Handlungsempfehlung

Rahmenlastenheft für die Umsetzung der (((etiCORE Kontrolle inkl. MOTICS-NFC bis Mai 2028

Dateiname:	Handlungsempfehlung - Umsetzung der (((etiCORE Kontrolle.docx
Zuletzt geändert am:	14.10.2026 09:02
Version:	0.4
Ersteller:	D. Brinkmann
Abnahme am:	

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkung
0.1	D. Brinkmann (ETS)	19.08.2026	Ersterstellung
0.2	D. Brinkmann (ETS)	18.09.2026	Überführung in Lastenheft-Struktur, Kapitel 2 bis 6 ergänzt,
0.3	D. Brinkmann (ETS)	29.09.2026	Einarbeitung der Review-Kommentare
0.4	D. Brinkmann (ETS)	13.10.2026	Einarbeitung weiterer Kommentare und Textkorrektur

Inhaltsverzeichnis

Versionsverwaltung 2
1 Management Summary 5
2 Geltungsbereich und regulatorischer Rahmen 7
2.1 Zweck und Charakter dieses Dokuments 7
2.2 Adressaten und regulatorischer Rahmen 7
2.3 Migrationsfristen 8
2.4 Herleitung der Kontrollpflicht 9
2.5 Status MOTICS-NFC 9
3 (((etiCORE Kontrolle 10
3.1 Meilenstein 01.05.2028 10
3.1.1 Allgemeine Anforderungen an Dienstleister-Terminal 11
3.1.2 Funktionale Anforderungen an Dienstleister-Terminal 12
3.1.3 Hintergrundsystem des Dienstleisters 14
3.1.4 Anbindung an das ION 14
3.1.5 Hintergrundsystem des Produktverantwortlichen 15
3.1.6 Hintergrundsystem des Kundenvertragspartners 16
4 MOTICS-NFC 17
4.1 Gegenstand und Verbindlichkeit 17
4.2 Wirkung der Übertragungswege 17
4.3 Nachweise und Abnahme 17
4.4 Begründung der Aufnahme in den Beauftragungsumfang 18
5 Beauftragung und Projektdurchführung 19
5.1 Unternehmensspezifische Angaben 19
5.2 Anforderungen an Lieferumfang und Leistungen 20
5.3 Termine und Meilensteine 21

5.4 Kosten und Kalkulation 22
5.5 Gemeinsames Vorgehen mit anderen Verkehrsunternehmen 22
6 Anlagen und mitgeltende Dokumente 23
6.1 Hinweis zum Versionsstand 23
6.2 (((etiCORE-Spezifikation 23
6.3 Weiterhin gültige Dokumente der VDV-KA 24
6.4 Unterstützende Dokumente der VDV-ETS 24
6.5 Zugänge und Online-Quellen 24

1 Management Summary

Der technische Standard von (((eTicket Deutschland wird erneuert. Die VDV-Kernapplikation wird ab 2026 durch (((etiCORE abgelöst. Der Grund ist technisch: Die Zertifizierungsstellen der heutigen Sicherheitsinfrastruktur laufen Ende 2031 endgültig aus und können nicht verlängert werden. Gleichzeitig werden die bisherigen Verschlüsselungsverfahren auf ein zukunftsfähiges Verfahren umgestellt. Beides zusammen bedeutet: Die neue Version ist nicht abwärtskompatibel. Auch wenn es sich im Kern um ein Software-Update handelt, sind die Änderungen umfangreich.

Was das für Ihr Verkehrsunternehmen bedeutet: Auf Grundlage des Beschlusses der Teilnehmerversammlung vom 28.11.2024 müssen alle Verkehrsunternehmen, die Fahrgäste kontrollieren, ab dem 1. Mai 2028 Deutschlandtickets im (((etiCORE-Format prüfen können. Bis Ende 2031 können Kernapplikation und (((etiCORE parallel betrieben werden; danach steht die bisherige Technik nicht mehr zur Verfügung. Der Parallelbetrieb verschiebt den Stichtag im Mai 2028 also nicht, er betrifft nur die Frage, wie lange Bestandssysteme daneben weiterlaufen können. Unabhängig davon, wie die Tickets ausgegeben werden, müssen Systeme beide Ticketvarianten verarbeiten: das elektronische Ticket auf dem Nutzermedium ebenso wie die statische Berechtigung im Barcode.

