IT-Sicherheit von OCIT-Systemen

Einführung

Ein wichtiger Teil der Investitions- und Zukunftssicherung von Systemen der Straßenverkehrstechnik ist die einfache, sichere und wirtschaftliche Vernetzung ihrer Komponenten. Die Standardisierung von Schnittstellen liegt damit sowohl im Interesse der Auftragnehmer als auch der Hersteller solcher Systeme oder Komponenten.

Die ODG (OCIT Developer Group) standardisiert unter der Markenbezeichnung OCIT® Schnittstellen für verkehrstechnische Systeme. Ziel ist es, in solchen Systemen Komponenten verschiedener Hersteller zu vernetzen. Die Standardisierung umfasst im Wesentlichen die Kommunikationsprotokolle und die Daten der Schnittstellen.

OCIT Systeme lassen sich bereits heute so in die vorhandene Infrastruktur einbetten, dass aktuelle IT-Sicherheitsrichtlinien erfüllt werden. Der aktuelle Stand des OCIT-Systems legt damit die Grundlage für zukünftige Anforderungen in der IT-Sicherheit. Der Investitions- und Zukunftssicherheit wird insbesondere dadurch Rechnung getragen, dass die IT Sicherheit stets ein Kriterium für die Neu- und Weiterentwicklung der Schnittstellen ist.

Die Schnittstellenbereiche von OCIT

OCIT standardisiert Schnittstellen für die Bereiche „Outstations“ und „Instations“. Instations umfasst Schnittstellen zur Vernetzung von zentralen Einrichtungen. Da diese zentralen Einrichtungen für gewöhnlich in abgesicherten Netzwerkumgebungen eingebunden sind, wird der Bereich Instations hier nicht weiter betrachtet. OCIT-Outstations (kurz: OCIT-O) standardisiert im Allgemeinen eine Schnittstelle zwischen zentralen Einrichtungen und Feldgeräten. OCIT-O bietet die Möglichkeit verschiedenartige Feldgeräte der Straßenverkehrstechnik einzubinden. Aktuell ist ausschließlich das „Lichtsignalsteuergerät“ als Feldgerät definiert. Zukünftig wird auch eine Spezifikation für die sog. „IRS“ (ITS Roadside Station) als Feldgerät zur Verfügung stehen, welches ebenfalls über OCIT-O an eine Zentrale angeschlossen und mit dem die Car2X-Kommunikation zu den Fahrzeugen gemäß ETSI ITS G5 realisiert werden kann.
Mittels OCIT-O ist die sichere Bedienung, Überwachung der Gerätefunktionen sowie die Versorgung aus der Ferne möglich. OCIT-O ist aufgrund der starken Verbreitung im Markt die bedeutendste OCIT-Schnittstelle.

Eigenschaften von OCIT-Outstations

Für die sichere Übertragung der Daten zwischen Zentralen und Feldgeräten werden die aus dem Internet bekannten Protokolle TCP und IP verwendet. Diese Protokolle sind unabhängig von der physikalischen Übertragungstechnik (Mobilfunk, Kabelverbindungen) einsetzbar. OCIT-O kann so die rasant wachsenden Möglichkeiten der Telekommunikations- und Netzwerktechnik auch auf der Straße nutzen und verfügt damit über eine zukunftssichere technische Basis. Diese erlaubt es auch, OCIT-Outstations im Laufe der Zeit an neue Anforderungen anzupassen und funktionell zu erweitern.

OCIT-O hat eine eigene Definition für das Übertragungsprotokoll der Anwenderebene, die mit den Internet-Standards koexistieren kann, das „Basis Transport Paket Protokoll Layer“ (BTPPL). BTPPL wurde mit Blick auf die in städtischen Steuernetzen häufig vorhandenen Kabelverbindungen mit teilweise eingeschränkter Übertragungsleistung entwickelt. Es arbeitet mit einem kleinen Verwaltungsdatenanteil und ermöglicht es dadurch auch diese Strecken zu nutzen.

Als fester Bestandteil des Protokolls nutzt OCIT-O eine kryptographische Hashfunktion, die mittels eines Passworts einen Prüfwert für ausgewählte Protokollnachrichten erstellt, mit dessen Hilfe Feldgeräte nicht authentisierbare Nachrichten identifizieren können. Dies verhindert eine nicht autorisierte Beeinflussung dieser Feldgeräte im Rahmen dieser Kommunikation.

