Anwendungshinweis für die Normenreihe IEC 62351

Informationssicherheit in der Netz- und Stationsleittechnik

DKE
VDE DIN

Inhalt

Anwendung der Normenreihe IEC 62351 zur sicheren Kommunikation in der Energieversorgung

Einführung

Durch die Verabschiedung des IT-Sicherheitsgesetzes [1] zum Schutz kritischer Infrastrukturen im Jahr 2015 werden auch die Betreiber von Grundversorgungsnetzen (Strom, Gas, Wasser) vor die Aufgabe gestellt, die vorhandene Leit- und Fernwirkinfrastruktur gegenüber Cyber-Angriffen zu schützen. Neben den eingesetzten Komponenten wie Netzwerkgeräte, Bediensysteme und Fernwirkgeräte wurde die Kommunikation zwischen diesen Komponenten als Angriffsziel identifiziert. Abbildung 1 zeigt den Aufbau eines typischen Leit- und Fernwirksystems.

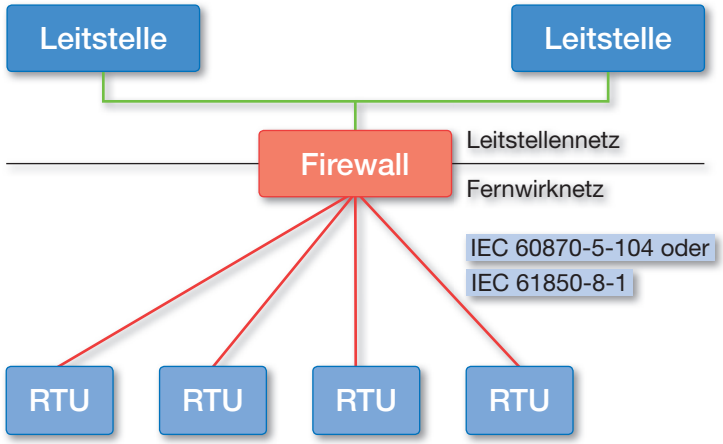

Abbildung 1: Aufbau eines typischen Leit- und Fernwirksystems

Während der Schutz der eingesetzten Komponenten durch Maßnahmen wie Systemhärtung oder Einsatz von Firewalls erreicht werden kann, stellen die eingesetzten Kommunikationsprotokolle (IEC 60870, IEC 61850) keine eigenen Sicherheitsmechanismen bereit, mit denen die Kommunikation hinreichend geschützt werden kann. Im Leitstellennetz stellen die fehlenden Mechanismen eventuell kein gravierendes Problem dar, die ungesicherte Kommunikation im Fernwirknetz ist auf jeden Fall aus Sicherheitssicht relevant.

Anwendung IEC 62351-3/5

Erfolgt die Kommunikation zwischen der Leitstelle und der Fernwirktechnik mittels IEC 60870-5-104 [2] kann der Normenteil IEC 62351-5 [6] in Verbindung mit Teil IEC 62351-3 [5] zur Absicherung der Kommunikation (Authentizität, Integrität, Vertraulichkeit) eingesetzt werden. Für IP-basierte Protokolle wird durch die IEC 62351 in diesem Fall kein neues Sicherheitsprotokoll definiert, sondern die Anwendung des bekannten SSL/TLS-Protokolls (Transport Layer Security) spezifiziert, das in vielen Anwendungen weit verbreitet ist, wie z. B. Zugriff auf Web Server, Online-Banking, etc. Für Kommunikation nach IEC 60870-5-101 [3] enthält der Teil IEC 62351-5 ein Verfahren zur Integritätssicherung der übertragenen Daten.

Anwendung IEC 62351-4

Beim Einsatz von IEC 61850-8-1 [4] zur Kommunikation zwischen Leit- und Fernwirktechnik stehen im Teil IEC 62351-4 [7] zwei Verfahren zur Verfügung. Beim sog. T-Profil wird analog zu IEC 60870-5-104 auf das Protokoll TLS gesetzt, während das A-Profil einen Integritätsschutz auf Datenebene bietet.

Anwendung IEC 62351-9

Die Nutzung der Sicherheitsmechanismen der Normenreihe IEC 62351 zum Schutz der Kommunikation setzt den Einsatz von Schlüssel- und Zertifikatsmaterial voraus, welches für die Verifikation der Kommunikationspartner und die Sicherung der Kommunikation benötigt wird.

Die Verwaltung des Schlüssel- und Zertifikatsmaterials bedeutet zusätzlichen Aufwand für den jeweiligen Betreiber. Zu diesem Zweck enthält der Teil IEC 62351-9 [8] Informationen, wie das notwendige Management umgesetzt werden kann. Neben der Verwaltung von Schlüssel- und Zertifikatsmaterial werden dort auch Themen wie die Verteilung und Aktualisierung von Schlüssel- und Zertifikatsmaterial behandelt.

Problemfall Diagnose/Wartung

Aktuell deckt jedoch die Normenreihe IEC 62351 das Themengebiet Diagnose und Wartung unzureichend ab, da keine geeigneten Verfahren oder Protokolle vorgeschlagen werden und typischerweise proprietäre Kommunikationsprotokolle zum Einsatz kommen, die nicht über eigene Sicherheitsmechanismen verfügen.

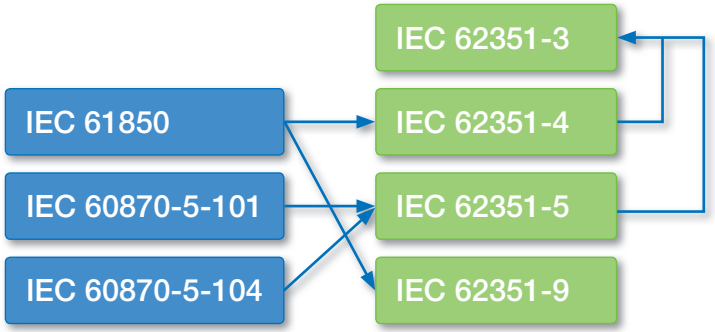

Abbildung 2: Normenverknüpfungen

Zusammenfassung

Durch den Einsatz verschiedener Normteile der IEC 62351 (siehe Abbildung 2) können die Protokolle IEC 60870-5-101/104 und IEC 61850-8-1 für die Prozesskommunikation zwischen Leit- und Fernwirktechnik so gesichert werden, dass sie den Anforderungen an das IT-Sicherheitsgesetz entsprechen. Für Diagnose- und Wartungsschnittstellen ist jedoch eine zusätzliche Sicherung (z. B. VPN) außerhalb der IEC 62351 notwendig.

