrastruktur nicht beeinträchtigt oder gestört werden. Die Migration soll unter Berücksichtigung der bestehenden Konfiguration durch zu entwickelnde Automatismen unterstützt und umgesetzt werden.

Lösung
Für die Installation, Migration und die Verwaltung der RheinEnergie PKI wurde jeweils ein Windows Powershell® Modul entwickelt, welches sich durch Portabilität, Effizienz und Betriebssystemübergreifende Kompatibilität auszeichnet.

Ergebnis
Durch die bereitgestellten Windows Powershell® Module konnte die Migration unter Einhaltung der fachlichen, terminlichen, finanziellen und qualitativen Vorgaben eingehalten werden.

„Ein qualifiziertes Review der Bestandsumgebung war längst überfällig. Die tiefgreifende Vorbereitung, inklusive Dokumentation und Eigenentwicklung durch exceet, hat die Administration unserer PKI nachhaltig vereinfacht."

Pascal Thimm
Systemadministrator Netzwerktechnologie (CIN) bei der RheinEnergie AG

Die RheinEnergie AG ist ein regionales Energieversorgungsunternehmen für Strom-, Gas-, Wasser- und Wärmeversorgung mit Sitz in Köln. Das Unternehmen versorgt rund 2,5 Millionen Menschen, Industrie, Handel und Gewerbe mit Energie und Trinkwasser. Die RheinEnergie befindet sich im Besitz zweier Gesellschafter: 80 Prozent der Anteile hält die GEW Köln, die als Holdinggesellschaft wiederum direkt und indirekt zu 100 Prozent im Besitz der Stadt Köln ist. In der Satzung der RheinEnergie ist festgelegt, dass sie sich immer mehrheitlich in kommunalem Besitz befinden muss. Die restlichen 20 Prozent befinden sich im Besitz der RWE.

Die RheinEnergie AG führt seit 2002 das operative Geschäft der GEW Köln AG aus, welche wiederum Mehrheitsanteilseigener der RheinEnergie ist. Neben der RheinEnergie AG gehören der GEW Köln AG noch die Net-Cologne GmbH, die Brunata Metrona-Gruppe Hürth (Wärmemessung und -abrechnung) sowie die Stadtwerke Düsseldorf an.

Die Situation

Die RheinEnergie AG betreibt für die Unternehmensteile GEW Köln AG und für die Brunata Metrona-Gruppe Hürth jeweils eine auf Microsoft Active Directory Certificate Services® basierende Public Key Infrastruktur (PKI), die in jeweils einer eigenen Active-Directory Domäne integriert ist (im Folgenden unter „RheinEnergie PKI" zusammengefasst).

Die RheinEnergie PKI beinhaltet sieben Zertifizierungsstellen, die sich auf die Organisationsteile der GEW Köln AG und der Brunata Metrona-Gruppe Hürth erstrecken und auf einer Version des Windows Server® Betriebssystems basieren, dessen Support vom Hersteller abgekündigt wurde.

Die RheinEnergie Enterprise-PKI stellt Zertifikate für Domänen-Benutzer, Domänen-Clients, Domänen-(Web-) Server, Netzwerkkomponenten, Code-Signatur, Mobile-Devices und für Smartcard-Logon aus. Die Registrierung der Antragssteller, die Zertifikatsausstellung und der Zertifikatsrollout läuft dabei sowohl manuell (bspw. über

Webservices/ Simple Certificate Enrollment Protocol (SCEP) als auch automatisiert ab (Active Directory Certificate Enrollment Policies).

Die Aufgabe

Gegenstand dieses Projekts war die Migration der RheinEnergie PKI, die in der beschriebenen Organisation verankert ist. Dabei sollte die bestehende Konfiguration analysiert, dokumentiert und übernommen werden.
Zu berücksichtigen war insbesondere der Umstand, dass die Migration in der Test- sowie Produktivumgebung die Funktionsfähigkeit und Operabilität der Bestands-Enterprise-PKI nicht beeinträchtigt und der Wechsel auf die migrierte Enterprise-PKI nahtlos abläuft. Dafür mussten folgende Kriterien eingehalten werden:

- Sicherstellung, dass die Konfiguration der migrierten RheinEnergie-PKI die der Bestands-Enterprise-PKI nicht überschreibt;
- Sicherstellung, dass die Clients nach Abschluss des Setups der Produktionsumgebung den neuen Vertrauensraum importieren, ohne dass manuelle Interaktion notwendig ist;
- Sicherstellung, dass die Bestands-Enterprise-PKI nicht mehr für die Ausstellung von Zertifikaten genutzt wird, aber weiterhin für Sperrungen und die Erzeugung von Sperrinformationen verwendet werden kann;
- Sicherstellung, dass Services und Implementierungen im Umfeld der Active Directory Certificate Services® weiterhin funktionieren und auf die neue Enterprise-PKI und deren Schnittstellen zugreifen bzw. diese nutzen können;
- Sicherstellung, dass verwendete Administrationswerkzeuge kompatibel zu der migrierten RheinEnergie-PKI sind;
- Sicherstellung, dass die bestehenden Hardware Security Module (HSM) an die Zertifizierungsstellen der migrierten RheinEnergie-PKI angebunden und genutzt werden können.

Die Lösung

Auf Basis dieser Anforderungen und unter Berücksichtigung der Aktualisierung auf ein aktuelles Betriebssystem wurden folgende Liefergegenstände erarbeitet und übergeben:

- Ein Projektplan, der für den Auftragnehmer und den Auftraggeber Inhalte, Meilensteine, Abhängigkeiten, Fortschritte und Ressourcenzuordnungen zeigt;
- Ein Migrationskonzept, welches als Basis für den Aufbau der maßgeblichen Test- und Produktivsysteme gilt;
- Ein Testkonzept, welches die technischen und funktionalen Tests beschreibt, die zur Nachweisführung der ordnungsgemäßen Migration durchzuführen sind;
- Ein Set aus drei Windows-Powershell-Modulen, die für die Installation, Migration und das Management der Active Directory Certificate Services® verwendet werden.

Modul 1: ADCS Installation - *„adcs_inst“*
Das erste Powershell-Modul ermöglicht ein Setup auf sehr hohem Automatisierungsgrad, bei gleichzeitiger Beibehaltung der Kontrolle über den Prozess. Vor der Durchführung der jeweiligen Installationsschritte wird die zu implementierende Konfiguration aufgeblendet, die der Installateur prüfen, ggf. anpassen und bestätigen muss. Sollte das Setup fehlschlagen, so lässt sich mit diesem Modul die Konfiguration auch restlos beseitigen, sodass eine Installation nach Korrektur der Fehlerursache erneut ausgeführt werden kann. Das Modul „adcs_inst“ bedient sich u.a. an vordefinierten Property-Dateien und den Daten die das Modul „adcs_mig“ (siehe unten) zentral bereitstellt.

Modul 2: ADCS Migration - *„adcs_mig“*
Das zweite Powershell-Modul ermöglicht eine Analyse der Konfiguration der Bestands-PKI inkl. eines zentralisierten Backups der relevanten Konfiguration der betreffenden Zertifizierungsstelle.

Der Datenexport dient dem Modul „adcs_inst“ als Input und ist zugleich Grundlage dafür, dass die Konfiguration der migrierten RheinEnergie-PKI identisch mit der der Bestands-PKI ist, zugleich aber alle Neuerungen des Releases der Active Directory Certificate Services reflektiert.

Modul 3: ADCS Management - *„adcs_mgmt“*
Das dritte Powershell-Modul ermöglicht das Management der jeweiligen Zertifizierungsstelle und erleichtert die Interaktion mit Schnittstellen. So lassen sich mit diesem Modul

- die jeweilige CA starten und stoppen;
- Sperrlisten manuell generieren;
- relevante Konfigurationen in Richtung des angebundenen Active Directories exportieren oder auch im Active Directory suchen;
- die Events, die die Zertifizierungsstelle betreffen, nach Typ und nach Zeitraum sortiert exportieren / filtern.

