AG CYSIS

IT Security bei ETCS

Autoren:

AG CYSIS
UG IT Security bei ETCS

29.06.2019

Inhaltsverzeichnis

1 Management Summary

Das European Train Control System (ETCS) ist ein Zugbeeinflussungssystem und grundlegender Bestandteil des zukünftigen einheitlichen europäischen Eisenbahnverkehrsleitsystems European Rail Traffic Management System (ERTMS). ERTMS/ETCS stellt die aktuelle Generation der Zugsteuerungs- und Zugsicherungssysteme dar und soll langfristig die verschiedenen Zugbeeinflussungssysteme in Europa ablösen und vereinheitlichen. Einher geht ETCS sowohl mit geringeren Kosten im Bahnbetrieb als auch mit der Möglichkeit, mehr Verkehre auf dem Eisenbahnnetz zu fahren.

In Deutschland wurden bisher mehrere Strecken mit ETCS ausgerüstet. Mit dem Fahrplanwechsel im Dezember 2015 wurde die im Rahmen von VDE 8 ausgerüstete Schnellfahrstrecke zwischen Erfurt und Halle/Leipzig mit ETCS in Betrieb genommen. Im Dezember 2017 wurde zusätzlich der Betrieb auf der Neubaustrecke Ebensfeld–Erfurt aufgenommen. Ein weiterer systematischer Ausbau von ETCS ist in den nächsten Jahren geplant.

Bei ETCS sind bereits IT-Sicherheitsmaßnahmen – wie z.B. dedizierte kryptografische Schlüssel – umgesetzt. Eine grundlegende Analyse hinsichtlich Bedrohungen, Angriffsvektoren und daraus abzuleitender Maßnahmen wurde bisher nicht durchgeführt.

Für ETCS kann ein hoher Schutzbedarf in den Schutzwerten Verfügbarkeit sowie Integrität festgestellt werden. In der Analyse der Angriffsvektoren wurde ermittelt, dass erfolgreiche Angriffe auf die Balisen und damit auf die Kommunikation aufgrund der implementierten Sicherheitsfunktionen sehr unwahrscheinlich sind. Man-In-the-Middle-Angriffe sind prinzipiell denkbar, hierfür bedarf es aber sowohl des Zugriffs auf die genutzten symmetrischen Schlüssel als auch das gezielte Abhören der Kommunikation. Ein weiterer, aber nur mit sehr hohem Aufwand durchzuführender Angriff, ist die gezielte Manipulation und der Nachbau der GSM-R Infrastruktur.

Demzufolge bestehen aktuell bei der Nutzung von ETCS keine Sicherheitsrisiken, dennoch sollten – gerade aufgrund der zunehmenden Verbreitung – neue Prozesse und Sicherheitsmaßnahmen Anwendung finden.

Durch die Verwendung eines zeitgemäßen Mechanismus zum Absichern der Kommunikation sowie eines skalierbaren Key Management Centers (KMC) und der dazugehörigen PKI ist es möglich, die hohen Anforderungen der IT-Sicherheit an ETCS zu erfüllen und dadurch das Risiko der unerkannten Verfälschung der über ETCS übermittelten Daten bedeutend zu mindern. Es können hierbei die aus der klassischen IT sehr gut bekannten Prozesse und Techniken einer hierarchischen PKI-Architektur genutzt werden. Damit die PKI von unterschiedlichen Eisenbahnverkehrsunternehmen (EVU) und Eisenbahninfrastrukturunternehmen (EIU) reibungslos zusammenarbeitet, wird empfohlen, dass ein interoperables Datennetz die beteiligten Unternehmen verbindet.

2 Einleitung

2.1 Zielgruppe und Zweck des Dokumentes

Mit ETCS kommen im Bereich der Zugsicherungstechnik neue Komponenten und daher auch neue Schnittstellen zwischen Eisenbahninfrastrukturunternehmen und Eisenbahnverkehrsunternehmen zum Einsatz. In Abhängigkeit des eingesetzten Levels von ETCS erfolgt die Kommunikation zwischen Zug und Infrastruktur über die Balisen im Gleis oder ergänzend über den digitalen Zugfunk GSM-R. Ab ETCS Level 2 kann sogar auf herkömmliche Streckensignale verzichtet werden.

Dieses Dokument betrachtet die neuen Funktionen und Schnittstellen, die durch ETCS eingeführt werden, es werden die wesentlichen Aspekte der IT-Sicherheit bei ETCS (Schutzbedarf, Angriffsvektoren, Gefährdungen, notwendige Maßnahmen, Architekturen, Kryptografie, …) beschrieben. Detailliert beschrieben wird eine mögliche Ausprägung der PKI-Funktionen, die bei ETCS eingesetzt werden sollten.

Das vorliegende Whitepaper der Arbeitsgruppe „IT Security bei ETCS“ richtet sich an Eisenbahnverkehrsunternehmen und Betreiber von Eisenbahninfrastrukturen, Hersteller von Systemen und Komponenten für den Eisenbahnbetrieb, Vertreter von Eisenbahnaufsichtsbehörden und Vertreter von Wissenschaft und Forschung in einschlägigen Themengebieten. Das Dokument soll auch als Input für Normierung verwendet werden können.

Die Untergruppe „IT Security bei ETCS“ in der Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen (CYSIS) wurde gegründet, um das wichtige Thema IT-Sicherheit bei ETCS in einer Expertengruppe aus Forschung, Wirtschaft und Bahnbetrieb zu erörtern und einen konsolidierten, ganzheitlichen Ansatz zu erarbeiten. Dies ist erforderlich, da bei vielen europäischen Bahnbetreibern in den nächsten Jahren ein Technologiewandel im Bereich der Sicherungstechnik, speziell bei ETCS ansteht.

Eine allgemeine Beschreibung zu Sinn und Zweck der Betrachtungen zur Cybersecurity for Railways ist im Dokument „Whitepaper Security for Safety“, Ref. [1], gegeben und wird hier nicht wiederholt.

Dieses Dokument ersetzt bei Einführung oder Nutzung von ETCS nicht die sorgfältige Durchführung der notwendigen Maßnahmen bezüglich IT-Sicherheit, z.B. IT-Risikomanagement, Sicherheitskonzepte oder Zulassungen.

3 Funktionen und Architektur von ETCS

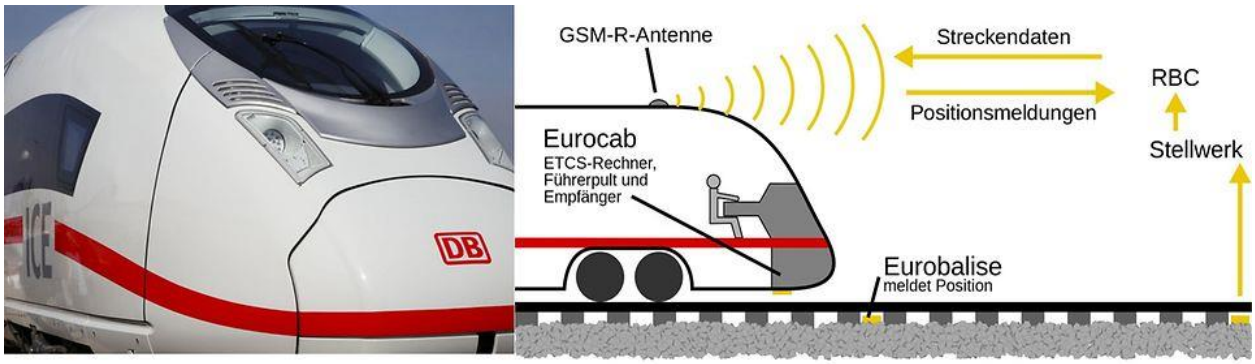
3.1 Allgemeines

Mit dem European Train Control System (ETCS) wird derzeit europaweit ein einheitliches Zugbeeinflussungssystem eingeführt. Damit sollen zum einen die Kosten für Fahrzeuge, die im internationalen Verkehr eingesetzt werden durch Verzicht auf nationale Zugbeeinflussungssysteme sinken, zum anderen vereinfacht ETCS die Arbeit des Triebfahrzeugführers (Tf) durch ein einheitliches Anzeige- und Bedienkonzept.