Warum der Zeitpunkt jetzt drängt: Zwischen der Beauftragung von Systemherstellern und dem einsatzfähigen Gerät liegen Entwicklung, Zertifizierung und Rollout. Rechnet man diese Schritte vom Stichtag zurück, ist der Zeitpunkt für die Beauftragung erreicht. Wer erst 2027 beginnt, gerät bei der Zertifizierung und beim flächendeckenden Ausbringen in Verzug. Deshalb ist jetzt zu prüfen, ob vorhandene Kontrollsysteme per Update ertüchtigt werden können oder ob eine Neubeschaffung ansteht.

Unsere Empfehlung: MOTICS-NFC gleich mitbeauftragen. Die Kontrolle des MOTICS-Kopierschutzes im Barcode ist für das Deutschlandticket bereits seit dem 01.01.2026 Pflicht. Damit entfällt die zwingende Prüfung des ID-Mediums als Kopierschutz. Für die Prüfung über NFC gibt es bislang keinen verbindlichen Umsetzungstermin. Aus wirtschaftlicher Sicht und mit Blick auf den Investitionsschutz empfehlen wir dennoch dringend, MOTICS-NFC zusammen mit der (((etiCORE-Umstellung zu beauftragen.

Der Hintergrund: Beim MOTICS-Barcode ersetzt ein Zeitstempel die Rückfrage des Dienstleister-Terminal. Der angezeigte Barcode wird deshalb innerhalb einer Toleranzfrist akzeptiert und kann in dieser Zeit per Screenshot oder Live-Übertragung an ein anderes Gerät weitergegeben werden. Über NFC sendet das Dienstleister-Terminal dagegen eine eigene Zufallsanfrage, die nur das Gerät beantworten kann, an das das Ticket gebunden ist. Gegenüber dem Barcode ergeben sich daraus folgende Vorteile:

- **Mehr Sicherheit:** Ein Ticket lässt sich nicht mehr per Screenshot oder Bildübertragung weitergeben.

- **Mehr Tempo:** Der Fahrgast hält sein Smartphone an das Dienstleister-Terminal, statt den Barcode auf dem Display auszurichten.
- **Geringer Zusatzaufwand:** MOTICS-NFC setzt auf derselben Datenstruktur auf wie die (((etiCORE-Chipkarte, deren Kontrolle bis Mai 2028 ohnehin umzusetzen ist.
- **Robustheit:** Die Kontrolle über NFC hängt nicht vom Zustand des Displays ab. Ein gesprungenes Display, geringe Helligkeit oder direktes Sonnenlicht verhindern das Auslesen nicht.

Entscheidend ist der Beauftragungszeitpunkt: Beide Themen betreffen dieselben Geräte und dieselbe Software. Werden sie gemeinsam beauftragt, fallen Entwicklung, Test, Zertifizierung und Rollout einmal an. Eine spätere separate Beauftragung löst denselben Zyklus ein zweites Mal aus und verursacht vermeidbare Zusatzkosten.

Was jetzt zu tun ist: Prüfen Sie den Umstellungsbedarf Ihrer Kontrollsysteme und sprechen Sie zeitnah mit Ihrem Systemhersteller. Die Kapitel 3 bis 5 enthalten die Anforderungen an Terminals, Hintergrundsystem und Projektdurchführung in einer Form, die als Grundlage für Ausschreibung und Beauftragung übernommen werden kann.

2 Geltungsbereich und regulatorischer Rahmen

2.1 Zweck und Charakter dieses Dokuments

Dieses Dokument hat den Charakter eines Rahmenlastenhefts. Es fasst die Anforderungen zusammen, die ein Verkehrsunternehmen in seiner Rolle als Dienstleister (Service-Operator) erfüllen muss, um Berechtigungen im (((etiCORE-Format kontrollieren zu können, und stellt sie in einer Form dar, die in eine Ausschreibung oder Beauftragung übernommen werden kann.