Die drei Module weisen folgende Eigenschaften auf:

- Sie sind jeweils mit der aktuellsten Version der Microsoft Power Shell® / Microsoft Powershell ISE® / sowie Microsoft Windows Server® kompatibel;
- Sie sind in der Lage Ihre eigene Konfiguration zu exportieren, welche über moduleigene Property-Dateien eingebracht wird;
- Sie werden ausschließlich über eigene Property-Files konfiguriert, sodass diese auch modular und voneinander losgelöst verwendet und portiert werden können;
- Sie können in Form einer gekapselten ausführbaren Datei genutzt werden, sodass nachträgliche Änderungen an den Inhalten und Funktionen nicht mehr möglich sind und diese auch nicht eingesehen werden können.

Das Ergebnis

Durch die modulare und transparente Gestaltung der Powershell-Module sowie der damit einhergehende Automatisierungsgrad haben zum Projekterfolg beigetragen, da die Durchführung der technischen Migration innerhalb eines kurzen Zeitraums erfolgreich abgeschlossen und ohne Auswirkungen auf den Nutzerkreis der RheinEnergie-PKI in den Produktwirkbetrieb überführt werden konnte.

Zudem operationalisieren die Powershell-Module wichtige administrative Regeltätigkeiten und bilden die Grundlage für eine zukünftige Migration auf ggf. folgende Versionen der Active Directory Certificate Services.

Vorteile auf einen Blick

- Automatisierung der Installation, Migration und des Managements der Active Directory Certificate Services
- Modulare Struktur erlaubt das unabhängige Verteilen der Module auf unterschiedliche Systeminstanzen
- Transparente Konfiguration der betroffenen Zertifizierungsstellen durch einsehbare Property-Dateien und Protokollierung des Setupvorgangs mit Zeitstempel
- Kompatibilität mit den aktuellen Versionen von Microsoft Windows Server® und Microsoft Windows Powershell®
- Geringer Anpassungsaufwand für Folgeversionen von Microsoft Windows Server® und Microsoft Windows Powershell®

Über exceet Secure Solutions

Die exceet Secure Solutions GmbH ist eine 100%ige Tochtergesellschaft der international agierenden exceet Group AG, einem Technologiekonzern, der sich auf die Entwicklung und Fertigung intelligenter, komplexer und sicherer Elektronik spezialisiert hat. Gestartet 2000, als Spezialist für die Absicherung elektronischer Geschäftsprozesse mit Hilfe von qualifizierten elektronischen Signaturen und Zeitstempel, liegt heute der Fokus des Unternehmens auf sicheren Lösungen in den Geschäftsbereichen Internet of Things (IoT) und IT Security. Ergänzt wird das Angebot durch Hardware Security Modules (HSMs), PKI-Lösungen und Produkte und Services für Signaturen und Zeitstempel, inkl. Trust-Center-Betrieb.

Erweiterung der Wertschöpfung

exceet Secure Solutions schafft Lösungen, die insbesondere hohen Anforderungen an Qualität, Stabilität und vor allem Sicherheit gerecht werden. Dazu fungiert das Unternehmen als Komplettlösungsanbieter oder befähigt seine Kunden zur Umsetzung eigener Lösungen. Als Komplettlösungsanbieter beginnt die Umsetzung bereits bei der Nutzenanalyse, reicht über die Erstellung von IT-Security-Konzepten und endet mit der Integration der Gesamtlösung in die bestehenden Prozesse. Als Tochterunternehmen eines innovativen Technologiekonzerns rundet die konzerninterne Produktion von benötigter Hardware das Leistungsspektrum ab.

Qualifizierte Zeitstempel und Signaturen

exceet Secure Solutions GmbH, vormals AuthentiDate International AG, wurde am 9. Nov. 2001 als erstes Unternehmen mit Schwerpunkt auf qualifizierte Zeitstempel von der Bundesnetzagentur als akkreditierter Zertifizierungsanbieter nach neuem deutschem Signaturgesetz und europäischen Richtlinien akkreditiert. Damit bieten die von exceet Secure Solutions GmbH gelieferten Zeitstempel für alle elektronischen Daten den gesetzlich anerkannten höchsten Schutz und können auch international für rechtssichere elektronische Prozesse verwendet werden.

exceet Secure Solutions GmbH
Phone +49 (0) 211 436989-0
Email info@exceet-secure-solutions.de
Web www.exceet-secure-solutions.de