Grundsätzlich kommunizieren Fahrweg und Fahrzeug über Balisen im Gleisfeld, dabei werden Informationen an das Fahrzeug übertragen. Ab ETCS Level 2 findet eine bidirektionale Kommunikation über GSM-R statt.

Grundlage der Einführung von ETCS ist die Verordnung (EU) 2016/919 der Kommission vom 27. Mai 2016 über die technische Spezifikation für die Interoperabilität der Teilsysteme „Zugsteuerung, Zugsicherung und Signalgebung“ des Eisenbahnsystems in der Europäischen Union (TSI ZZS[1]). Sie fordert in Kapitel 7.4.4. von den Mitgliedsstaaten die Ausarbeitung und Notifizierung nationaler Umsetzungspläne bezüglich der Ausrüstung ihrer Eisenbahnnetze mit dem europäischen Zugbeeinflussungssystem ETCS und der Außerbetriebsetzung der bestehenden nationalen Systeme („Klasse-B-Systeme“).

Die folgende Abbildung zeigt das Funktionsprinzip und die eingesetzten Komponenten bei ETCS am Beispiel von Level 2.



3.2 Level 1

3.2.1 Allgemeines

In ETCS Level 1 werden die Informationen von der Strecke ans Fahrzeug praktisch ausschließlich über Balisen übertragen. Es handelt sich damit um eine punktförmige unidirektionale Schnittstelle. Es gibt zwar noch die Möglichkeit, mit dem EuroLoop – eine Art Antennenkabel in Gleismitte, i. d. R. kurz vor Hauptsignalen verlegt – eine linienförmige unidirektionale Schnittstelle oder mittels Radio-Infill über GSM-R eine linienförmige bidirektionale Schnittstelle zu nutzen. Beide Möglichkeiten erfordern jedoch streckenseitig – im Fall des EuroLoop auch fahrzeugseitig – hohen Aufwand und werden daher zumindest in Deutschland nicht angewendet.

Um die veränderlichen Signalbegriffe in geeigneter Weise abzugreifen, werden LEU-s (lineside electronic units) eingesetzt, die aus dem jeweiligen Signalbegriff (z. B. Hauptsignal- und Vorsignalbegriff bei gleichem Standort) die entsprechenden Telegramme erzeugen oder über eine Matrix der Eingangsinformationen ermitteln und an die Balise senden.

3.2.2 Full Supervision

Bereits mit ETCS Level 1 Full Supervision (L1FS) ist es auf Basis von Balisen möglich, ein anzeigeführendes System aufzubauen: Dem Tf wird neben der Ist- auch die Sollgeschwindigkeit

[1] Technische Spezifikationen Interoperabilität für Zugsicherung, Zugsteuerung und Signalgebung

angezeigt. Allerdings ist der Aufwand für Projektierung und Installation so hoch, dass er bei geringerer Leistungsfähigkeit über dem Aufwand von Level 2 liegt. L1FS kommt daher in Deutschland nicht zur Anwendung.

3.2.3 Limited Supervision

Limited Supervision (LS) überwacht im Gegensatz zu Full Supervision nur im Hintergrund. Die Anforderungen an Präzision und Sicherheit der übertragenen Daten sind daher geringer. Der Tf fährt nach den Signalen, da keine Anzeigeführung vorhanden ist. Aus diesem Grund sind die Implementierungen von Limited Supervision auch stark durch den nationalen Betriebsprozess geprägt und unterscheiden sich bei unterschiedlichen EIUs teilweise substanziell.

In Deutschland orientiert sich die „ETCS signalgeführt“ genannte nationale Implementierung von Limited Supervision an der PZB 90. So gesehen wurde keine betriebliche Interoperabilität erreicht, sehr wohl jedoch eine technische. Diese unterstützt den Tf durch einheitliche – also gleichbedeutende – Anzeigen und Bedienungen. Der Vorteil der deutschen Implementierung gegenüber L1FS liegt einerseits in der Standardprojektierung der Datenpunkte (DP), die den Aufwand für die Projektierung signifikant reduziert. Andererseits werden die benötigten Informationen überwiegend aus den PZB-Kontakten ausgelesen, was den technischen Aufwand für die Anschaltung und Zulassung dieser Komponenten substanziell reduziert.

3.3 Level 2

Auch wenn der in Abschnitt 3.2.3 für L1 beschriebene Mode Limited Supervision auch in Level 2 (L2) verfügbar ist, spielt er hier keine nennenswerte Rolle. Daher bezieht sich diese Beschreibung ausschließlich auf Full Supervision (L2FS).

In L2FS wird die Balisen-gestützte Kommunikation durch einen bidirektionalen Funkkanal ergänzt. Diese Verbindung wird mittels Euroradio kryptografisch geschützt. Über sie können einerseits jederzeit aktualisierte Informationen, wie z.B. Fahrterlaubnisse gesendet werden. Andererseits ist der Zug in der Lage, darüber initiale Informationen zur Zugfahrt (u.a. Höchstgeschwindigkeit und Bremsvermögen) sowie laufend Standortmeldungen an die Streckenseite zu senden.

Wie L1FS bietet auch L2 Anzeigeführung. Eine erste Infrastrukturoptimierung ist durch den Verzicht auf Haupt- und Vorsignale möglich, wie sie auf der Neubaustrecke Nürnberg – Erfurt – Halle / Leipzig seit 2015 erstmals zum Einsatz kommt.

3.4 Level 3

Der Level 3 von ETCS bietet alle unter Level 2 beschriebenen Möglichkeiten. Hinzu kommt die fahrzeugseitige Zugvollständigkeitsprüfung, sodass die aufwändige streckenseitige Gleisfreimeldeanlage verzichtbar ist oder zumindest substanziell reduziert werden kann.

Zudem können sich die Züge neu im Bremswegabstand folgen (moving block). Alternativ dazu kann mit den gleichen Mitteln die Gleisfreimeldeanlage über ETCS virtualisiert werden, was bei sinkenden Infrastrukturkosten eine höhere Flexibilität, verglichen mit einer entsprechenden festen Installation, mit sich bringt.

3.5 Schutzbedarf

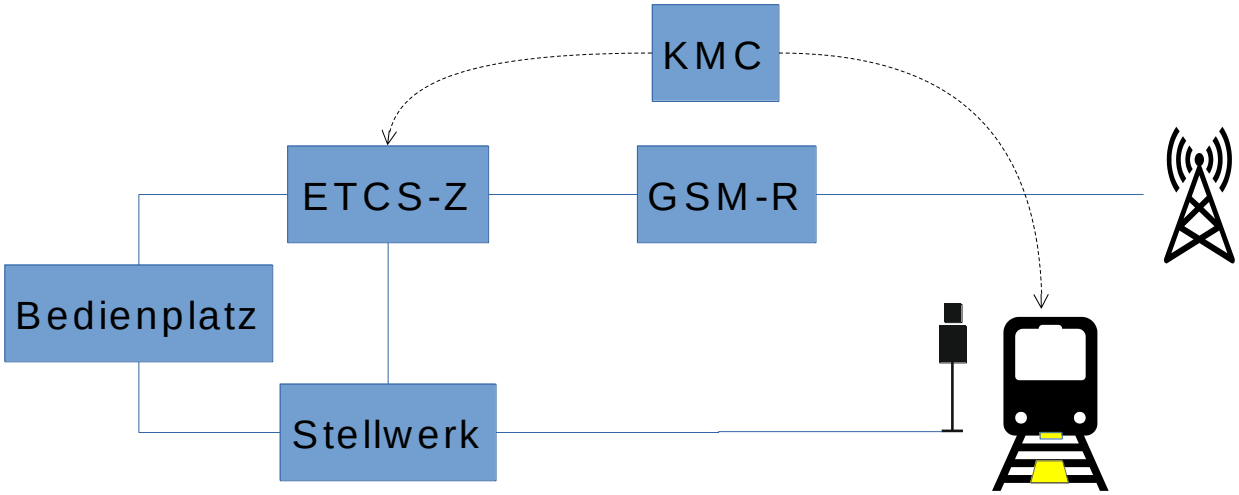
Der für die ETCS-Zentrale (ETCS-Z) ermittelte hohe Schutzbedarf für die Schutzwerte Verfügbarkeit und Integrität ergibt sich im Wesentlichen aus zwei Punkten:

- Es handelt sich um eine Anlage, deren Ausfall namentlich auf Strecken ohne konventionelle Signalisierung – also aktuell der VDE 8 von Nürnberg über Erfurt nach Halle und Leipzig, künftig aber noch weitere Strecken – gravierende Auswirkungen hat. Ein Ausfall hätte demnach zwei Folgen:
    - Zum einen wäre die Strecke nahezu unbenutzbar, Züge müssten umgeleitet werden und würden demnach auf anderen Strecken zur Überlastung führen.
    - Zum andern müssen die sich auf der betroffenen Strecke befindlichen Züge diesen Bereich räumen, was zwangsläufig mit für die Betriebssicherheit einschränkenden Maßnahmen verbunden ist.