Sichere Fernwartung am Beispiel des Fernzugriffs auf Störfallaufzeichnungen

Einführung rollenbasierte Zugriffssteuerung

Unternehmen geraten immer häufiger ins Visier von Cyberkriminellen, denn oft mangelt es an dem notwenigen Sicherheitsknowhow. Um die Komplexität von IT-Sicherheit zu beleuchten, fängt es schon bei der Fragestellung an, „Wer darf in einem IT-System auf welche Ressourcen wie zugreifen?“. Sicherheitsorientierte Unternehmen müssen sich darauf konzentrieren, Mitarbeitern genau die Berechtigungen zuzuweisen, die sie benötigen. Zu viele Berechtigungen können ein Konto zum leichten Angriffsziel machen. Wenn die Berechtigungen nicht ausreichen, können Mitarbeiter nicht effizient arbeiten.

Eines der primären Ziele von unternehmensweiten Rollen- und Berechtigungskonzepten ist eine elegante und effiziente Berechtigungssteuerung. Role-based Access Control (RBAC) oder rollenbasierte Zugriffssteuerung ist ein bewährtes Konzept in IT-Systemen, das von vielen (Betriebs-)Systemen zur Steuerung des Zugriffs auf die Systemressourcen genutzt wird. Bei einer rollenbasierten Modellierung werden die Berechtigungen zur Nutzung geschützter Komponente direkt an Rollen und damit an Aufgaben geknüpft. Das primäre Ziel der Berechtigungssystematik ist es einzelne Berechtigungen in größere Einheiten zusammen zu fassen, um sie damit schneller, übersichtlicher und eleganter zuordnen zu können. Statt Nutzern spezielle Zugriffsrechte zu gewähren, unterstützt RBAC das Prinzip der geringsten Rechte (Least Privilege).Dies ermöglicht die Zuordnung eines Subjekts (Nutzers) zu einer Rolle, die nur die zur Ausführung einer bestimmten Aufgabe notwendigen Rechte hat. So kann eine Organisation durch RBAC dedizierte Rechte festlegen und in bestimmten zuweisbaren Rollen zusammenfassen.

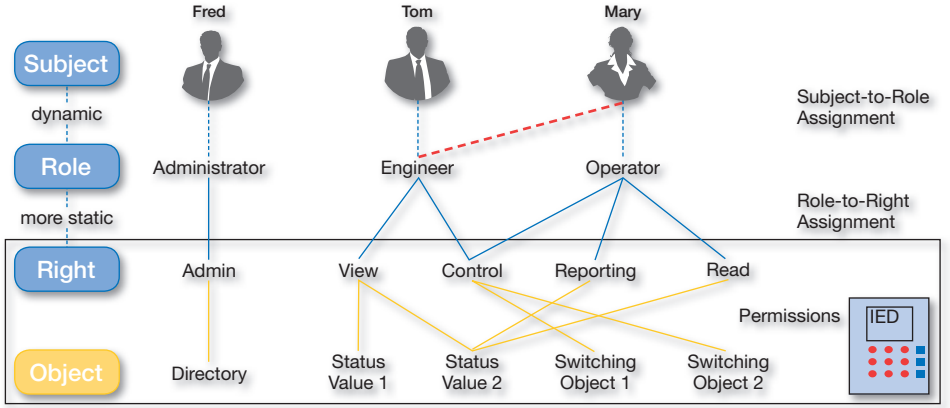

Abbildung 3 : allgemeine Konzept von RBAC mit der Zuordnung der Subjekt-Rolle-Rechte

Eine Rolle kann von 1 bis n Gruppenzugehörigkeiten gebunden sein. Mithilfe von RBAC kann eine präzise Zugriffsverwaltung ermöglicht werden; Aufgaben im Team können besser verteilt werden und Benutzern nur den Zugriff gewährt werden, den sie zur Ausführung ihrer Aufgaben benötigen. Somit ist es eine Verbesserung gegenüber dem weitverbreitet unsicheren Einzeladministrator-Gast-Modell. RBAC verringert Komplexität und Kosten der Sicherheitsadministration in Netzen mit einer großen Zahl von Subjekten.

Subjekte können Nutzer, Anwendungen oder Geräte sein. Die Grundidee besteht darin, Subjekten Rollen zuzuweisen, um die Zuweisung individueller Rechte zu vermeiden. In Abbildung 3 ist das allgemeine Konzept von RBAC mit der Zuordnung der Subjekt-Rolle-Rechte dargestellt. Dabei ist Tom die Rolle Ingenieur zugewiesen. In dieser Rolle kann Tom Objekte anzeigen und steuern. Objekte können zum Beispiel Statuswerte oder Schaltobjekte sein.

Wie in den Anforderungen des BDEW Whitepaper [9] und in der Norm IEC 62351-8 [10] behandelt, müssen bei Anwendung von Zugriffskontrolle und Nutzermanagement die dabei genutzte Infrastruktur und die zugehörigen Richtlinien ständig verwaltet werden.

IEC 62351-8: Role-based access control

Zentrales Thema im Teil 8 der IEC 62351 ist der rollenbasierte Zugangskontrollmechanismus und dessen Integration in der gesamten Domäne der Energieversorgung.

Der Schwerpunkt des Normdokuments liegt in der Entwicklung einer standardisierten Methode zur Definition und Entwicklung benutzerdefinierten Rollen, ihrer Rollen zu Recht Zuordnung und der entsprechenden Infrastrukturunterstützung, die zur Verwendung dieser benutzerdefinierten Rollen in Stromversorgungssystem erforderlich ist. Der Zugriff auf Objekte erfordert die Definition entsprechender Rechte und die Zuweisung dieser Rechte zu entsprechenden Rollen, die wiederum eine bestimmte Menge an Subjekten zusammenfassen.