Das Dokument ersetzt weder die (((etiCORE-Spezifikation noch das (((eTicket-Regelwerk und begründet keine über die bestehenden Verpflichtungen hinausgehenden Anforderungen. Verbindlich bleiben allein:

- die (((etiCORE-Spezifikation in ihrer jeweils gültigen Fassung,
- das (((eTicket-Regelwerk einschließlich seiner Anlagen,
- der Teilnehmervertrag,
- die Beschlüsse der Teilnehmerversammlung.

Die Anforderungen in den Kapiteln 3 bis 5 sind durchnummeriert und können als Textbausteine in die eigenen Vergabeunterlagen übernommen werden. Jede Anforderung ist mit einer Stufe und mit ihrer Grundlage gekennzeichnet.

Stufe	Bedeutung	Erläuterung
M	Muss-Anforderung	Ergibt sich aus dem Beschluss der Teilnehmerversammlung oder unmittelbar aus der (((etiCORE-Spezifikation. Ohne Erfüllung ist die Kontrollfähigkeit zum 01.05.2028 nicht gegeben.
S	Soll-Anforderung	Von der VDV-ETS empfohlen, jedoch nicht verpflichtend. Die Aufnahme in die Beauftragung liegt im Ermessen des Verkehrsunternehmens.
I	Information	Nachrichtlicher Hinweis ohne Anforderungscharakter, etwa zu angrenzenden Rollen.

Die unternehmensspezifischen Angaben, die ein Lastenheft zusätzlich enthalten muss, sind in Kapitel 5.1 als Vorlage angelegt und vom Verkehrsunternehmen zu ergänzen. Die Kapitel 1 und 2 dienen der Einordnung und werden für die Beauftragung nicht benötigt.

2.2 Adressaten und regulatorischer Rahmen

Das Dokument richtet sich an Verkehrsunternehmen und Verkehrsverbünde in ihrer Rolle als Dienstleister (Service-Operator), also an diejenigen Teilnehmer, die Berechtigungen kontrollieren. Angesprochen sind sowohl die Entscheidungsebene, die Beauftragungen auslöst, als auch die fachlich

Verantwortlichen für Kontrollsysteme und Hintergrundsysteme. Mittelbarer Adressat ist der Systemhersteller, dem die Anforderungen aus diesem Dokument übergeben werden.

Nicht Gegenstand dieses Dokuments ist die Vertriebsseite. Die Ausgabe von Berechtigungen im (((etiCORE-Format erfordert erheblich mehr Funktionalität und wird an anderer Stelle behandelt.

Regelwerk und Teilnehmervertrag bleiben für (((etiCORE im Grundsatz unverändert. Damit gelten die bestehenden Pflichten fort, insbesondere die Vorgabe aus Anlage 1 des (((eTicket-Regelwerks, dass ausschließlich zertifizierte Komponenten eingesetzt werden dürfen. Vor dem Hintergrund deutschlandweit gültiger Tickets gewinnt die Zertifizierung zusätzlich an Bedeutung.

Die technische Verbindlichkeit ergibt sich aus der Spezifikation, die organisatorische aus Regelwerk und Teilnehmervertrag, die terminliche aus dem Beschluss der Teilnehmerversammlung.

2.3 Migrationsfristen

Termin	Bedeutung
12/2026	Bereitstellung der zentralen Systeme. Die Sicherheitsinfrastruktur des (((eTicket Deutschland wird auf die zweite Generation (2GSI) umgestellt; (((etiCORE wird mit allen aktualisierten Hintergrundsystemen in Betrieb genommen.
05/2028	Stichtag für die Kontrollfähigkeit. Nach Beschluss der Teilnehmerversammlung muss jeder Teilnehmer bis dahin seine Kontrollsysteme auf (((etiCORE angepasst haben
09/2028	Ende der Laufzeit des Rahmenvertrags für KA-1.X-Chipkarten. Bis dahin können Chipkarten nach dem bisherigen Standard bezogen werden.
12/2031	Abschaltung der KA. Die Root- und Sub-CA-Zertifikate der VDV-Kernapplikation laufen endgültig aus und können nicht erneuert werden. Damit endet der Betrieb der KA-Systemlandschaft.