- Zum anderen ist bei sicherungstechnischen Anlagen – ebenfalls nicht überraschend – das unverfälschte Erfassen, Übertragen und Verarbeiten der Daten von entscheidender Bedeutung. Auch aus diesem Punkt resultiert ein hoher Schutzbedarf, da verfälschte, unzeitige oder unterdrückte Informationen weitreichende Folgen haben können.

3.6 Kommunikationsbeziehungen in ETCS

Das folgende Bild zeigt die Kommunikationsbeziehungen im ETCS-Umfeld.



Dabei sind die folgenden Subsysteme und Funktionen relevant für die nachfolgenden Analysen.

- Schnittstellen Balise (gelbe Markierung in oberem Bild)
  - Programmierung der Balise
  - Schnittstelle Balise / Infrastruktur (Zug, Stellwerk bzw. Feldelemente)

- Schnittstellen Fahrzeuggerät On Board Unit (OBU)
  - OBU – RBC via GSM-R oder zukünftig weiterer Datenverbindungen entsprechend der Spezifikation Future Railway Mobile Communication System (FRMCS)
  - OBU – Fahrzeugbussystem(e) → (nicht ETCS spezifisch und wird deswegen hier nicht weiter analysiert)

- Schnittstellen ETCS-Zentrale Radio Block Center (RBC)
  - RBC – OBU via GSM-R oder zukünftig weiterer Datenverbindungen
  - RBC Bedienerschnittstelle
  - RBC – Stellwerk

- Key Management Center (KMC) für ETCS. Aktuell erfolgt die Schlüsselübertragung offline. Zukünftig wird dies online erfolgen.
  - Bedienerschnittstelle Einrichten der Schlüssel und Zugriffsberechtigungen
  - Übertragung der Schlüssel auf die operativen Subsysteme OBU, RBC

Mögliche Angriffsvektoren werden im Folgenden genauer analysiert.

4 Angriffsvektoren

Denkbare Angriffe auf die Sicherheit des Systems erfolgen beispielsweise durch Eindringen in die Kommunikation zwischen Fahrzeug und Fahrweg. Der Angriff über einzelne manipulierte Balisen und ihrer Telegramme erscheint angesichts des lokal begrenzten Wirkradius als sehr aufwändig. Kritischer ist die Kommunikation über die Funk-Schnittstelle zu sehen, da diese gegebenenfalls von einem entfernten Arbeitsplatz attackiert werden kann und somit zeitgleich mehrere Fahrzeuge betroffen sein können.

4.1 Definition Cyberangriff

Eine Cyber-Attacke oder ein Cyberangriff ist der gezielte Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf ein für eine spezifische Infrastruktur wichtiges Rechnernetz von außen mit dem Ziel, die Vertraulichkeit, Integrität oder Verfügbarkeit der angebundenen IT-Systeme und/oder des Rechnernetzes selbst zu beeinträchtigen. Verschiedene Rechnernetze können gleichzeitig Ziel eines Cyberangriffs sein.

4.2 Gefährdungen für ETCS Level 1

Wie bereits eingangs dargelegt, erfolgt – zumindest in Deutschland – die Kommunikation zwischen Strecke und Fahrzeug ausschließlich über Balisen. Demzufolge muss sich der Angriff gegen dieses Kommunikationsmedium richten.

Denkbar ist es beispielsweise, einen Zug auf einer Strecke mit L1LS nach L1FS zu kommandieren und eine Fahrterlaubnis z.B. für 300 km/h zu übertragen. Der Ablauf lässt sich wie folgt skizzieren:

1. Der Tf bemerkt die Veränderung, weil nicht nur das Symbol für den Mode LS erlischt, sondern auch – noch wesentlich auffälliger – der Tachokreis für Anzeigeführung erscheint. Ein aufmerksamer Tf wird dies sicher bemerken und sollte den Fahrdienstleiter geeignet informieren. Spätestens dann, wenn sogenannte Signalisierungswidersprüche zwischen der zulässigen Geschwindigkeit gemäß Anzeige und Strecke auftreten, werden entsprechende Meldungen durch die Tf immer wahrscheinlicher.
2. In vielen Fällen fährt der Zug – bspw. ein Güterzug – bereits an der durch die Fahrzeuge bestimmten Höchstgeschwindigkeit. Diese lässt sich infrastrukturseitig nicht beeinflussen und wird daher auch in L1FS entsprechend überwacht. Eine effektive Geschwindigkeitserhöhung namentlich eine, die zu gefährlichen Situationen führen könnte, ist damit unwahrscheinlich, da der Tf über zusätzliche Informationen verfügt, z.B. Buchfahrplan, Streckenkenntnis.
3. An jedem eine Fahrterlaubnis ausgebenden Datenpunkt werden dem Zug wieder die korrekten Werte übertragen, sodass die Auswirkungen eines solchen Angriffs begrenzt sind.

<u>Bewertung:</u>

Die praktischen Auswirkungen eines solchen Angriffs sind unter Berücksichtigung der o. g. Punkte vergleichsweise gering.

4.3 Session-Inhalte verfälschen

Die Inhalte einer ETCS-Session lassen sich gezielt über einen Man-In-The-Middle-Angriff verfälschen. Dazu muss man

1. den individuellen ETCS-Schlüssel in Erfahrung bringen,
2. die Session mithören sowie
3. Pakete (ggf. bestimmten Inhalts) unterdrücken und stattdessen eigene senden.

Der Angriffsvektor ist hier das In-Erfahrung-bringen des symmetrischen Schlüssels, der für das Signieren der Pakete verwendet wird. Bei der DB Netz AG wird zwar für jede Kombination von

RBC und Fahrzeug ein eigener Schlüssel verwendet, sodass die Reichweite eines erfolgreichen Angriffs nicht hoch ist. Jedoch entspricht das verwendete Verfahren 3DES (Triple-DES) nicht mehr dem Stand der Technik[2] und wird perspektivisch durch ein Zertifikate-basiertes System (Public-Key-Infrastruktur– PKI) mit modernen kryptografischen Verfahren ersetzt, welches die Schlüssel und Zertifikate über das Netzwerk verteilt (Online-KMC).

Bewertung:

Auch wenn die eingesetzte Verschlüsselung nicht mehr – zumindest für Neusysteme – dem aktuellen Stand der Technik entspricht, ist davon auszugehen, dass dieser Angriff praktisch ausgeschlossen werden kann.

4.4 Eigene Session aufbauen (Level 2)

Ein weiterer Angriffsvektor betrifft das Vortäuschen einer Infrastruktur, die nicht die erwartete ist. Dazu sind folgende Maßnahmen notwendig:

- Es ist ein eigenes GSM-R-Netz aufzubauen, das eine für die gefahrene Strecke und Geschwindigkeit relevante Ausdehnung hat.
- Es ist ein eigenes RBC zu implementieren, welches die Kommunikation nach TSI beherrscht.
- Es muss ein zum Fahrzeug passender ETCS-Schlüssel vorhanden sein.
- Die Streckenprojektierung im „Fake-RBC“ muss zur vorhandenen passen.

Bewertung:

Dieser Angriff erfordert ein sehr hohes Maß an Wissen und Erfahrung. Zudem ist der technische und logistische Aufwand immens sowie die Gefahr des Scheiterns und des Entdeckt-werdens sehr hoch.

Dieser Angriff kann daher praktisch ausgeschlossen werden.