Durch die IEC 62351 wird eine Ende-zu-Ende-Sicherheit für die Kommunikation von Komponenten innerhalb der Automatisierungsstrukturen von Energieversorgern realisiert. Als weitere Sicherheitsfunktion beschreibt die IEC 62351-8 einen sicheren Zugriff auf Datenobjekte mittels RBAC.

Einen Einstieg in die Norm erlangt man durch das PULL-Verfahren: Das Subjekt kontaktiert das Objekt, dessen Ressourcen genutzt werden sollen und sendet Informationen sowie die gewünschte Rolle für den Zugriff. Das Objekt greift auf die Quelle des Identity Providers (Ein Identity Provider IdP ist ein zentrales Anmeldesystem bei dem sich die Benutzer von Service-Provider-Diensten anmelden) zu und holt das entsprechende Access Token(entsprechende Zugriff). Nach erfolgreichen Authentifikation eines Benutzers erzeugt das Teilsystem ein fälschungssichere Datenstruktur, welches den Sicherheitskontext eines Prozess definiert. Voraussetzung ist ein bestehender Authentisierungs-

dienst durch IdP sowie eine gesicherte Verbindung zu diesem Dienst. Nach erfolgreicher Anmeldung wird ein Nutzer mit einem Access Token ausgestattet, welches alle Benutzer- und Gruppenzugehörigkeit eines Subjekts enthält. Wird ein Zugriff erfordert werden die Token Einträge mit einer Access Control List des Objekts verglichen und der Zugriff sowie die damit verbundenen Berechtigungen (lesen, schreiben, ändern) festgelegt.

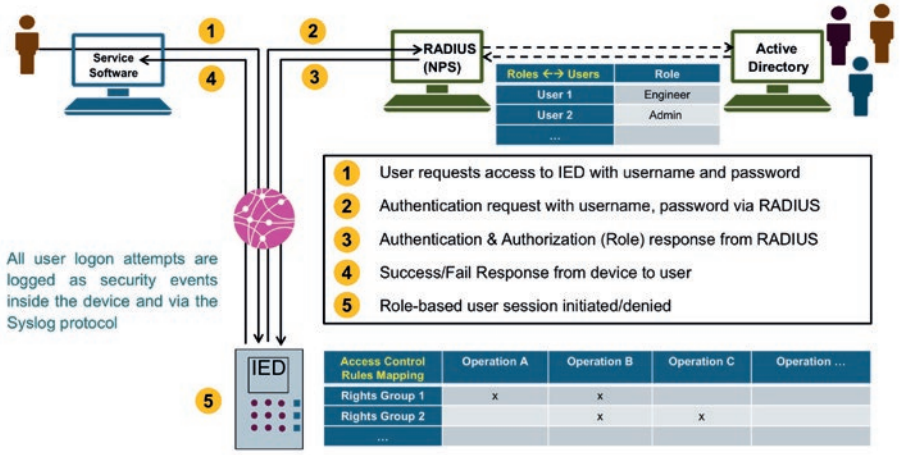

Abbildung 4: Konzept von RBAC nach dem PULL-Verfahren

In absehbare Zukunft wird erwartet, dass Betriebsmittel RBAC Informationen direkt lokal verifizieren zu können.

Hierbei muss sichergestellt werden, dass Skalierbarkeit und Interoperabilität herstellerübergreifend funktioniert. Dazu ist es notwendig, eine interoperable, skalierbare und sichere Lösung zur übergreifenden Anwendung von RBAC bei sekundären Betriebsmitteln verschiedener Hersteller über mehrere Unterstationen zu entwickeln. Letztlich sollte es Netzbetreibern möglich sein, RBAC wirksam und mit angemessenem Betriebskostenaufwand umzusetzen und zu betreiben. Die Realisierung dieser Methode ist über die Verwendung von digitalen Zertifikaten möglich, welches in der IEC 62351-8 als PUSH-Verfahren beschrieben ist.

Im PUSH-Modell holt das Subjekt das Access Token vom Identity Provider Dienst, bevor der Zugriff auf das Objekt erfolgt. Das Token muss allerdings vom Objekt validiert werden, darf nur eine begrenze Lebensdauer besitzen und muss ausreichend sichere kryptografische Verfahren zur Speicherung der Automatisierungsinformationen aufweisen.

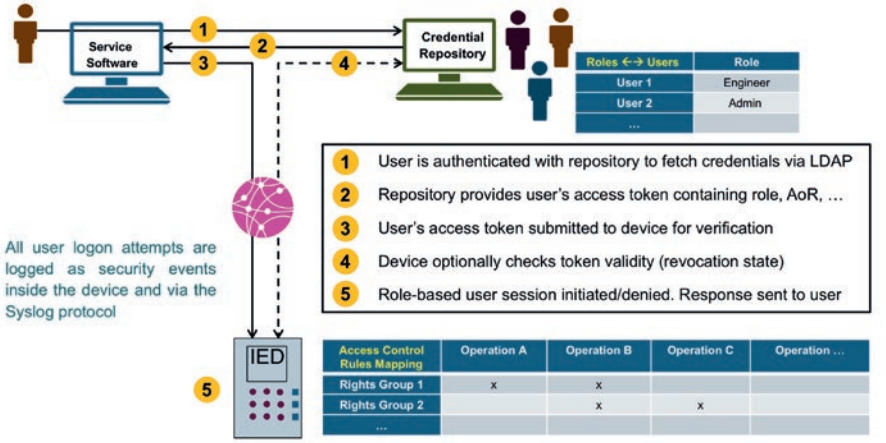

Abbildung 5: Konzept von RBAC nach dem PUSH-Verfahren

IEC 62351-10: Leitfaden für eine Sichere Systemarchitektur

Der Fernzugriff auf Störfallaufzeichnungen stellt grundsätzlich ein potentielles Risiko dar und eröffnet die Möglichkeiten eines unautorisierten Zugriffs.

