ew
Magazin für die Energiewirtschaft
www.ew-online.de
Sonderdruck (Nr. 7266) aus 2015 (Jg. 114), Heft 2, S. 85-88

Sichere Datenverbindung

Sicherheitsprozesse der Gateway-administration erfolgreich getestet

von Dr. Werner Kremer und Jürgen Ruf

mtG media transfer AG

Sonderdruck im Auftrag von mtG

Sichere Datenverbindung

Sicherheitsprozesse der Gateway-administration erfolgreich getestet

Mit der Technischen Richtlinie TR-03109 des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind die Prozesse und Sicherheitsanforderungen für das künftige Smart Metering in Deutschland festgelegt. Die technologische Umsetzung der Richtlinie stellt hohe Anforderungen an das Verständnis zur Zusammenarbeit der verschiedenen Komponenten im System, an die Einordnung der Abläufe in die heutigen Marktrollen und an die entstehenden Schnittstellen zwischen den Marktteilnehmern. Im Fokus stehen in diesem Aufsatz die komplexen sicherheitsrelevanten Abläufe. Die darauf aufbauenden, rein administrativen Prozesse sind vergleichsweise einfach zu beherrschen.

Die Richtlinie TR-03109 des BSI stellt im internationalen Vergleich die vermutlich höchsten Anforderungen an Datenschutz und Datensicherheit für Smart Metering. Sie regelt auch, wie berechtigte externe Marktteilnehmer (EMT) unter Einhaltung des hohen Sicherheitsniveaus auf die intelligenten Messsysteme zugreifen können.

Mit der Beschreibung der verschiedenen Tarifanwendungsfälle (TAF) ist auch geregelt, wie die Messsysteme sowohl zur Übertragung abrechnungsrelevanter Werte als auch zu netzdienlichen Zwecken eingesetzt werden. Dabei werden anonymisierte Netzzustandsdaten wie Strom-, Spannungs- und Phasenwerte gesendet. Auf Basis dieser Daten steuern Energieversorger Erzeugungsanlagen und Verbraucher. Dies wird ebenfalls auf der gleichen, sicheren Infrastruktur stattfinden.

Labortests

Im MTG-Labor wurden deshalb im Auftrag der Deutschen Telekom AG die sicherheitskritischen Abläufe über alle eingebundenen Komponenten vollständig implementiert, integriert und getestet. Sie bilden die Grundlage für das sichere Abwickeln der administrativen Geschäftsprozesse.

In der Komponente Smart-Meter-Gateway (SMGW) ist als Sicherheitselement das Security-Modul eingebaut, das als dedizierte Hardwarekomponente bei Auslieferung die Gütesiegelzertifikate und nach der Inbetriebnahme die Schlüssel- und Wirkzertifikate enthält. Beim Installationsprozess wird die eindeutige und nicht mehr zu ändernde Verbindung der Komponenten hergestellt. In *Bild 1* entspricht dies der Verknüpfung des Smart-Meter-Gateways mit dem Haushaltszähler und dem Wechselrichter der Photovoltaikanlage.

Das Security-Modul des Gateways wird mit einem von der Telekom entwickelten Betriebssystem für sicherheitsrelevante Funktionen betrieben. Das Gateway enthält die Kommunikationskomponente zur Datenübertragung – bevorzugt über Mobilfunk oder Festnetz. Vor der Datenübertragung verschlüsselt und signiert das Smart-Meter-Gateway die Dateninhalte