4.5 Level-Transition

Folgender Angriff ist auf Strecken mit ETCS Level 2 denkbar:

- Mittels einer vom Angreifer im Gleis eingebrachten Balise (Wurf-Balise) wird eine Transition nach L1FS kommandiert.
- Der Zug wechselt nach L1FS – optimalerweise mit der gleichen Geschwindigkeitsvorgabe wie bei L2.
  Anmerkung: Ein Wechsel nach L1LS ist zwar auch möglich, jedoch verlöschen dann die Führungsgrößen, was auf Strecken ohne konventionelle Signalisierung jeden Tf stutzig macht.
- Die Anzeigen wechseln zwar, unterscheiden sich aber nicht signifikant von denen bei L2 (Level-Symbol ähnlich, Symbol für die Session mit dem RBC verlischt).
  → Der Tf bemerkt den Levelwechsel auf einer Strecke ohne konventionelle Signalisierung nicht zwangsläufig. Auf Strecken mit Signalen wird die Reaktion des Stellwerks auf die verloren gegangene Eigenschaft des Zuges, geführt zu werden, offensichtlich: Die bis eben noch Fahrt (hell oder dunkel) zeigenden Signale werden auf Halt gestellt. Auch hier ist demnach die Möglichkeit der Entdeckung durch den Tf sehr hoch.
- Um eine Zwangsbremsung nach 1,8 km wegen fehlender Ortung zu vermeiden, ist eine Streckenprojektierung passend zur vorhandenen Infrastruktur notwendig.

Aus diesem Grund wurde der Change Request (CR) 1240 gegen die TSI erstellt, der dem RBC das Senden eines unconditional emergency stop bei unerwartetem Levelwechsel ermöglicht. Dieser CR wird voraussichtlich Eingang in die kommende Version der TSI finden.

[2] Gemäß aktueller Empfehlung vom BSI sind bezüglich 3DES keine praktischen Angriffe bekannt. Es entspricht grundsätzlich für neue Systeme nicht mehr dem Stand der Technik [2].

Bewertung:

Trotz des vergleichsweisen hohen Aufwands ist dieser Angriff durchführbar, wenngleich nur auf Strecken ohne konventionelle Signalisierung wirklich Erfolg versprechend. Hier schafft jedoch der o. g. CR dauerhaft und wirkungsvoll Abhilfe.

5 Cybersecurity Maßnahmen für ETCS

5.1 Maßnahmen für die Balise

Das Signieren von Daten bietet die Möglichkeit, deren Authentizität überprüfen zu können. Diese grundsätzlich auch für Baliseninhalte wünschenswerte Maßnahme lässt sich aber nicht ohne weiteres anwenden:

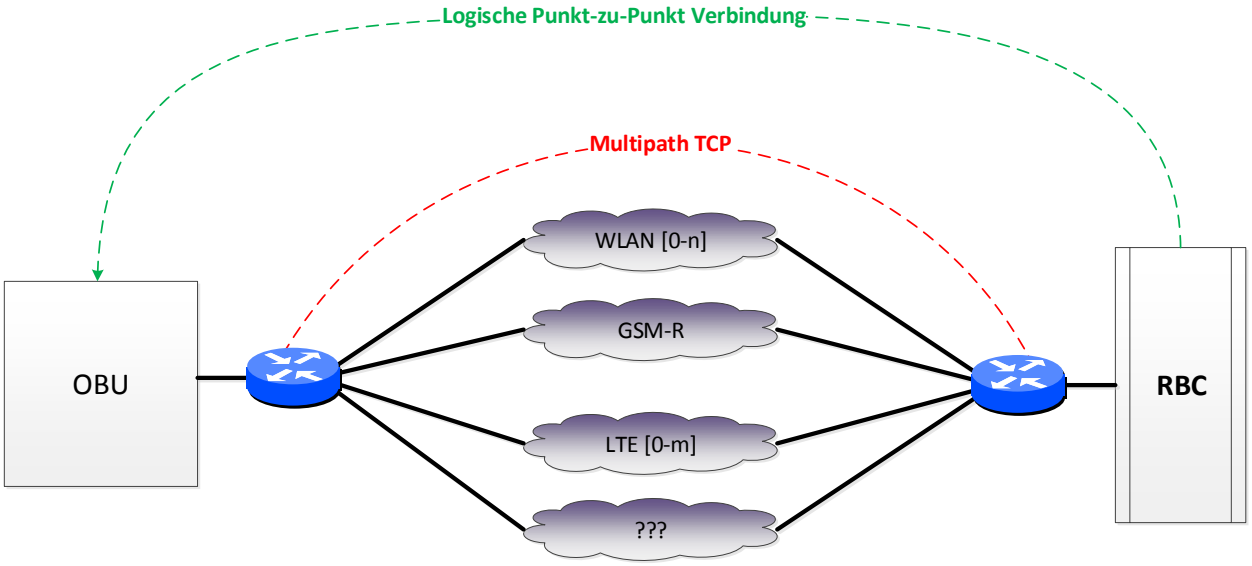
1. Wie kommt der öffentliche Schlüssel aufs Fahrzeug? Um eine Signatur prüfen zu können, muss der zugehörige öffentliche Schlüssel auf das Fahrzeug übertragen werden. Ein Übertragen per Balise scheidet aus, da dieser Schlüssel ebenso leicht wie der Baliseninhalt verändert werden kann, der eigentlich dadurch geschützt werden soll. Zudem wird dadurch ein katastrophaler Denial-of-Service-Angriff möglich: Es muss nur der Schlüssel verändert oder unbrauchbar gemacht werden und schon werden alle Baliseninhalte verworfen.
   Falls das Zertifikat online abgerufen werden soll, hat das Auswirkungen auf die Zeit bis zur Bereitschaft von ETCS Level 1 (ähnlich L2) sowie eine Ausrüstung mit GSM-R ähnlich L2 zur Folge.
2. Wie lange ist das für das Signieren verwendete Zertifikat gültig? Unabhängig von seiner Gültigkeit (außer größer 100 Jahre) muss von Anfang an eine Strategie für dessen Tausch erarbeitet werden, da die Balisen eine Lebensdauer von 20 Jahren und mehr haben. Es ist daher davon auszugehen, dass sie von einer (Sub-)Certificate Authority (CA) mit mindestens 20 Jahren Restlaufzeit abgeleitet werden müssen. Das ist insofern kritisch, als dass bereits mit den heute verfügbaren Mitteln das Kompromittieren eines Zertifikats innerhalb von 40 Jahren wahrscheinlich scheint (Annahme: Das Zertifikat wird mittels Brute-Force-Attacke etwa nach der Hälfte der möglichen Versuche geknackt).
3. Bei einer Gültigkeitsdauer von mindestens 20 Jahren ist das Führen einer Certificate Revocation-List (CRL) unerlässlich, was folgende Fragen aufwirft:
   - Wie geht das Fahrzeug mit Baliseninhalten zurückgezogener Zertifikate um?
   - Welche Maßnahmen sind infrastrukturseitig in welcher Zeit beim Zurückziehen eines Zertifikats notwendig? Wie groß dürfen die Bereiche sein, in denen ein einzelnes Zertifikat angewendet wird? Welche Infrastruktur ist für das Verwalten notwendig?
   - Was passiert mit Baliseninhalten, deren Authentizität nicht verifiziert werden konnte (siehe auch Punkt 1)? Dürfen sie verworfen werden? Und falls nicht, was nützt dann noch die Signatur?

<u>Bewertung</u>

Das Signieren von Baliseninhalten ist nicht sinnvoll möglich, da der Aufwand beim Wechsel des Zertifikats für die statisch projektieren Balisen und Lineside Electronic Units (LEUs) zu hoch ist.

5.2 Maßnahmen für die OBU

Ein verhältnismäßig einfach durchführbarer Angriff auf das Mobilfunknetz ist das Stören der Sendefrequenzen. Um den daraus resultierenden Schaden durch verringerte Verfügbarkeit zu mindern, kann die Punkt-zu-Punkt-Verbindung zwischen OBU und RBC virtualisiert werden. Eine Nachricht über den zukünftig virtualisierten Kanal kann zeitgleich über mehrere drahtlose Verbindungen (z.B. GSM-R, LTE, 5G, WLAN, usw.) übertragen werden. Da alle Technologien unterschiedliche Frequenzen verwenden, erschwert die Virtualisierung einen Jamming-Angriff, denn der Angreifer muss alle Frequenzen stören.



Kryptographische Schlüssel auf der OBU

In einer zukünftigen PKI muss die OBU lediglich einen öffentlichen Schlüssel pro Infrastrukturbetreiber speichern können, der aber eine verhältnismäßig kurze Gültigkeitsdauer hat. Dadurch wird das Schlüsselmanagement auch robust gegen kurzfristige Umleitungen.