Das BDEW-Whitepaper „Anforderungen an sichere Steuerungs-und Telekommunikationssysteme“ [10] fordert im Abschnitt „Bereich Netze / Kommunikation“ eine sichere Netzwerkarchitektur (Abschnitt 2.3.12). Insbesondere wird hier eine geeignete Segmentierung der Netzwerksegmente gefordert. Darüber hinaus wird im Abschnitt „Anforderungen an die Wartungsprozesse“ explizit auf sichere Fernwartungszugänge eingegangen.

Zur Gestaltung einer sicheren Netzwerkarchitektur (inklusive sichere Fernwartungszugänge) bietet die Norm IEC 62351-10 [11] Lösungen zur Realisierung einer sicheren Systemarchitektur, besonders im Bereich der Stationsautomatisierung. Dabei werden folgende Bereiche besonders beleuchtet:

- Netzwerk Segmentierung
- Strenge Authentifizierung
- Zugangskontrolle (RBAC)
- Daten- und Kommunikationssicherheit
- Sicherheitsüberwachung und vorbeugende Maßnahmen

Dabei sollte ein besonderer Fokus auf das Thema Netzwerk Segmentierung sein. Eine Netzwerksegmentierung beschreibt in der IT den Vorgang, dass Unternehmensnetz in einzelne Bereiche zu unterteilen, die nicht oder nur noch bedingt miteinander vernetzt sind. Dabei unterscheidet man zwischen vertikale- und horizontale Netzwerksegmentierung. Bei vertikaler Netzwerksegmentierung wird die dem System zugrundeliegende Netzwerkstruktur in Zonen mit verschiedenen Funktionen und unterschiedlichem Schutzbedarf aufgeteilt. Soweit es technisch möglich ist, werden diese Netzwerk-Zonen durch Firewalls, mit filternden Router oder Gateways getrennt. Weitere Kommunikation, mit weiteren Netzwerken hat ausschließlich über vom Auftraggeber zugelassenem Kommunikationsprotokoll zu erfolgen.

Bei der vertikalen Netzwerksegmentierung wird das zugrundeliegende Netzwerk in unabhängige Zonen (z.B. nach Standorten) aufgeteilt, wobei die Trennung der Zonen ebenfalls durch Firewalls, filternde Router oder Gateways erfolgen muss.

Dabei wird die Einrichtung einer demilitarisierten Zone (DMZ: geschütztes Computernetz für einen oder mehrere Computer, das sich neben zwei Computernetzen befindet) dringend empfohlen. Mit deren Einrichtung kann verhindert werden, dass ein Fernzugriff direkt auf die IEDs erfolgen kann. Es ist wichtig, dass ein Fernzugriff zwingend in der DMZ terminiert wird und kein direkter Durchgriff auf die IEDs erfolgen darf.

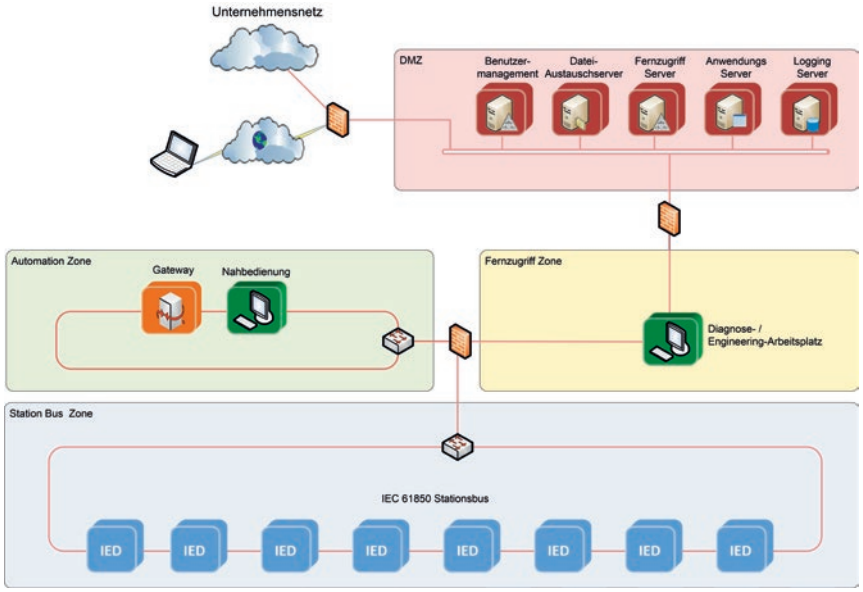

Abbildung 6: Sichere Systemarchitektur für den Fernzugriff

Mit der Einrichtung eines Engineering-Arbeitsplatzes wird eine Möglichkeit geschaffen, vollständig auf den Einsatz von Service-Laptops zu verzichten, da diese stets ein besonderes Risiko bezüglich der Sicherheit darstellen. Der hier dargestellte Weg eignet sich sowohl für Neuinstallation, als auch für bestehende Systeme. Es ist nicht zwingend erforderlich, die oben gezeigte Architektur vollständig zu implementieren. Es ist durchaus möglich nur einzelne Teile zu installieren.

Verfügbare Kommunikationsprotokolle

Erfolgt der entfernte Zugriff auf Störfallaufzeichnung über standardisierte Kommunikationsprotokolle wie IEC 61850 [12] oder IEC 60870-5-104 können für eine sichere Übertragung die IEC Norm 62351 Teil 4 und 5 angewendet werden. Beide Teile unterstützen eine beidseitige Authentifizierung der Kommunikationsteilnehmer auf Basis von X509 Zertifikaten (X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate). Beim Einsatz von IEC 61850 kann zusätzlich der Zugriff auf Diagnosedaten mittels der rollenbasierten Zugriffskontrolle (RBAC nach) IEC 62351-8 eingeschränkt werden. Somit wird sichergestellt, dass nur Zugriff auf Diagnosedaten besteht und keine Schalthandlungen ausgelöst werden können.