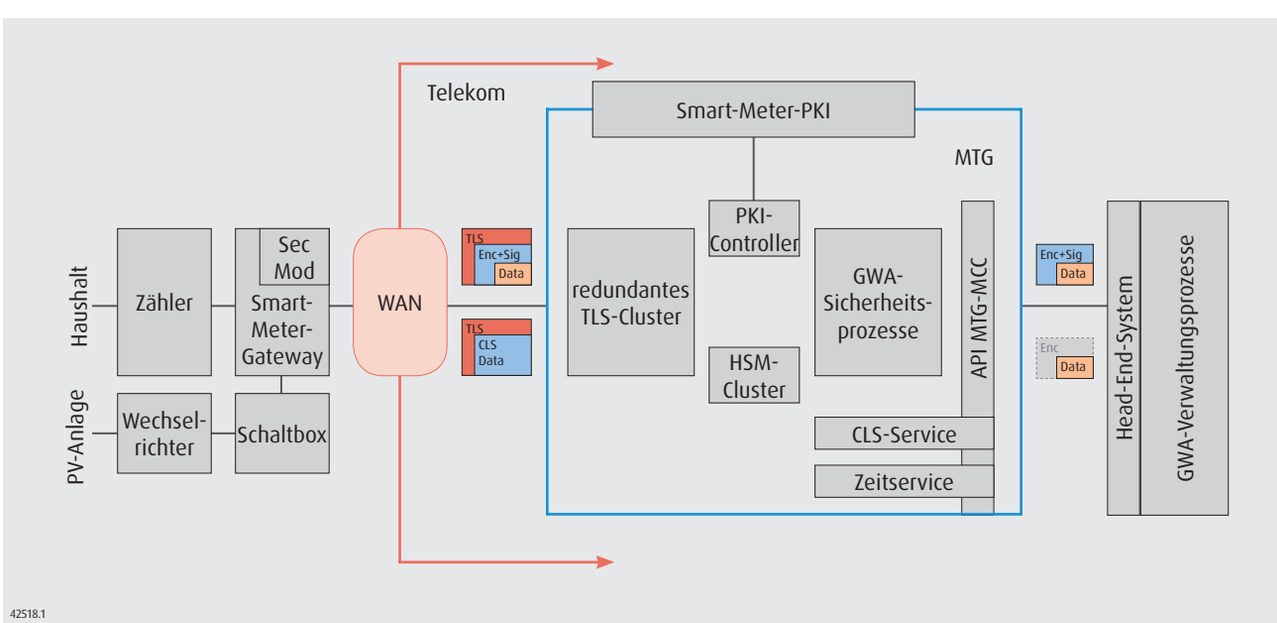

Bild 1. Komponenten für die sicherheitsrelevanten Abläufe im Smart Metering

und sendet diese zusätzlich verschlüsselt über den Transport-Layer-Security-Kanal (TLS-Kanal). Empfangen werden die Daten im redundant ausgelegten TLS-Cluster, das einen von der Media Transfer AG (MTG) entwickelten Load Balancer hat. Dieser sorgt für eine skalierende und gleichmäßige Verteilung der Lasten auf die Kommunikationskanäle.

Es können mehrere tausend TLS-Kanäle gleichzeitig offen gehalten werden. Erst damit wird ein schneller und direkter Datenaustausch möglich, ohne dass die Verbindung erst aufgebaut werden muss. Dies ist für zeitkritische Funktionen entscheidend, wie dem Schalten der angeschlossenen PV-Anlage über die Funktion des »Controlable Local Service (CLS)«[1].

Das als dedizierte Hardwarekomponente ausgeprägte Cluster des Hardware-Security-Moduls (HSM) enthält die entsprechenden Schlüssel und Zertifikate, um die Daten des TLS-Kanals wieder zu entschlüsseln und die Signaturen auf Echtheit zu prüfen. Sofern vom Datenempfänger gefordert, können auch die Dateninhalte selbst entschlüsselt werden.

Der Public-Key-Infrastructure-Controller (PKI-Controller) übernimmt das Zertifikatsmanagement und bildet die Schnittstelle zur Smart-Meter-PKI. Diese PKI betreibt die Telekom als Dienstleistung, die von allen Gatewayherstellern sowie -administratoren genutzt werden kann. Sie basiert auf der Root Policy, die den Zugang zu den Gütesiegelzertifikaten für die Gatewayhersteller mit den sicherheitstechnischen Prozessen regelt.

Die Komponente der Gatewayadministratorsicherheitsprozesse enthält die von MTG entwickelten Abläufe zum Management der Sicherheitsprozesse und -funktionen wie Ent- und Verschlüsselung. Darüber hinaus befinden sich hier die über Webservices ausgeprägten Schnittstellen zum Head-End-System, bei dem die nachgelagerten Verwaltungsprozesse der Gatewayadministration nach TR-03109 stattfinden. Der Crypto-Controller enthält eine Schnittstelle zum externen Zeitserver, der entsprechend der TR-03109 die Zeit korrekt synchronisiert.

Technischer Aufbau

Für die Entwicklung und die Integrationstests wurden die in *Tafel 1* dargestellten Komponenten eingesetzt. Aktuell werden die Prozesse zur Ansteuerung der CLS-Kanäle getestet. Die Ergebnisse stehen im Februar 2015 zur Verfügung.

