

Schutz der Verbrauchsdatenübertragung vor Manipulation

Die Übertragung von Verbrauchsdaten über die Telekommunikationsnetze oder per Funk ist im Facility Management bereits Alltag. Doch je mehr sie sich durchsetzt (etwa bei der Zählerfernauslese), desto größer wird die Gefahr der Manipulation. Der Einsatz so genannter Public Key Infrastrukturen (PKI) kann hier Abhilfe schaffen.

Die Zeiten, in denen eine Person jedes Jahr zur Ablesung der Zähler ins Haus kommt, sind vielerorts bereits lange vorbei. Denn die Zählerfernauslese (ZFA) des Strom-, Gas-, Wasser- oder Fernwärmeverbrauchs setzt sich immer mehr durch. Die neueste Zählergeneration nutzt dabei kostengünstig das offene Internet, um die erhobenen Messwerte an einen zentralen Server beim Energieversorger zu übermitteln. Das Risiko dabei: Mit dem Einsatz der Kommunikationswege auf Basis des Internet-Protokolls (IP) steigt auch die Manipulationsgefahr (beispielsweise durch Hacker- oder Virenangriffe). Da die per Fernzugriff ausgelesenen Daten aber in der Regel auch für die Abrechnung genutzt werden, ist es für die Beteiligten von entscheidender Bedeutung, dass der Datenursprung nachvollziehbar ist und die Daten selbst unverfälscht sind.

Vertraulichkeit, Integrität, Verfügbarkeit

Diese als CIA-Dreieck (Confidentiality, Integrity, Availability) bekannten Ziele der Datensicherheit gelten heute nicht nur für das E-Business, das Online-Banking oder die E-Mail-Kommunikation. Auch im Facility Management zählen sie zu den Grundanforderungen an geschäftliche Transaktionen. Im Gegensatz zu vielen Bereichen der Kommunikationstechnologie ist Sicherheit hier aber nicht allein durch technische Interoperabilität gekennzeichnet. Das notwendige Vertrauen der beteiligten Unternehmen entsteht erst durch eine Kombination aus sicherer Technologie und sicheren organisatorischen Prozessen. Das dazu nötige Sicherheitsbewusstsein kann nur in einer gemeinsamen Anstrengung erreicht werden.

Der Schutz der Vertraulichkeit soll den Zugriff nur für Berechtigte ermöglichen. Der Integritätsschutz hat das Ziel, die Veränderung von Daten zu verhindern. Verfügbarkeit in diesem Kontext ist die Sicherstellung

eines zuverlässigen und zeitnahen Zugriffs zu IT-Diensten für autorisierte Benutzer. Diese zumeist konträren Anforderungen müssen in ein sinnvolles Gleichgewicht gebracht werden und bei der Einführung einer Public Key Infrastructure (PKI) berücksichtigt werden. Darunter wird ein komplexes System verstanden, das es ermöglicht, zur Absicherung der Kommunikation digitale Zertifikate auszustellen, zu verteilen und zu prüfen.

Zwei Schlüssel für die Sicherheit

Das Grundprinzip der digitalen Zertifikate beruht auf dem Einsatz eines asymmetrischen Verschlüsselungsverfahrens, bei dem nach bestimmten mathematischen Verfahren zwei zueinander gehörige Schlüssel berechnet werden. Der eine wird veröffentlicht und den Kommunikationspartnern zur Verfügung gestellt, den zweiten Schlüssel hält der Besitzer

geheim. Ähnlich wie der Personalausweis im realen Leben, erlaubt das digitale Zertifikat die zweifelsfreie Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person oder Organisation. Dazu werden sie von einer Zertifizierungsstelle (Certificate Authority oder CA) – wie etwa der Bundesnetzagentur – beglaubigt, die ähnlich wie das Einwohnermeldeamt beim Personalausweis dazu berechtigt ist. Sie betreibt außerdem u. a. ein Verzeichnis, das die automatisierte Überprüfung von Zertifikaten in Echtzeit ermöglicht, sowie eine Sperrliste für ungültige Schlüssel.

Die Zertifikate enthalten neben dem eigentlichen „Schlüssel“ noch weitere Zusatzinformationen, die zur Authentifizierung sowie zur Ver- und Entschlüsselung vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Im Facility Management-Umfeld stellen die PKI-basierten Methoden sicher, dass die technischen Verfahren nicht



durch Angriffe manipuliert werden können, indem sie die Authentizität der beteiligten Systeme gewährleisten. Darüber hinaus lässt sich das Verfahren auch zur individuellen Verschlüsselung von Daten einsetzen, die dann nur von einem ganz bestimmten Empfänger (im Fall der Zählerfernauslese beispielsweise vom Energieversorger) wieder entschlüsselt werden können.