5.3 Maßnahmen für die LST

ETCS-Zentrale

Die ETCS-Zentrale stellt keine besonderen Anforderungen an die IT-Sicherheit verglichen mit den übrigen zentralen Systemen der Leit- und Sicherungstechnik, allen voran der ESTW-Zentrale.

Integrität und Authentizität

Im Gegensatz zu den vergleichsweisen mittleren Anforderungen hinsichtlich der Vertraulichkeit sind Integrität und Authentizität im Umfeld der Leit- und Sicherungstechnik ein hohes Gut: Es ist essenziell, sicher zu stellen, dass die empfangene Nachricht vom angeblichen Absender stammt und unverfälscht ist.

Das Signieren der Nachrichten ist daher unerlässlich. Diese Signatur muss jedoch nicht in der Applikationsschicht (Telegrammebene) erfolgen. Sie kann auch auf Basis der Applikationskommunikation (Verbindungsebene, IPSec) erfolgen.

5.4 Security-Anforderungen für OBU, RBC und KMC

Die OBU, das RBC und das KMC müssen ein standardgemäßes Zeitnormal wie NTP (RFC 1305) unterstützen und die Systemzeit von einer zentralen Zeitstelle beziehen.

Sie müssen eine standardgemäße Ereignisprotokollierung wie Syslog (RFC 5424) unterstützen, und Ereignisprotokolle an eine zentrale Logsenke, soweit wie möglich, in Echtzeit senden.

Sie müssen eine zentralisierte und rollenbasierte Benutzer- und Berechtigungslösung, wie z.B. Microsoft Active Directory, Cisco TACACS+ oder LDAP/Kerberos unterstützen. Die Benutzer- und Berechtigungsverwaltung muss zentral implementiert werden.

Sie müssen die Verwaltung bei Benutzern mit administrativen Rechten die Zweifaktor-Authentifizierung unterstützen, und diese muss implementiert und aktiviert werden.

Sie dürfen keine direkte Internetverbindung haben und nicht mit Remote-Zugriff durch einen Benutzer mit administrativen Rechten verwaltet werden.

Sie müssen gegen Cyberangriffe gehärtet werden, unnötige Dienste, Schnittstellen, Protokolle und Port-Nummer müssen entsprechend deaktiviert, gesperrt oder verboten werden (Stichwort „Whitelist“).

Die Subnetze, in denen sie betrieben werden, müssen durch eine Firewall isoliert werden. Die Firewall darf nur die benötigten Protokolle erlauben und muss diese in allen Richtungen inspizieren, ggf. Ereignisprotokolle über verdächtige Aktivitäten generieren.

Sie müssen in einem physisch gesicherten und überwachten Bereich installiert und betrieben werden.

5.5 Verschlüsselung und Zertifizierung

Der aktuell genutzte symmetrische Verschlüsselungsalgorithmus 3DES (Triple-DES) benutzt zwei Schlüssel (oder drei). 3DES arbeitet bei Verwendung von zwei Schlüsseln von jeweils 56 Bit mit einer Schlüssellänge von 112 Bit. 3DES gilt zwar noch heute als nicht kompromittiert, stellt aber nicht den Stand der Technik dar [2].

Eine moderne Schlüssel- oder Zertifikatsverwaltung und -verteilung ist daher eine Grundvoraussetzung für die Zukunftsfähigkeit. Die notwendigen Anpassungen gehen in zwei Richtungen:

1. Es ist ein Key Management Center (KMC) zu installieren, dass einerseits die Endgeräte mit Zertifikaten versorgt und andererseits für andere KMCs als Instanz für das Überprüfen von Zertifikaten dient.
2. Es ist ein Verfahren zu etablieren, mit dem Schlüssel Ende zu Ende online übertragen werden, sodass keine Lücken durch USB-Sticks, Wartungs-Notebooks u. dgl. überbrückt werden können oder müssen.

Die Details zur optimalen Ausgestaltung der PKI werden ausführlich im Anhang beschrieben.

6 Zusammenfassung

Der geplante weitere Ausbau der Nutzung von ETCS bedingt eine systematische Beschäftigung mit den relevanten Angriffsvektoren und eine Analyse der notwendigen Maßnahmen bezüglich IT-Sicherheit. Einher geht dies mit aktuell eingesetzten kryptografischen Verfahren und Prozessen, für die aktuell (noch) keine Angriffe bekannt sind, die aber nicht mehr dem aktuellen Stand der Technik entsprechen.

Die Analyse belegt, dass aktuell bei der Nutzung von ETCS kein Sicherheitsrisiko besteht, dennoch sollten – gerade aufgrund der zunehmenden Verbreitung – neue Prozesse und Sicherheitsmaßnahmen Anwendung finden.

Es wird empfohlen im weiteren Ausbau von ETCS zeitgemäße kryptografische Mechanismen zum Absichern der Kommunikation, ein skalierbares Key Management System sowie eine Public Key Infrastruktur (PKI) aufzubauen. Damit kann sichergestellt werden, dass die hohen Sicherheitsanforderungen langfristig angemessen erfüllt werden können und das potenzielle Risiko einer unerkannten Verfälschung der im ETCS übermittelten Daten bedeutend gemindert wird.

7 Anhang - Schlüssel und Zertifikate (PKI) für ETCS

Ziel des Einsatzes der Public-Key-Infrastruktur (PKI) im ETCS ist es, kryptografische Schlüssel und Zertifikate für den Aufbau von gesicherten Verbindungen bereitzustellen und die eindeutige gegenseitige Authentifizierung zwischen Zügen und RBCs sowie RBCs untereinander zu gewährleisten.

Für die PKI für ETCS wird der Einsatz eines interoperablen Datennetzes präferiert, das europaweit für alle beteiligten Eisenbahnunternehmen zugänglich ist.

Durch dieses Datennetz sind Eisenbahnunternehmen, die die hier vorgeschlagene einheitliche PKI betreiben und diese für einen sicheren Verkehr benutzen, unabhängig von der Architektur der PKI.

In diesem interoperablen Datennetz können Eisenbahnunternehmen unter anderem die Validation Authority (CRL oder Online Certificate Status Protocol (OCSP)-Responder) aller anderen Eisenbahnunternehmen erreichen, um die Gültigkeit der Zertifikate von Zügen bzw. von RBCs zu prüfen.

CRL oder OSCP-Responder

Für den Fall, dass die Kompromittierung eines Zertifikats oder die Erkennung des Diebstahls eines privaten Schlüssels länger dauert als diese gültig sind, kann auf das Führen einer CRL / OCSP-Responder verzichtet werden.

7.1 Erforderliche Vertrauensbeziehungen

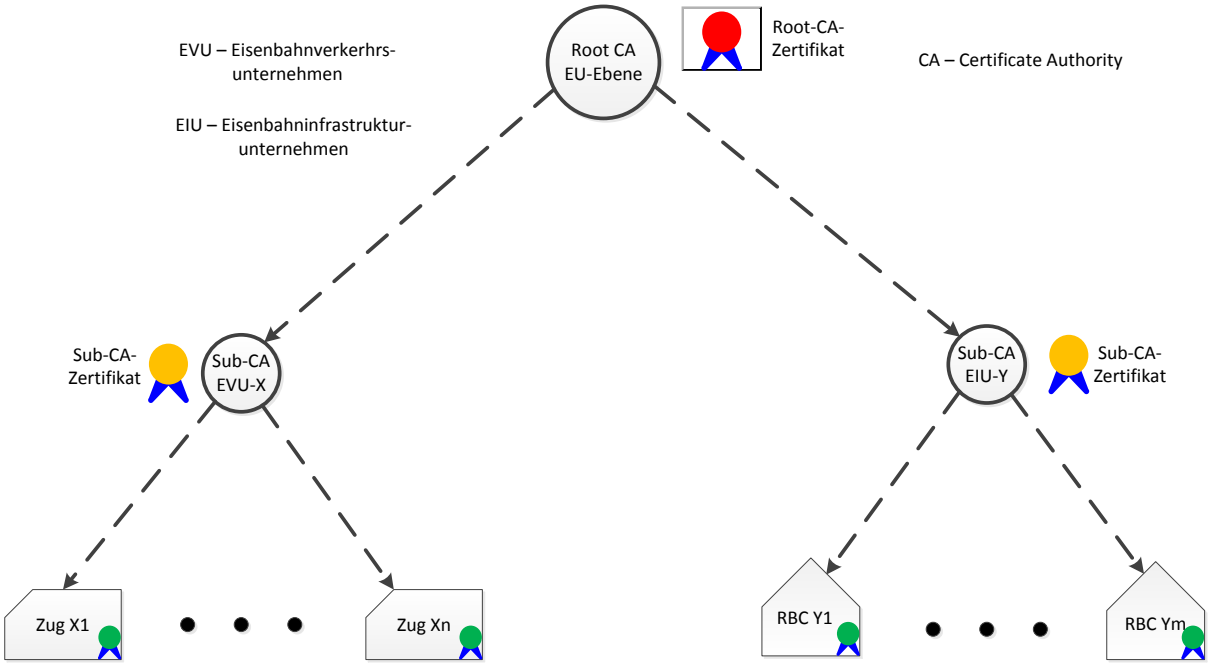
Für die sichere Durchführung von Zugfahrten sind Vertrauensbeziehungen Zug-RBC und RBC-Zug notwendig. Ein Zug muss sich gegenüber jedem RBC authentifizieren, durch dessen Infrastruktur er fährt. Umgekehrt, muss ein RBC sich gegenüber jedem Zug authentifizieren, von dem seine Infrastruktur befahren wird.