Zertifikatsmanagement im Kontext der Energieautomatisierung

Einführung und Motivation

In der Energieautomatisierung werden Protokollfamilien wie die IEC 61850 oder auch die IEC 60870-5 genutzt, um eine Kommunikation zwischen einzelnen Geräten einer Unterstation oder auch von einer Unterstation zu einer Zentrale zu realisieren. Unter anderem für diese Protokollfamilien wurden in der Normenreihe der IEC 62351 verschiedene Sicherheitsdienste definiert, die diese Kommunikation schützen, entweder direkt auf der Transportschicht oder aber auch integriert in der Applikationsschicht. Charakteristisch für beide Ansätze ist, dass die Identifikation und die Authentisierung der Gegenstelle über Zertifikate durchgeführt wird.

Zertifikate werden im Kontext asymmetrischer kryptographischer Verfahren (Public Key Verfahren) genutzt. Hierbei besteht das Schlüsselmaterial aus einem öffentlichen und einem privaten Schlüssel (siehe auch Begriffsklärung unten) die von den Kommunikationspartnern typischerweise im Kontext der Authentisierung und Sitzungsschlüsselaushandlung verwendet werden. Dies ist Gegensatz zu symmetrischen Verfahren, bei denen Kommunikationspartner einen gemeinsamen Schlüssel kennen müssen. Bei einer steigenden Zahl von Kommunikationsverbindungen, ist es damit aufwendiger ein System mit rein symmetrischen Schlüsseln, die zum Schutz der Kommunikationsverbindungen genutzt werden, zu konfigurieren und zu pflegen, wie in Abbildung 7 dargestellt.

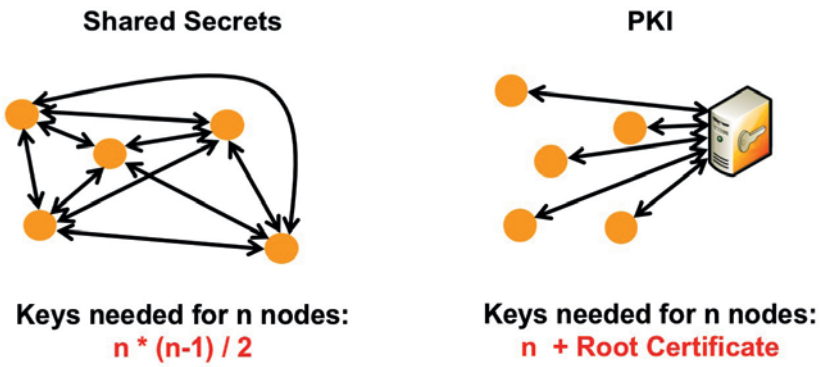

Abbildung 7: links symmetrisches verfahren, rechts asymmetrisches Verfahren

Um ein effizientes Management der Zertifikate, angepasst an die Bedürfnisse der Energieautomatisierung zu unterstützen, wurde daher in der IEC 62351-9 [14] das Thema Schlüsselmanagement für Energiemanagementsysteme standardisiert.

Generell können die Zertifikate Nutzern im Sinne einer Person (z.B. Servicetechniker) aber auch im Sinne eines Gerätes zugeordnet sein.

Begriffsklärung Zertifikate und Zertifikatsmanagement Infrastruktur

Zertifikate sind elektronische Ausweisdokumente und dienen der Bindung eines öffentlichen kryptographischen Schlüssels an einen Nutzer (Person oder Gerät). Wie eingangs erwähnt, werden diese typischerweise im Kontext Public Key Verfahren verwendet. Die Besonderheit dabei ist, dass zu jedem öffentlichen Schlüssel ein korrespondierender privater Schlüssel existiert, der entsprechend sicher aufbewahrt werden muss. Zertifikate werden von einer vertrauenswürdigen Stelle ausgegeben und haben eine beschränkte Laufzeit. Abbildung 8 zeigt einen Vergleich von Zertifikatstypen mit anderen, bekannten Ausweisformen.

Dabei existieren zwei Arten von Zertifikaten:

- Public Key Zertifikate (oftmals auch als ID-Zertifikat bezeichnet), bei denen ein öffentlicher Schlüssel an die Identität eines Nutzers gebunden wird. Sie sind vergleichbar mit einem Personalausweis. Zu dem öffentlichen Schlüssel existiert ein privater Schlüssel, der geheim gehalten werden muss. Mit diesem können z.B. digitale Signaturen erstellt werden, die mit Hilfe des Zertifikats überprüft werden können.

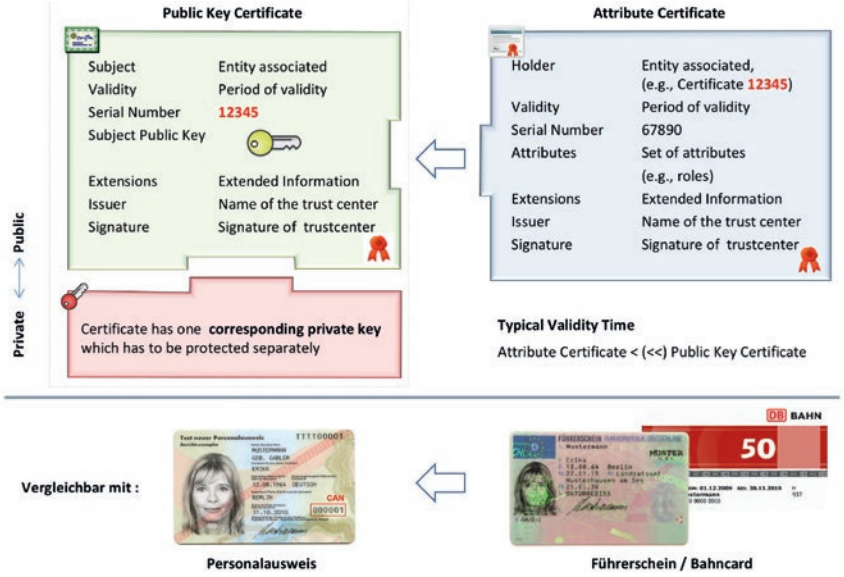

Abbildung 8: Vergleich von Zertifikatstypen mit anderen, bekannten Ausweisformen

- Attribut Zertifikate, bei denen ein bestimmtes Attribut, z.B. eine Rolleninformation an den Besitzer des Zertifikates gebunden werden. Hier gibt es keinen zugehörigen privaten Schlüssel. Sie haben eine kürzere Laufzeit, sind an ein Public Key Zertifikat gebunden und stellen somit eine temporäre Erweiterung dar. Als Vergleich kann z.B. ein Führerschein gesehen werden, das den Namen des Nutzers zur Referenzierung nutzt. Ein anderes Beispiel ist eine Bahncard.