Bevor eine solche PKI im Facility Management-Umfeld allerdings eingesetzt werden kann, sind einige besondere Vorkehrungen zu treffen, damit das Verfahren höchstmögliche Datensicherheit gewährleistet. So ist es in der Regel an bereits existierende Prozesse gebunden, die nicht verändert werden dürfen.

Die Zähler haben ein feststehendes Hardware-Design, das meist nicht einfach verändert oder erweitert werden kann.

Deshalb muss eine Möglichkeit gefunden werden, das Schlüsselmaterial sicher und unveränderbar auf der vorhandenen Hardware zu speichern.

Denn wenn der private Schlüssel missbräuchlich verwendet werden kann (etwa weil eine Vielzahl von Mitarbeitern Zugriff darauf hat), ist das gesamte Verfahren nutzlos. Viele Unternehmen entscheiden sich deswegen für den Einsatz eines externen Speichermediums wie beispielsweise eine Smartcard oder ein HSM (Hardware Security Module). Auf diese Weise können die entsprechenden Zugangsdaten ausschließlich auf dieser Karte generiert bzw. gespeichert werden. Der Nutzer authentifiziert sich mit Hilfe einer PIN. Wird diese PIN mehrfach falsch eingegeben, wird nicht nur der Zugriff verweigert, sondern auch das Schlüsselmaterial selbst kann nicht mehr verwendet werden.

SELMA und die Ziele

An SELMA beteiligt sind Hersteller von Zählergeräten, industrielle Anwender aus der Energiewirtschaft, die Physikalische Bundesanstalt als oberste Eichinstanz, das BSI sowie eine rechtlich orientierte wissenschaftliche Begleitung und eine sicherheitstechnisch orientierte, wissenschaftliche Moderation des Prozesses.

SELMA – so das Ziel – soll ein PKI-basiertes Sicherheitskonzept liefern, das auf die Geschäftsprozesse rund um die Energieverbrauchs-messung abgestimmt ist. Die Signatur der Messdaten ermöglicht an allen Stellen des Prozesses (bis hin zur Rechnungsstellung) eine vereinfachte Validierung der gemessenen Verbrauchsdaten. Damit können Rückfragen und Nacherfassungen weitgehend vermieden werden. Auch die heute noch eichrechtlich geforderte Anzeige der Messdaten am Zähler könnte damit entfallen.

Zudem will SELMA mittelfristig die Möglichkeit schaffen, durch Herunterladen von digital signierten und zertifizierten Software-Paketen den Unterhaltsprozess für die Messgeräte zu automatisieren und damit die Betriebskosten beträchtlich zu senken.

Sollen dagegen so genannte Soft Token verwendet werden (etwa weil das Hardware-Design bereits abgeschlossen ist oder Standardkomponenten eingesetzt werden sollen), müssen geeignete Maß-

nahmen zur Sicherung des Schlüsselmaterials implementiert werden.

Darüber hinaus spielen aber auch die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine große Rolle. So ist bereits in der Design-Phase eines Geräts die vorausschauende Integration geeigneter Algorithmen nötig, damit nicht während des Produktlebenszyklus ein Sicherheitsleck identifiziert wird. Deswegen sind auch geeignete und im Zweifelsfall höhere Schlüssellängen zu wählen. Marktüblich sind derzeit 2048 Bit RSA-Keys.

Branchenübergreifende Lösung gefragt

Hat ein Energieversorger bereits eine PKI realisiert (z. B. zur Absicherung seiner elektronischen Geschäftsprozesse oder E-Mail-Kommunikation), will er in der Regel nicht noch eine zusätzliche Infrastruktur zur ZFA aufbauen. Deshalb ist eine weitere Bedingung, dass es möglich sein muss, bereits existierende PKI-Systeme an die neue Lösung anzubinden. Dabei ist auch zu beachten, dass derzeit im Rahmen des Projekts „Sicherer elektronischer Messdatenaustausch“ (SELMA) an einer übergreifenden PKI-Lösung gearbeitet wird. Es wurde als Förderprojekt im Rahmen der VERNET-Initiative des Bundes vergeben, mit der die Entwicklung von „sicheren und verlässlichen Transaktionen in offenen Kommunikationsnetzen“ unterstützt werden soll.



Der Autor

Marcus Hanke,
Consultant Trusted Identity and Smartcards
bei Siemens Enterprise Communications,
Nürnberg