Es muss ein Mechanismus eingebaut werden, über den erfolgreiche Verbindungsaufbauten gezielt unterdrückt werden können, auch wenn die Authentifizierung erfolgt. Das ist nötig z.B. in dem Fall, wenn ein Zug eine bestimmte Strecke aus anderen Gründen nicht befahren darf.

7.2 Auswahl verschiedener PKI-Architekturen

In der IT-Welt werden grundsätzlich zwei verschiedene PKI-Architekturen verwendet: hierarchische oder flache PKI-Architektur. In diesem Kapitel werden diese Lösungsvarianten beschrieben und ihre Vorteile und Nachteile erläutert.

7.2.1 Hierarchische PKI-Architektur



In der zentralen Stelle der PKI steht eine Root Certificate Authority (Root CA), die auf EU-Ebene betrieben wird. Diese Root-CA wird benötigt, damit alle Endgeräte von Eisenbahnverkehrsunternehmen (EVUs) und Eisenbahninfrastrukturunternehmen (EIUs) (Züge und RBCs) in der Europäischen Union einer zentralen Stelle vertrauen.

Die Root-CA erstellt und signiert die Zertifikate von Sub-Certificate Authorities (Sub-CAs).

Die Root-CA ist besonders zu schützen und im Regelbetrieb "offline". Sie wird aktiviert, wenn die Zertifikate für die Sub-CAs erneuert werden müssen.

EVUs und EIUs haben Ihre eigene Sub-CA, die dafür eingesetzt wird, Zertifikate für eigene Züge bzw. für eigene RBCs zu erstellen.

Vorteile der hierarchischen Architektur:

- Einfach handhabbar und skalierbar. Mit einer Aktion wird automatisch allen Teilnehmern (EIU und EVU) vertraut.

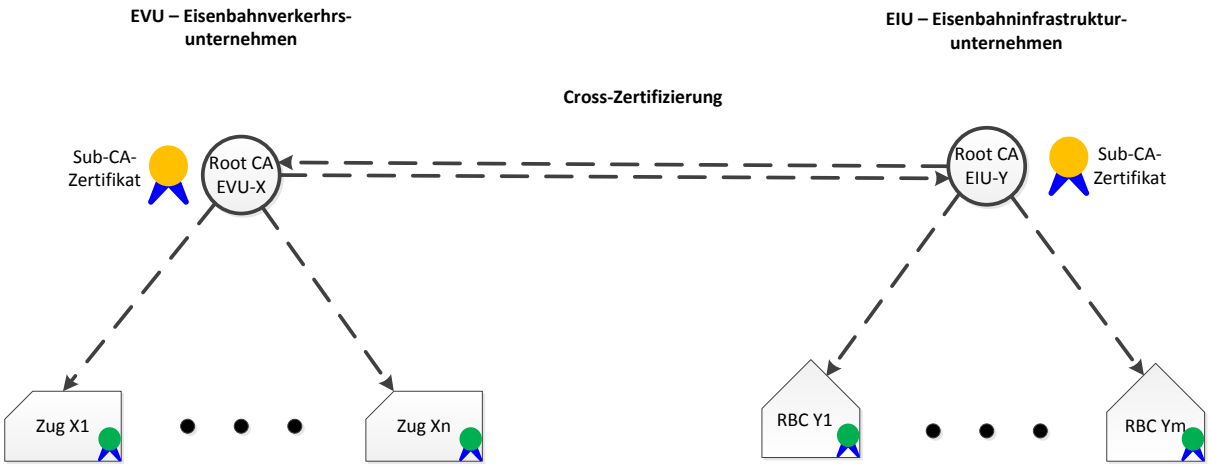
Nachteile der hierarchischen Architektur:

- Es werden unnötige Vertrauensverhältnisse geschaffen, die die Sicherheit des PKI-Systems mindern können.
- Eine zentrale CA auf europäischer Ebene lässt sich möglicherweise aus politischen Gründen schwer durchsetzen.

7.2.2 Flache PKI-Architektur

Eine Vertrauensbeziehung zwischen Zügen gleicher oder verschiedener EVU ist allerdings nicht notwendig. Dies wird von der hierarchischen Architektur zwar ermöglicht, aber eine solche Kommunikation findet im Allgemeinen nicht statt.

Diese erleichterten Anforderungen können durch eine flache PKI-Architektur erfüllt werden, wie folgt:



Es gibt keine zentrale Stelle der PKI auf EU-Ebene.

EIUs und EVUs haben ihre eigenen Root-CAs, die dafür eingesetzt werden, Zertifikate für eigene Züge bzw. für eigene RBCs zu erstellen. Die Root-CAs der einzelnen Eisenbahnunternehmen können sich je nach Bedarf gegenseitig zertifizieren.

Vertrauen wird nur zwischen Unternehmen aufgebaut, die auch Geschäftsbeziehungen haben.

Die Root-CAs der einzelnen Eisenbahnunternehmen sind besonders zu schützen, die im Regelbetrieb "offline" sind. Sie werden aktiviert, wenn die Zertifikate für Endgeräte erneuert werden müssen.

Vorteile der flachen Architektur:

- Keine zentrale Root-CA erforderlich, die politisch schwer durchsetzbar sein kann.
- Es werden keine unnötigen Vertrauensverhältnisse geschaffen, damit ist die Sicherheit des PKI-Systems höher.

Nachteile der flachen Architektur:

- Cross-Zertifizierungen müssen im Rahmen des Verfahrens der Etablierung des Netzzuganges zusätzlich entworfen und implementiert werden.
- Weniger skalierbar, die Cross-Zertifizierung braucht zusätzliche Arbeit und Dokumentation während des Verfahrens der Etablierung des Netzzuganges, und der Aufwand steigt mit der Anzahl der Geschäftsbeziehungen exponentiell.

7.2.3 Gemeinsamkeiten

Züge von EVUs und RBCs von EIUs können sich gegenseitig mit Zertifikaten authentifizieren, denn das Vertrauen wird in jedem Fall auf die Root-CA zurückgeführt:

- Züge von EVUs vertrauen Zertifikaten von RBCs von EIUs, deren Vertrauenskette auf die Root-CA zurückgeführt werden kann.
- RBCs von EIUs vertrauen Zertifikaten von Zügen von EVUs, deren Vertrauenskette auf die Root-CA zurückgeführt werden kann.
- RBCs von EIUs vertrauen Zertifikaten von RBCs von EIUs, deren Vertrauenskette auf die Root-CA zurückgeführt werden kann.

Es gibt keine zentrale Validation Authority, jedes Eisenbahnunternehmen betreibt seine eigene Validation Authority in Form eines OCSP-Responders, die durch das einheitliche Datennetz für alle anderen Eisenbahnunternehmen erreichbar ist, um die Gültigkeit von Zertifikaten überprüfen zu können

Über beide vorgeschlagenen Architekturen ist es möglich, Vertrauensbeziehungen Zug-Zug und RBC-RBC herzustellen, falls es nötig ist.