Übertagungswege von OCIT-Outstations

BTPPL kann mittels TCP/IP über verschiedene Übertragungswege kommunizieren. Für etliche dieser Kommunikationsarten existieren Standards und damit auch Standard-Kommunikationsgeräte. Beispiele: DSL, Ethernet, GSM, GPRS, UMTS, LTE, öffentliches Telefonnetz, Lichtwellenleiter und Standleitungsbetrieb in privaten Netzen. Im OCIT-System können sämtliche dieser Standardtechniken zur Kommunikation zwischen Feldgeräten und Zentralen genutzt werden. Die entsprechenden Festlegungen dazu im OCIT-Standard werden als OCIT-Übertragungsprofile bezeichnet. Mit den standardisierten OCIT-Übertragungsprofilen sind unterschiedliche Lichtsignalsteuergeräte verschiedener Hersteller ohne weitere Absprachen an zentralen Einrichtungen anschließbar.

Bisher für OCIT-Outstations standardisierte Übertragungsprofile:

Für OCIT-O sind bisher drei Übertragungsprofile mit folgenden Eigenschaften standardisiert:

„Profil 1 – Übertragungsprofil für Punkt-zu-Punkt-Verbindungen auf fest geschalteten Übertragungswegen“

- veröffentlicht seit 2002
- Festlegungen für analoge Vollduplex-Modems
- Datenrate bis 28 kbit/s
- Reichweite bis zu 12 km

„Profil 2 – Übertragungsprofil für Wählverbindungen im Festnetz und GSM-Mobilfunknetz“[1]

- veröffentlicht seit 2005
- Festlegungen für digitale Vermittlungsnetze
  - LSA-seitig üblicherweise GSM (9,6 kbit/s)
  - zentralenseitig üblicherweise ISDN (64 kbit/s)

[1] Das Profil 2 wird von der ODG nicht weiterentwickelt und wird für neue Projekte nicht empfohlen.

- Wählverbindung => keine Standleitung!
- Reichweite theoretisch unbegrenzt

„Profil 3 – Ethernet mit DHCP“ (Dynamic Host Configuration Protocol)

- veröffentlicht seit 2009
- Festlegungen für das Einbinden von Feldgeräten in das Netzwerk über Ethernet
- Zwischen den Ethernet-Endpunkten können eine Vielzahl von Übertragungstechnologien (z.B. DSL, LWL) eingesetzt werden
- Datenrate wird über die im Netzwerk beteiligten Komponenten bestimmt (Netzwerkkarten der Feldgeräte, Switches, Router, etc.)
- Reichweite theoretisch unbegrenzt

Das Profil 1 ist für abgeschlossene und damit anderweitig abzusichernde Netze konzipiert und wird daher bei nachfolgender Sicherheitsbetrachtung nicht berücksichtigt. Je nach Voraussetzung setzt der Betreiber eigene Sicherungsmaßnahmen ein oder es werden bei Bedarf zwischen Betreiber und Hersteller entsprechende Maßnahmen abgestimmt.

Das Profil 2 nutzt das öffentliche digitale Vermittlungsnetz. Die damit mögliche Rufnummernerkennung wird genutzt, um einen nicht autorisierten Zugriff auf das Steuergerät oder die Zentrale zu verhindern. Da das Profil 2 von der ODG nicht weiterentwickelt wird, wird der Einsatz für neue Projekte nicht mehr empfohlen. Für neue Projekte wird stattdessen der Einsatz von Profil 3 in Kombination mit Mobilfunk empfohlen.

Das Profil 3 eignet sich für abgeschlossene Netze, in die die Feldgeräte über Ethernet eingebunden werden können Ethernet ist eine Datennetztechnik für lokale Datennetze, die den Datenaustausch zwischen den angeschlossenen Geräten im lokalen Datennetz ermöglicht. Mit zusätzlichen Einrichtungen wie Routern oder Umsetzern verbindet Ethernet die Geräte per Kupferkabel, Glasfaser oder Mobilfunk aber auch über sehr weite Entfernungen. Dies erlaubt den gewünschten und notwendigen Ausbau der Vernetzung verkehrstechnischer Systeme schnell, effektiv und wirtschaftlich voranzutreiben.