IEC 62351-9 [14] definiert hier in erster Linie mit X.509 [15] das zu nutzende Format der Zertifikate, nicht jedoch die spezifischen Inhalte.

Um Zertifikate im Betrieb effektiv nutzen zu können, müssen sie entsprechend verwaltet werden. Im Folgenden wird auf Public Key Zertifikate fokussiert, da diese zur Identifikation und Authentisierung an verschiedenen Stellen eine entscheidende Rolle spielen. Attributzertifikate werden im Kontext der rollenbasierten Zugriffskontrolle näher beschrieben. Die Verwaltung der Zertifikate (siehe auch Abbildung 9) beinhaltet die

- Registrierung von Nutzern (Personen oder Geräte) bei einer Registrierungsstelle (Registration Authority oder RA) zur Beantragung von Zertifikaten
- Generierung von Schlüsselpaaren (bestehend aus öffentlichen und privaten Schlüssel), idealerweise auf dem Endgerät
- Beantragung eines Zertifikates basierend auf dem generierten Schlüsselmaterial durch den Nutzer (Enrollment)
- Generierung eines Zertifikates für einen autorisierten Nutzer in einer Zertifizierungsstelle (Certification Authority oder CA)
- Verteilmechanismen für erstellte Zertifikate in Zusammenhang mit der Beantragung (Distribution)
- Bereitstellung von Verzeichnisdiensten zum Abfragen von Zertifikatsinformationen
- Bereitstellung von Gültigkeitsinformationen, z.B. über einen LDAP Server, da auch während der eigentlichen Laufzeit eines Zertifikates dieses wiederrufen werden kann, z.B. wenn der dazugehörige private Schlüssel in falsche Hände gekommen ist (Revocation Information).

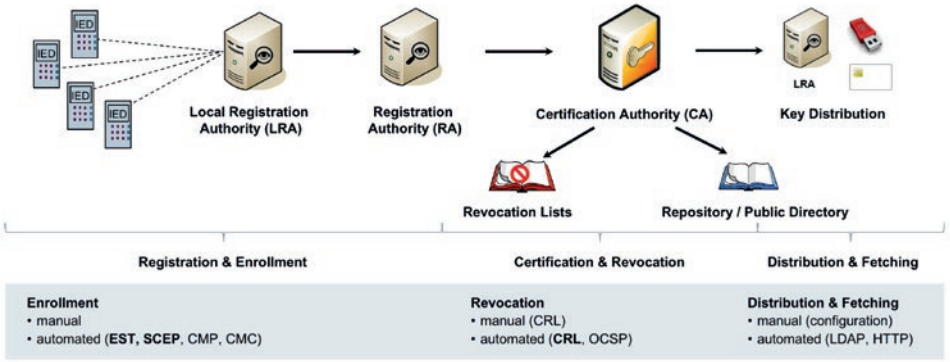

Abbildung 9: Verwaltung der Zertifikate

Speziell für das Thema Zertifikate für Geräte ist es sinnvoll ein weitestgehend automatisiertes Zertifikatsmanagement zu ermöglichen. Dazu werden im Standard IEC 62351-9 verschiedene schon existierende Protokolle beschrieben, die die Installation und Aktualisierung sowie Abfragen zur Gültigkeit von Zertifikaten ermöglichen.

Im Folgenden wird der Umgang mit diesen Protokollen erläutert. Dabei wird zwischen zwei verschiedenen Arten von Zertifikaten unterschieden die in den verschiedenen Phasen des Produktlebenszyklus eine Rolle spielen:

- Herstellerzertifikate, die während der Produktion eines Gerätes eingebracht werden. Diese Zertifikate enthalten in der Regel Daten wie den Hersteller, den Produktnamen und die Seriennummer, die auch auf dem Produkt Label stehen und das Gerät eindeutig bezeichnen. Diese Zertifikate können auch dazu genutzt werden, bei der Inbetriebnahme ein vereinfachtes Einbringen operativer Zertifikate zu unterstützen. Der Vorgang des Einbringens von einem Herstellerzertifikat während der Fertigung (Imprinting) kann mit der Ausstellung einer Geburtsurkunde verglichen werden. Herstellerzertifikate für Geräte haben eher eine lange Laufzeit.

- Operative Zertifikate, die während des Betriebs eines Gerätes genutzt werden. Diese Zertifikate haben eher eine kurze Laufzeit und müssen im laufenden Betrieb regelmäßig aktualisiert werden. Das erstmalige Verteilen dieser Zertifikate wird auch als Bootstrapping bezeichnet. Zum Absicherung des Bootstrapping kann das existierende Herstellerzertifikat für das Gerät genutzt werden.

Die Ausstellung und Verteilung dieser Zertifikate ist an bestimmte Prozesse des Austellers gebunden. Die Infrastruktur dazu wird als PKI – Public Key Infrastruktur – bezeichnet und ist in der Abbildung 9 dargestellt.

Im Folgenden wird der Prozess des Imprinting und des Bootstrapping beschrieben. Beides ist dafür gedacht potentiellen Anwendern einen Einstieg in das Zertifikatsmanagement zu geben und potentielle Schritte für eine Integration aufzuzeigen.