7.3 Anforderungen an Schlüssel und Zertifikate der PKI

7.3.1 Zertifikatsgültigkeit

Gültigkeitsbereich

Bei den symmetrischen Schlüsseln setzt die DB Netz AG auf eine 1:1-Beziehung der Entitäten Strecke und Fahrzeug: Für jede Kommunikationsbeziehung zwischen Infrastruktur (ETCS-Z) und Fahrzeug (EVC) wird ein eigener Schlüssel verwendet. Hiermit wird das Risiko der Kompromittierung in der Breite begrenzt.

Durch den Einsatz von asymmetrischen Schlüsseln und dem Verfahren der Online-Übertragung in Verbindung mit einer kurzen Gültigkeitsdauer des Zertifikats ließe sich diese Beziehung nach 1:n abwandeln: Ein einzelner Schlüssel ist für die Kommunikation eines Fahrzeugs mit der gesamten Infrastruktur vorgesehen. Dadurch sinkt auch der Aufwand für das Generieren und Verteilen der Schlüssel substanziell.

Gültigkeitsdauer

Die akzeptable Gültigkeitsdauer ist primär vom verwendeten Algorithmus und der Schlüssellänge abhängig. Sie sinkt stetig mit Zunahme der allgemein verfügbaren Rechenleistung (Mooresches Gesetz), wodurch das Ende der Zulässigkeit dieser Kombination vorhersagbar wird. Es müssen weitere Aspekte, wie beispielsweise die Anwendbarkeit der in Betracht kommenden Algorithmen oder die Verfügbarkeit einer Hardwareunterstützung, betrachtet werden.

Bei Verwendung einer Validation Authority, wie oben beschrieben, sollten die Zertifikate so lange wie möglich gültig sein.

Aufgrund steigender Rechenleistung ist anzunehmen, dass private Schlüssel bei gleichbleibender Schlüssellänge in der Zukunft berechnet werden können. Die Zertifikate sollten daher maximal so lange gültig sein, wie das Berechnen innerhalb ihrer Gültigkeitsdauer ausgeschlossen ist.

Es sind folgende Lebensdauern für Zertifikate anzunehmen:

- Zertifikat für Root die Root-CA: z.B. 10 Jahre
- Zertifikate für Sub-CAs: z.B. 5 Jahre
- Zertifikate für Endgeräte: Entsprechend einer durchzuführenden Risikoabschätzung, z.B. 1 Woche

7.3.2 Schlüssellängen

Alle Systeme müssen ein Ändern von Schlüssellänge und Algorithmus unterstützen. Daher müssen mindestens zwei Algorithmen gleichzeitig beherrscht werden, um auf Abruf (Schritt für Schritt oder in einer konzertierten Aktion) umgestellt werden zu können.

Wenn das Key Management System die Funktion der Sub-CA erfüllt, muss es die Erstellung von Zertifikaten und Zertifikat-Signierung durch die Hash-Algorithmen SHA-2 und SHA-3 unterstützen.

Das Key Management System muss Schlüssellängen verwalten können, die für die langfristige Bedienung der PKI benötigt wird, um die mit der Zeit evolvierenden Schlüssellängenempfehlungen vom BSI zu unterstützen.

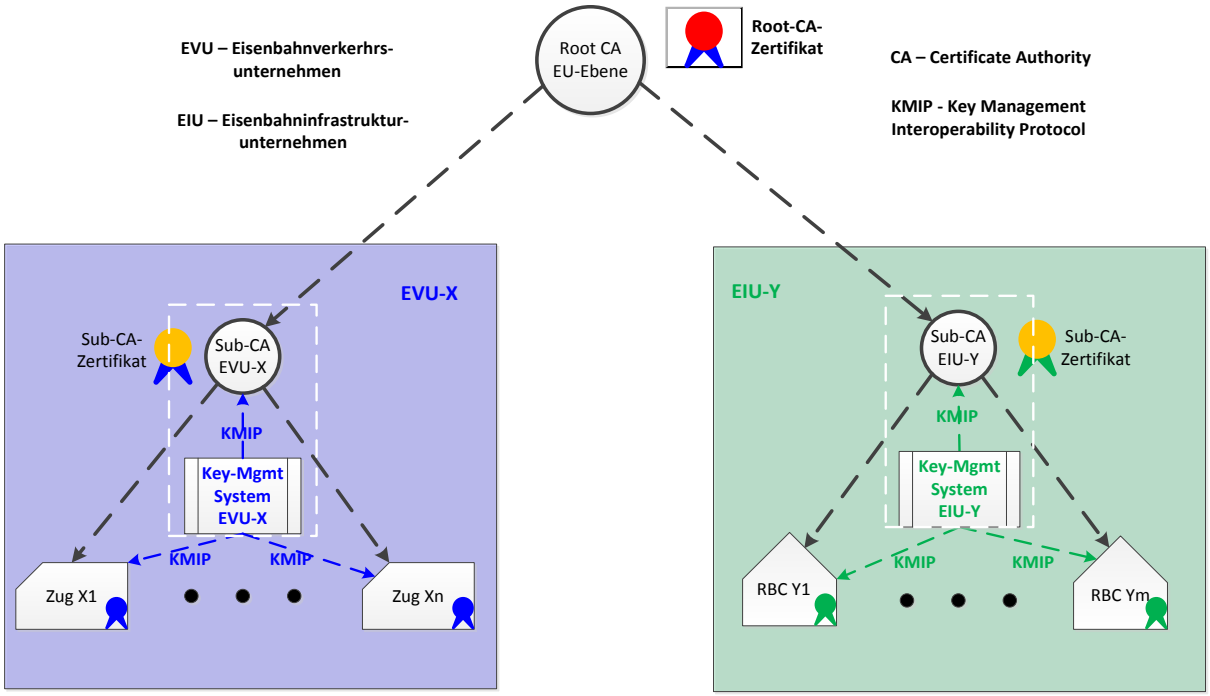
Für Schlüssellängen und Verfahren ist der jährliche BSI-Report [2] zu Grunde zu legen. Die Schlüssellänge ist jährlich hinsichtlich ihrer Sicherheit zu überprüfen.

7.4 Anforderungen an das Key Management System (KMS)

Aufgrund der Anforderungen an Häufigkeit des Schlüsseltausches muss ein skalierbares Key Management System aufgebaut und betrieben werden, das den automatisierten Tausch einer großen Menge von Schlüsseln und Zertifikaten innerhalb von kurzer Zeit erlaubt.

Jedes EVU und EIU muss über ein Key Management System verfügen, um die Vertraulichkeit ihrer gemanagten Schlüssel zu garantieren.

In der folgenden Abbildung wird ein möglicher Einsatz solcher Key Management Systeme dargestellt. Key Management Systeme können eine CA-Funktion enthalten, deshalb ist die Implementierung auch möglich, in der das Key Management System die Sub-CA-Funktion (oder in der flachen PKI-Architektur die Root-CA-Funktion) wahrnimmt.



7.4.1 Leistungsfähigkeit

Das Key Management System muss von seiner technischen Leistung her die entsprechend erwartete Anzahl zeitgleich gültiger Zertifikate verwalten können.

Für den Betrieb des Key Management Systems muss ein entsprechend leistungsfähiges Netzwerk zur Verfügung stehen, damit das KMS seine vielzähligen Kommunikationsbeziehungen und den Validierungs- und Verwaltungsverkehr unterstützen kann.

Endgeräte in einer PKI, die ihr PKI-Schlüsselpaar selbst generieren, müssen über die entsprechende Prozessorleistung verfügen.

7.4.2 Interoperabilität

Das Key Management System muss ein standardisiertes Schlüsselverwaltungsprotokoll, z.B. das Key Management Interoperability Protocol (KMIP) unterstützen.

Das KMIP ermöglicht die Kommunikation und Interoperabilität zwischen dem Key Management System und den Endgeräten verschiedener Hersteller während des Prozesses der Schlüsselverwaltung.

Daraus folgt, dass alle Endgeräte, wie Züge und RBCs, so implementiert werden müssen, dass diese auch das KMIP unterstützen.