Kommunikation über das Internet mittels projektspezifischem kryptographischen VPN

OCIT ist aufgrund seiner IP-basierten Kommunikation bestens zur Kommunikation über das Internet geeignet. Da das Internet öffentlich ist, müssen geeignete Methoden angewandt werden, um die Datenkommunikation zu schützen. Diese notwendigen Methoden können sehr einfach projekt- oder herstellerspezifisch mit Hilfe von technisch etablierten und bewährten Lösungen realisiert werden. Das OCIT Profil 3 kann daher als Basis dienen, um Lichtsignalsteuergeräte auch über das Internet an einer Zentrale zu betreiben.

Für die Absicherung der Datenkommunikation können kryptographisch basierte VPNs (**Virtual Private Network**) genutzt werden. Mit Hilfe eines VPN kann im „unsicheren“ Internet ein überlagertes, abgesichertes Netzwerk aufgebaut werden und gegen unautorisierte Zugriffe

abgesichert werden. Es stehen verschiedene VPN-Protokolle zur Verfügung, die dem Stand der Technik entsprechen und mit denen ein Höchstmaß an Sicherheit erzielt werden kann.

Im Zusammenspiel mit OCIT Profil 3 wird für ein kryptographisch basiertes VPN die Unterstützung von einem Kommunikationsdienstleister benötigt. Dieser Kommunikationsdienstleister hat einen OCIT-O Profil 3 transparenten Tunnel bereit zu stellen. Der Kommunikationsdienstleister kann ein zusätzlicher Projektpartner, der Zentralen- oder einer der Steuergerätelieferanten sein. (siehe Abbildung 1)

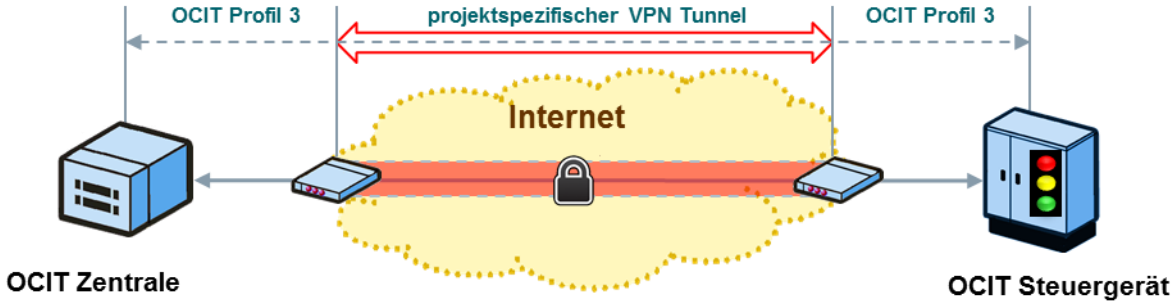

Abbildung 1: Beispiel einer abgesicherten OCIT-Kommunikation über projektspezifischen VPN-Tunnel

In einem VPN können Nachrichten in einem Netzwerk authentisiert und verschlüsselt werden. Sichere Systeme können bei geeigneter Wahl der Parameter (z.B. der Schlüssellänge) nach heutigem Kenntnisstand nicht in überschaubarer Zeit gebrochen werden. Ein etablierter VPN-Tunnel sichert damit die Kommunikation grundsätzlich ab.

Das zukünftige OCIT Profil 4 mit standardisiertem kryptographischen VPN

Auch wenn heute schon sichere OCIT-Datenverbindungen projekt- oder herstellerspezifisch über das Internet aufgebaut werden können, arbeitet die ODG an dem neuen Übertragungsprofil „Profil 4 – Netzkopplung mittels OpenVPN“, um auch hier durch die Standardisierung die Interoperabilität zu vereinfachen und die Sicherheit weiter zu erhöhen.

Das OCIT Profil 4 hat folgende Standardisierungsschwerpunkte:

- OpenVPN wird als Lösung für die Etablierung eines VPN-Tunnels eingesetzt
- Es soll ein sicherer, praxistauglicher und einheitlicher Zertifikatsaustausch ermöglicht werden

OpenVPN ist eine Open-Source-Software und aufgrund seiner Sicherheitseigenschaften und einfachen Anwendbarkeit äußerst verbreitet. OpenVPN nutzt asymmetrische Verfahren für die initiale Aushandlung von kryptographischen Parametern für den VPN-Tunnel. Diese ermöglichen eine beiderseitige Authentifizierung unter Nutzung von öffentlichen und privaten Schlüsseln beider Kommunikationspartner. Der öffentliche Schlüssel wird dabei über eine vertrauenswürdige Instanz der sogenannten Zertifizierungsstelle (Certification Authority, kurz CA) zertifiziert.