[1] vgl. TR-03109-1 unter anderem Punkt 3.4.2.3

Komponenten

Komponente	Modul	Version/Quelle
Smart-Meter-Gateway	Betriebssystem-Security-Module	T-Systems
	Smart-Meter-Gateway	Dr. Neuhaus 1.1.1180, Betriebssystem SMGW DNT8209-13
MTG-Crypto-Controller	PKI-Controller, TLS-Cluster, GWA-Sicherheitsprozesse, HSM-HA-Cluster	MTG-CC Version 1.0
Hardware-Security-Module	HSM	Utimaco
Smart-Meter-PKI	Public-Key-Infrastructure	T-Systems, MTG
Zeitserver	extern	Telekom
GWA-Verwaltungsprozesse	GWA-Emulator	MTG Version 1.0

Tafel 1. Eingesetzte Komponenten für die Entwicklung und die Integrationstests

Sicherheitsprozesse der TR-03109

Die TR-03109 beschreibt die Rahmenbedingungen für die Implementierung der Vorgaben, ohne sie jedoch zu spezifizieren. Die Implementierung der kryptografischen Vorgaben erfordert deshalb langjährige Praxiserfahrung, um die komplexen Prozesse so umzusetzen, dass sie vom Gatewayadministrator (GWA) und EMT schnell und einfach konfiguriert und bedient werden können.

In die Integrationsumgebung wurden die in *Tafel 2* dargestellten Funktionen implementiert. Sie umfassen TR-relevante Vorgaben sowie darüber hinausgehende Management- und Administrationsfunktionen.

Messaufbau und Testergebnisse

Hinter den beschriebenen Funktionen stehen umfangreiche einzelne Methoden, die mit allen dazugehörigen Fällen getestet werden mussten. Der für die Testreihe entwickelte GWA-Emulator simuliert hierbei sämtliche Verwaltungsprozesse des GWA. Der Testtreiber ruft entsprechende Funktionen in der MTG-Crypto-Controller-API auf und kontrolliert deren Korrektheit und Performance (*Bild 2*).

Über den Test der einzelnen API-Methoden hinaus wurden mit einem GWA-Emulator die Interaktionen zwischen den Komponenten überprüft. Eine auf den ersten Blick einfach erscheinende Funktion ist beispielsweise das Anlegen eines GWA-Mandanten. Dahinter stehen jedoch sehr komplexe Funktionen und Arbeitsschritte.

Im ersten Schritt werden in diesem Beispiel die Datenstrukturen für den GWA angelegt. Das HSM- und TLS-Cluster sowie deren Kommunikationswege müssen ebenfalls konfiguriert werden, um später Inhaltsdaten austauschen zu können.

Im zweiten Schritt werden die privaten und öffentlichen Schlüsselpaare im HSM-Cluster erzeugt. Die privaten Schlüssel werden dabei im HSM sicher gespeichert. Danach wird die Verbindung zur Smart-Metering-PKI aufgebaut, um die GWA-Zertifikate zu erzeugen. Die Zertifikate werden von der Smart-Metering-PKI ausgestellt und im PKI-Controller gespeichert.

Im dritten Schritt werden Datenpakete per TLS mit dem SMGW ausgetauscht. Bei den empfangenen Inhaltsdatenpaketen wird die Signatur mit dem öffentlichen Schlüssel der SMGW überprüft und die Datenpaketinhalte mit dem privaten Schlüssel des GWA auf dem HSM entschlüsselt.

Funktionen

Konfigurationsmanagement	GWA-Betrieb	EMT-Betrieb
▪ Systemadministration: Plattformverwaltung (HSM, Load Balancer) ▪ Mandantenverwaltung: GWA/externe Marktteilnehmer ▪ Entitäten: SMGW, CLS-Verwaltung, Zertifikatsüberwachung	▪ Administratorendienstleistungen ▪ Administratorenmanagement ▪ Wake-up-Paket-Versand (siehe TR-03109-1)	▪ Datenempfang (Inforeport) ▪ CLS-Kanal

Tafel 2. In die Integrationsumgebung sind die dargestellten Funktionen implementiert.