7.4.3 Gestaltung der Sicherheit des Key Management Systems

Das Key Management System kann eine Hardware-Appliance sein, oder als vorkonfiguriertes virtualisiertes System funktionieren. In beiden Fällen muss die physische Sicherheit der Hardware Appliance oder des Virtualisierungshosts gegeben werden, um die Vertraulichkeit des Schlüsselmaterials zu garantieren.

Ein Vorteil eines virtualisierten Systems wäre, die Hochverfügbarkeit durch redundante Hosts zu gewährleisten.

Die Hardware-Appliance oder das vorkonfigurierte virtualisierte System müssen durch Konfiguration des Betriebssystems und der Anwendung gehärtet sein, um die Vertraulichkeit des Schlüsselmaterials zu garantieren.

Die Hardware-Appliance muss ein Hardware-Security-Modul (HSM) enthalten, um die Generierung, Speicherung, das Rotieren und die Vernichtung des Schlüsselmaterials (den Zyklus des Schlüsselmanagements) mit entsprechender Leistungsfähigkeit und Vertraulichkeit zu unterstützen.

Ein vorkonfiguriertes virtualisiertes System kann ein externes Hardware-Security-Modul für das Schlüsselmanagement nutzen, oder es kann die Funktionalität eines Hardware-Security-Modul in Software als virtuelle Instanz implementieren und nutzen.

Das Key Management System muss mindestens den Anforderungen des Security Level 3 des FIPS140-2 Standard von NIST [3] erfüllen, unabhängig davon, ob das KMS eine Hardware-Appliance oder ein vorkonfiguriertes virtualisiertes System ist.

7.4.4 Client-Zugriff

Das Key Management System muss den Client-Geräten (Endgeräten) die Möglichkeit anbieten, über mindestens eine der folgenden Methoden zu den Schlüsselmanagement-Funktionen des KMS zuzugreifen:

1. Durch einen Software-Agenten, der in den Endgeräten installiert und konfiguriert werden kann.
2. Durch ein standardisiertes Application-Programming-Interface (API)
3. Durch das standardisierte Protokoll KMIP

7.4.5 Schlüsselverwaltung im Key Management System

Das Key Management System muss den gesamten Zyklus des Key Managements unterstützen: Registrierung von Geräten oder Anlagen, Generierung, Speicherung, das Rotieren und die Vernichtung des Schlüsselmaterials.

7.4.6 Generierung und Speicherung von Schlüsseln im Key Management System

In der Industrie werden grundsätzlich zwei Arten von Key Management Systemen unterschieden:

- Ein KMS mit zentraler Schlüsselgenerierung und Speicherung
- Ein KMS mit dezentraler (lokaler) Schlüsselgenerierung und Speicherung

KMS mit zentraler Schlüsselgenerierung und Speicherung

In einem KMS mit zentraler Schlüsselgenerierung und Speicherung werden die privaten und öffentlichen Schlüsselpaare durch die zentrale Hardware und Software generiert und sicher in einem zentralen HSM oder TPM gespeichert.

Vorteile der zentralen Schlüsselgenerierung:

- Zentral ist mehr Rechenleistung und Speicherkapazität vorhanden
- Eine Änderung der Schlüsselparameter ist einfacher durchsetzbar

Nachteile der zentralen Schlüsselgenerierung:

- Die Schlüssel müssen sicher an die Client-Geräte transportiert werden
- Eine Kompromittierung eines zentralen Systems führt zur Kompromittierung aller Schlüssel

KMS mit dezentraler Schlüsselgenerierung und Speicherung

In einem KMS mit dezentraler Schlüsselgenerierung und Speicherung werden die privaten und öffentlichen Schlüsselpaare durch die lokale Hardware und Software generiert und sicher in einem lokalen HSM oder TPM gespeichert.

Die Vorteile der dezentralen Schlüsselgenerierung sind folgende:

- Die Schlüssel müssen nicht sicher transportiert werden
- Eine Kompromittierung eines lokalen Systems führt nicht zur Kompromittierung aller Schlüssel

In den beiden Lösungen sind folgende Voraussetzungen zu erfüllen:

- Das zentrale KMS muss besonders stark gehärtet und abgesichert werden, denn eine Kompromittierung des zentralen KMS führt zur Kompromittierung aller Schlüssel
- Sichere Speicher durch HSM oder TPM sind in den zentralen und lokalen Komponenten nötig
- Eine Client-Software (z.B. ein Agent des KMS) muss in den Client-Geräten installiert werden, um das übergreifende Schlüsselmanagement durch das KMS umsetzen zu können.
- Eine gesicherte Verbindung zwischen dem KMS und seinen Client-Geräten ist nötig.

7.4.7 Systemverwaltungsfunktionen

Das Key Management System muss eine rollenbasierte Zugangskontrolle ermöglichen.

Mindestens folgende Rollen müssen im Key Management System möglich sein:

1. System Admin – Verwaltung des Key Management Systems, wie z.B. Backup and Restore, ohne Zugriff auf das Schlüsselmaterial.
2. Application Manager – zuständig für die Verwaltung der Anwendung und des Schlüsselmaterials.
3. Das Key Management System muss die Funktion getrennter Rechte für Application Manager unterstützen. Alle Schlüsselfunktionen, die den Zugriff zu den Schlüsseln mit einbeziehen, dürfen nicht von einem einzelnen Manager durchgeführt werden können.
4. Audit und Reporting Manager– zuständig für Untersuchung und Analyse von System Reports und Ereignisprotokollen.

   Audit und Reporting muss folgende Funktionen beinhalten:

   - Ereignisprotokollierung und Reporting aller Zugriffe auf das Schlüsselmaterial
   - Ereignisprotokollierung und Reporting aller Schlüssel-Operationen, inklusive Generierung und Rotieren von Schlüsseln
   - Ereignisprotokollierung und Reporting aller administrativen Funktionen des Key Management Systems

8 Fazit

Im vorliegenden Dokument wurde der aktuelle Stand der IT Security von ETCS untersucht. Dazu wurden ausgewählte Angriffsvektoren identifiziert, analysiert und sinnvolle Maßnahmen beschrieben. Allen voran sind das Einführen einer Public-Key-Infrastruktur(PKI) als Grundlage für ein nachgelagert zu implementierenden Online-Keymanagements wichtige Faktoren zum Erhöhen der IT Security von ETCS.

9 Quellen

Ref. #	Titel	Datum / Version
[1]	Whitepaper CYSIS AG Security for Safety https://www.seceng.informatik.tu-darmstadt.de/media/seceng/ag_cysis/Whitepaper_Security_for_Safety.pdf	
[2]	BSI – Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102-1 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html	
[3]	FIPS 140-2 Sicherheitsanforderungen für kryptographische Module - Standard von NIST: https://csrc.nist.gov/publications/detail/fips/140/2/final	

10 Kontakt

Kontakt

Dr. Matthias Drodt, DB Netz AG, Mainzer Landstraße 205, 60326 Frankfurt a.M.
Telefon: 069 265 17502 | Mail: Matthias.Drodt@deutschebahn.com

Markus Heinrich, M.Sc., TU Darmstadt, Mornewegstr. 32, 64293 Darmstadt
Telefon: 06151 16 25631 | Mail: heinrich@seceng.informatik.tu-darmstadt.de

Weitere Informationen

Die Arbeitsgruppe „Cybersecurity für sicherheitskritische Infrastrukturen – CYSIS“ wurde am 25. Januar 2016 von der Deutschen Bahn AG und der TU Darmstadt im Rahmen der Innovationsallianz und des bestehenden DB RailLab gegründet. Ziel der AG ist es, den durch die Digitalisierung im Eisenbahnsektor gestiegenen Herausforderungen der Cybersecurity in sicherheitskritischen Infrastrukturen wirksam begegnen zu können.
Die AG Cybersecurity ist eine Basis für intensiven Informationsaustausch zwischen Industrie und Wissenschaft im Eisenbahnsektor, um von den gegenseitigen Erkenntnissen profitieren zu können. Mit Hilfe der Partner aus dem wissenschaftlichen Bereich, u.a. CYSEC, dem Profilbereich für Cybersicherheit an der TU Darmstadt, können effektive Abwehrtechniken und Gegenmaßnahmen erforscht und weiterentwickelt werden. Angestrebter Effekt ist die Vernetzung des Eisenbahnsektors mit der akademischen Forschung zum Thema Cybersecurity.

Webseite

www.seceng.tu-darmstadt.de/cysis