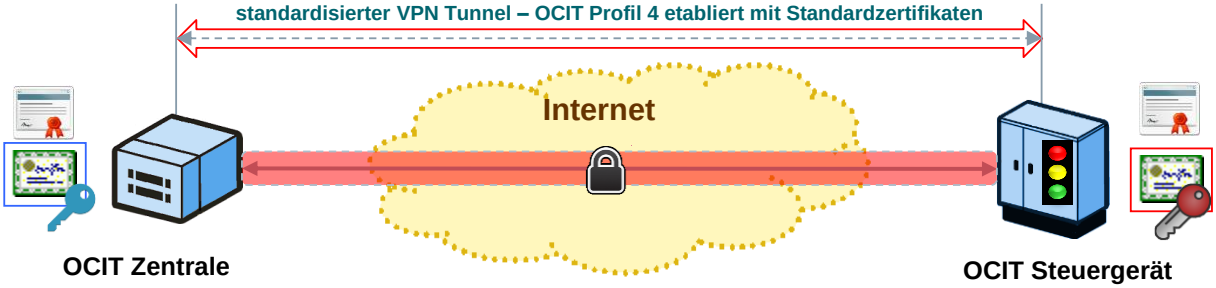

Abbildung 2: standardisierter OpenVPN-Tunnel mit Zertifikaten auf Basis eines standardisierten Zertifikat-Profils

OpenVPN, in einer geeigneten Konfiguration, ermöglicht die Aushandlung und Nutzung von Schlüsselmaterial für den Schutz einer Kommunikationsverbindung. Die so geschützte Verbindung kann nach aktuellem Kenntnisstand als extrem sicher angesehen werden. Von elementarer Bedeutung ist aber das Zertifikatsmanagement, mit dessen Hilfe die Aushandlung des Schlüsselmaterials geschützt wird, damit dies nicht in unbefugte Hände gelangen kann. Bei der Erarbeitung des OCIT Profils 4 werden daher die für das Zertifikatsmanagement notwendigen Formate (Schnittstellen) und Strukturen festgelegt. Alternativ kann auch eine vorhandene PKI genutzt werden, da das Profil 4 auf schon standardisierten Zertifikatsformaten aufsetzt. Es müssen also lediglich die Inhalte im Sinne des OCIT Profil 4 in den Zertifikaten ergänzt werden.

Die PKI ermöglicht die Erstellung, Verteilung und ggf. das Zurückziehen von digitalen Zertifikaten und unterstützt deren Prüfung. Der Aufbau und Betrieb einer PKI erfolgt durch den Anlagenbetreiber direkt oder durch ein von ihm beauftragtes Unternehmen als PKI-Dienstleister. Im Mittelpunkt stehen dabei eine Software zum Betrieb der Zertifizierungsstelle (CA) und eine Organisation zur Ausgabe und Verteilung sowie zum regelmäßigen Austausch der Zertifikate.

Fazit

Mit Hilfe des OCIT Profil 3 in Kombination mit einem kryptographischen VPN können projektspezifisch sichere OCIT-Datenverbindungen über offene Netze, insbesondere über das Internet aufgebaut werden.

Heute auf dem Markt verfügbare VPN-Techniken genügen dem aktuellen Stand der Technik und bieten das erforderliche Niveau an Sicherheit für OCIT-Systeme. VPN-Techniken sind sehr stark verbreitet und gehören heutzutage zum Arbeitsalltag von IT-Fachkräften, was einen routinierten Einsatz dieser Techniken für OCIT-Systeme sicherstellt.

Mit dem zukünftigen OCIT Profil 4 wird die ODG die Netzkopplung mittels OpenVPN standardisieren. Davon werden sowohl die Betreiber als auch die Hersteller von OCIT-Systemen im Hinblick auf die Interoperabilität und die erhöhte Sicherheit profitieren.

Das OCIT Profil 4 wird vor dem Hintergrund erarbeitet, dass existierende OCIT-Systeme später möglichst wirtschaftlich nachgerüstet werden können, was die Investitions- und Zukunftssicherheit von OCIT-Systemen einmal mehr unterstreicht.

OCIT-Systeme sind, insbesondere mit dem Profil 4, bestens gerüstet, um die künftigen Anforderungen, die sich aus der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) bezüglich geschützter Kommunikation ergeben, erfüllen zu können.