Ausstellung von Herstellergerätezertifikaten – Imprinting

Während der Produktion eines Geräts wird durch das Gerät ein Schlüsselpaar (öffentlicher und zugehöriger privater Schlüssel) generiert. Der öffentliche Schlüssel wird, ebenfalls als Teil der Produktion, mit gerätespezifischen Informationen (Gerätename, Identifier, etc.) als Zertifikat durch eine herstellerspezifische Zertifizierungsstelle signiert. Die Kommunikation zwischen dem Gerät und der Zertifizierungsstelle (RA/CA) wird herstellerspezifisch realisiert, kann jedoch auch Protokolle anwenden, die im späteren Betrieb für das Zertifikatsmanagement genutzt werden.

Die Abbildung 10 zeigt einen möglichen Aufbau für die Ausstellung von Zertifikaten durch einen Hersteller während der Produktion.

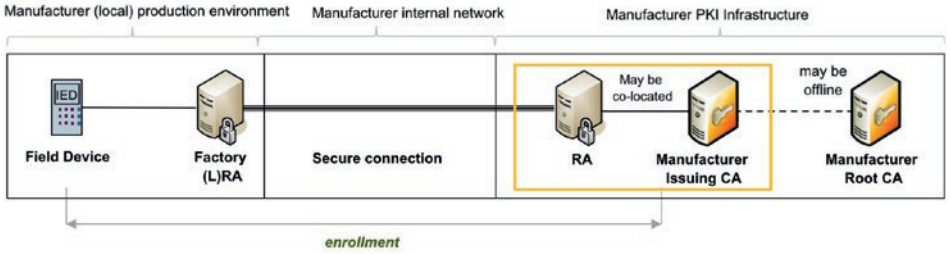

Abbildung 10: möglichen Aufbau für die Ausstellung von Herstellergerätezertifikaten – Imprinting

Ausstellung von operativen Zertifikaten – Bootstrapping

Die Norm IEC 62351-9 definiert für den Bereich Energieautomatisierung die Nutzung von zwei Protokollen für das Zertifikatsmanagement:

- Enrollment over Secure Transport – EST [16]: Ermöglicht das Management von RSA und ECDSA (Elliptic Curve Digital Signature Algorithm, asymmetrisches Kryptoverfahren) basierten Zertifikaten über eine gesicherte Verbindung (gesichert im Sinne einer Transportsicherung mittels TLS (Transport Layer Security)) Durch die Unterstützung von RSA und ECDSA basierten Zertifikaten, bietet dieses Protokoll eine hohe Flexibilität.

- Simple Certificate Enrollment Protocol – SCEP [17]: Ermöglicht das Management von RSA (Rivest, Shamir, Adleman, asymmetrisches Kryptoverfahren) basierten Zertifikaten z.B. über ein http Verbindungen. Das Protokoll schützt die eigentlichen Nachrichten in erster Linie gegen unbemerkte Veränderung.

Neben den genannten existieren weitere Möglichkeiten für Zertifikatsmanagement wie z.B. CMP (Certificate Management Protocol) bei Mobilfunknetzen.

IEC 62351-9 sieht vor, dass die Infrastruktur beim Betreiber beide Protokolle unterstützt, während die Feldgeräte die Wahl haben welches Protokoll implementiert wird. Im Folgenden wird von der Wahl EST als Protokoll für Zertifikatsmanagement ausgegangen.

Die Abbildung 11 zeigt den generellen technischen Ansatz mit dem Fokus auf der Kommunikation. Im Vergleich zur Darstellung beim Imprinting ist ersichtlich, dass der generelle Aufbau ähnlich ist.

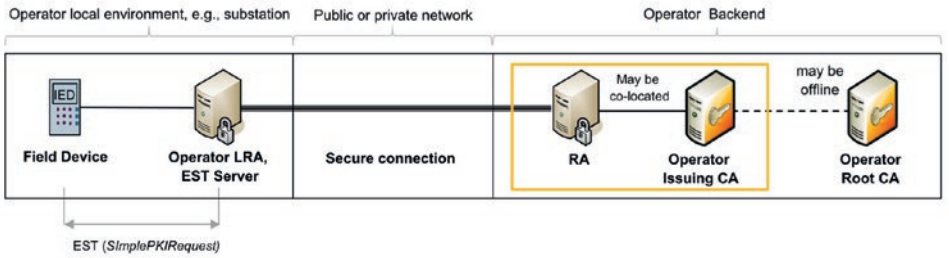

Abbildung 11: möglicher Aufbau für die Ausstellung von operativen Zertifikaten – Bootstrapping

Prozedural gibt es jedoch Unterschiede zwischen dem Imprinting und dem Bootstrapping eines Gerätes. Beim Imprinting befindet sich das Gerät im abgeschlossenen (internen) Teil der Kommunikationsinfrastruktur des Herstellers. Der Hersteller hat entsprechend seinem Entwicklungsprozess eine Anbindung an eine LRA realisiert, zu der nur autorisiertes Personal Zugang hat. Dies wird z.B. durch physikalisch abgetrennte Bereiche realisiert, die eine entsprechende Zugangskontrolle erfordern. Diese physikalische Sicherheit ist notwendig, um die Zertifizierungsanfragen aus einer geschützten Umgebung heraus als autorisiert zu betrachten.

Bei einem Betreiber kann diese Autorisierung durch eine explizierte Freischaltung eines Gerätes für eine Zertifizierungsanfrage erfolgen. Dazu ist ein Prozess notwendig, der das auf dem Gerät schon existierende Herstellerzertifikat sinnvollerweise nutzt. Dieser Prozess ist im Folgenden beispielhaft (und vereinfacht) dargestellt.