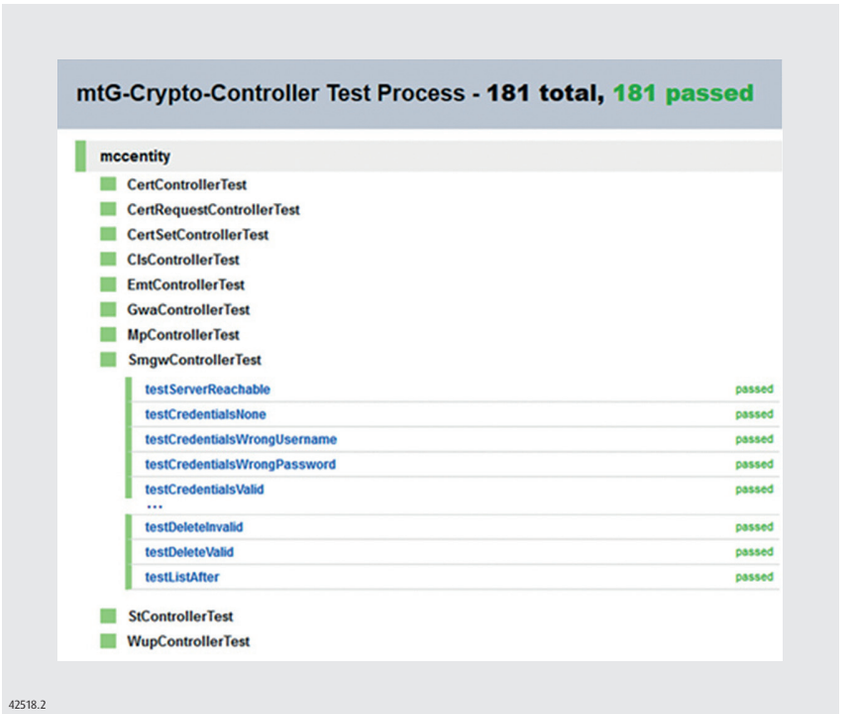

Bild 2. Beispiel – Testergebnisse ausgewählter Methoden: Einzelansicht für SMGW-Test

Die Tests müssen nach jedem Entwicklungsschritt automatisch durchlaufen und bestanden werden. Nur so ist sichergestellt, dass das System nach jedem Entwicklungsschritt weiterhin interoperabel mit allen Komponenten ist und die Software eine hohe Qualität hat.

Im Rahmen der Lasttests wurde je TLS-Server bestätigt, dass abhängig von der eingesetzten Hardware bis zu 15 000 TLS-Verbindungen parallel aufgebaut und gehalten werden können. Für eine größere Zahl von TLS-Verbindungen wurde die eingesetzte Hardware in einem Cluster skaliert. Das Testen mit realen Hardware-Security-Modulen in Verbindung mit einem SMGW ist eine besondere Herausforderung: Bei fehlerhafter Bedienung und Konfiguration bestand beim Testen immer die Gefahr eines Totalausfalls des SMGW. Die Tests wurden daher nach einem vorbereiteten Plan durchgeführt und die Interoperabilität der Hardware bestätigt.

Zusammenfassung und Ausblick

Im Labor ist es gelungen, das Zusammenspiel der Komponenten zu testen, die gemäß der TR-03109 die sicherheitsrelevanten Abläufe betreffen. Die Herausforderung bestand unter anderem darin, das Zusammenspiel der Prozesse zu verstehen und so umzusetzen, dass sie von den rein administrativen Prozessen architektonisch getrennt werden. Gleichzeitig war das System skalierbar und mit hoher Ausfallsicherheit aufzubauen, so dass es beim Smart-Meter-Rollout dynamisch mitwachsen kann.

Durch den Betrieb dieses Systems im Trust-Center der Telekom werden nicht nur diese Skaleneffekte genutzt, sondern auch die Anforderungen des IT-Grundschutzes zum sicheren Betrieb der Anwendung erfüllt.

Es ist gelungen, das System so aufzubauen, dass echtzeitnahe Anwendungen wie das Schalten von Photovoltaikanlagen und das Einspeisemanagement aufgrund der Aufrechterhaltung der TLS-Kanäle möglich sind. Mit dem Smart-Meter-Rollout wird dadurch nicht nur eine hochsichere Infrastruktur für die abrechnungsrelevante Zählerauslesung geschaffen, sondern auch das Einspeisemanagement und weitere netzdienliche Funktionen auf Basis der TR-03109 ermöglicht.

Dr. **Werner Kremer**, Senior Portfolio Manager Smart Metering und Grid, T-Systems, Bonn

Jürgen Ruf, Vorstandsvorsitzender, Media Transfer AG, Darmstadt

>> werner.kremer@t-systems.com
jruf@mtg.de

>> www.t-systems.de
www.mtg.de

42518