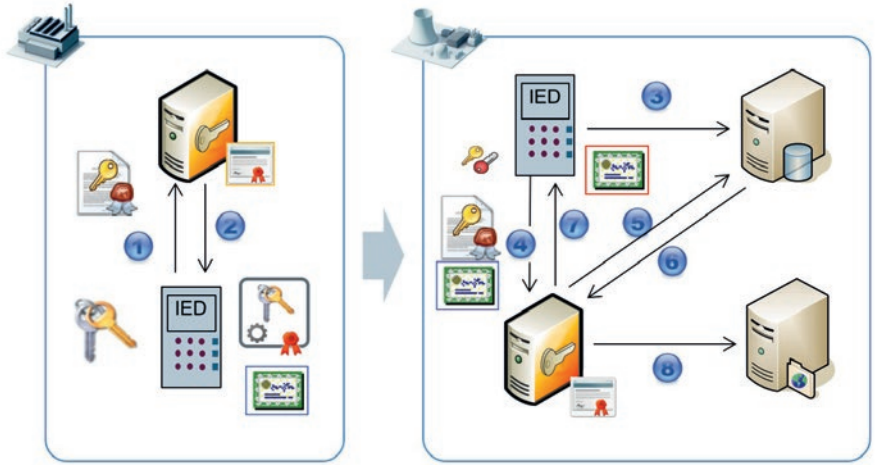

Abbildung 12: Prozess für explizierte Freischaltung eines Gerätes

Die linke Seite zeigt dabei den Prozess beim Hersteller, während die rechte Seite einen möglichen Prozess beim Betreiber darstellt.

Im Folgenden eine kurze Erläuterung der einzelnen Schritte auf Basis von EST:

1. Während der Herstellung wird vom Gerät in einem Produktionsschritt ein Schlüsselpaar generiert und eine Zertifizierungsanfrage für den öffentlichen Schlüssel an die herstellerspezifische PKI gestellt. Diese Zertifizierungsanfrage kann schon über das später im Feld genutzte Enrollment–Protokoll EST realisiert werden.

2. Die Hersteller-PKI erzeugt aus den Daten der Zertifikatsanfrage (öffentlicher Schlüssel, Seriennummer des Gerätes, Produkt- und Herstellername und ggf. weiteren Informationen) nach der Prüfung ein Zertifikat und liefert dieses an das Gerät zurück. Informationen zum Herstellergerätezertifikat können den Teil der Lieferpapiere des Gerätes sein oder können direkt abgefragt werden.

3. Nachdem der Betreiber ein Gerät erworben hat, werden die Gerätedaten inklusive der Geräteseriennummer des Zertifikates und der Informationen zum Aussteller des Hersteller (Root CA.) in ein Inventarverzeichnis eingetragen. Dies unterstützt den Schritt 5 im Folgenden.

4. Bei der Inbetriebnahme des Gerätes wird ein operatives Schlüsselpaar durch das Gerät erzeugt. Des Weiteren wird eine Zertifizierungsanfrage an die Betreiber PKI generiert. Zur Betreiber PKI wird ein sicherer Kanal als Teil von EST aufgebaut, bei dem sich das Gerät mit dem Herstellergerätezertifikat authentisiert. Über diesen sicheren Kanal schickt das Gerät die Zertifizierungsanfrage.

5. Die Betreiber PKI überprüft nun mittels des Inventarverzeichnisses und dem empfangenen Herstellerzertifikates des Gerätes, die Autorisierung zur Ausstellung eines operativen Zertifikats für dieses Gerät. Im Inventarverzeichnis kann ebenfalls geprüft werden, ob das Gerät einer spezifischen Anlage zugeordnet ist.

6. Prüfergebnis und ggf. weitere Informationen aus dem Inventarverzeichnis werden an die Betreiber PKI weitergeleitet.

7. Die Betreiber PKI generiert bei vorhandener Autorisierung ein operatives Zertifikat (mit entsprechenden betreiberspezifischen Daten, wie z.B. den Namen des Betreibers oder auch der zugeordneten Anlage) und übermittelt dies zurück an das Gerät.

8. Die Betreiber PKI kann nun das Zertifikat bei einem (internen) Verzeichnisdienst ablegen.

9. Optional kann auch ein externer Verzeichnisdienst über die Ausstellung eines operativen Zertifikates informiert werden. Damit kann z.B. festgestellt werden, ob ein Herstellerzertifikat zum mehrfachen Bootstrappen bei einem unterschiedlichen Betreiber genutzt wird.

10. Das Bootstrappen des Gerätes im Betreibernetz kann in einem separaten Netzwerk oder aber im produktiven Netzwerk realisiert werden. Die Umsetzung hängt vom jeweiligen Betreiber ab.

11. Die operativen Zertifikate selbst unterliegen einem Lebenszyklus und müssen regelmäßig aktualisiert werden. Auch hierfür kann EST als Zertifikatsmanagementprotokoll genutzt werden.

Literaturverzeichnis

[1] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), vom 17. Juli 2015, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015

[2] IEC 60870-5-104:2016, Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standardtransport profiles

[3] IEC 60870-5-101:2003, Telecontrol equipment and systems – Part 5-101: Transmissionprotocols – Companion standard for basic telecontrol tasks

[4] IEC 61850-8-1:2011, Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

[5] IEC 62351-3:2014, Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

[6] IEC/TS 62351-5, Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives

[7] IEC/TS 62351-4:2007, Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS

[8] IEC 62351-9:2017, Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment

[9] Whitepaper, Anforderungen an sichere Steuerungs-und Telekommunikationssysteme, Überarbeitete Version 1.1, 03/2015BDEW Bundesverband der Energie-und Wasserwirtschaft e.V.

[10] IEC 62351-8:2011, Power systems management and associated information exchange –Data and communications security – Part 8: Role-based access control

[11] IEC/TR 62351-10:2012, Power systems management and associated information exchange –Data and communications security –Part 10: Security architecture guidelines, Edition 1.0 2012-10

[12] IEC 61850, Communication networks and systems for power utility automation

[13] ISO/IEC 9594-8:2017, Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks

[14] IEC 62351-9:2017, Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment, Edition 1.0

[15] x.509 (10/2016), Information technology – Open Systems Interconnection – The Directory: Public- key and attribute certificate frameworks

[16] Enrollment over Secure Transport – EST, RFC 7030, https://tools.ietf.org/html/rfc7030, 10-2013

[17] Simple Certificate Enrollment Protocol – SCEP, draft-nourse-scep-23, https://tools.ietf.org/html/draft-nourse-scep-23, 09-2011

Herausgeber:

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.

als Träger der

DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
im DIN und VDE

Andreas Harner
Stresemannallee 15
60596 Frankfurt am Main
Tel. +49 69 6308-392
andreas.harner@vde.com
www.dke.com

DKE
VDE DIN