Zwischen 2026 und 2031 laufen beide Standards im Parallelbetrieb. Dieser Parallelbetrieb verschiebt den Stichtag im Mai 2028 nicht, er bestimmt lediglich, wie lange Bestandssysteme daneben weiterbetrieben werden dürfen.

VDV-ETS empfiehlt, die Übergangsphase möglichst kurz zu halten. Der parallele Betrieb zweier Infrastrukturen bindet über die gesamte Dauer zusätzliche Betriebskosten. Die maximal mögliche Dauer bis Ende 2031 auszuschöpfen, ist nicht zu empfehlen. Es sollte dringend ein ausreichender zeitlicher Puffer zur Deadline – 01.12.2031 – eingerichtet werden, um auf unvorhergesehene Ereignisse reagieren zu können.

2.4 Herleitung der Kontrollpflicht

Die Kontrollfähigkeit muss der Ausgabe vorausgehen. Solange deutschlandweit gültige Tickets im Umlauf sind, muss die Kontrollfähigkeit bundesweit hergestellt sein, bevor die ersten Vertriebssysteme Nutzermedien oder Berechtigungen im (((etiCORE-Format ausgeben. Andernfalls entstünden Berechtigungen, die außerhalb des ausgebenden Verbundes nicht geprüft werden könnten.

Genau aus dieser Reihenfolge folgt die Notwendigkeit eines bundesweit einheitlichen Termins. Ein einzelnes Unternehmen kann die Kontrollfähigkeit nicht für sich allein herstellen, sie wirkt nur, wenn alle Teilnehmer sie zum selben Zeitpunkt erreicht haben. Die Teilnehmerversammlung hat diesen Termin deshalb auf den 01.05.2028 festgelegt.

2.5 Status MOTICS-NFC

Die Spezifikationen zu MOTICS-NFC hat die Teilnehmerversammlung beschlossen. Nicht beschlossen ist ein verbindlicher Termin, bis zu dem die Prüfung über NFC auf der Kontrollseite umgesetzt sein muss. Es besteht damit keine Verpflichtung, MOTICS-NFC bis zum 01.05.2028 umzusetzen. Die Aussagen dieses Dokuments zur Umsetzung von MOTICS-NFC sind deshalb Empfehlungen. Sie beruhen auf wirtschaftlichen Erwägungen und auf dem Ziel der Einnahmensicherung, nicht auf einer regulatorischen Verpflichtung.

Davon zu unterscheiden ist die Kontrolle des MOTICS-Kopierschutzes selbst. Sie ist nicht optional: Für den MOTICS-Barcode besteht die Pflicht zur Kontrolle beim Deutschlandticket bereits seit dem 01.01.2026, und die zum 01.05.2028 umzusetzende Ausbauvariante „D-Ticket Full" enthält die Kontrolle des MOTICS-Kopierschutzes als festen Bestandteil. Über welchen Übertragungsweg geprüft wird, gibt die Ausbauvariante nicht vor. Verpflichtend ist damit die Kontrolle des MOTICS-Kopierschutzes, empfohlen die zusätzliche Prüfung über NFC. Die Anforderungen finden sich in Kapitel 3, die Abgrenzung zwischen den Übertragungswegen in Kapitel 4.

3 (((etiCORE Kontrolle

Bevor eine interoperable Berechtigung im (((etiCORE-Format ausgegeben werden kann, muss der Meilenstein in Kap 3.1 erfüllt sein. Kapitel 3.1beschreibt die Mindestanforderungen an die Komponenten für die Kontrolle. Die Ausgabe einer (((etiCORE-Berechtigung erfordert sehr viel mehr Funktionalität, insbesondere wenn zur Ausbauvariante „D-Ticket Full“ noch das optionale Aktionsmanagement eingesetzt wird. Das ist aber nicht Bestandteil dieses Dokuments.

Das Aktionsmanagement (Ordered Action Management) ist der Rolle des ausführenden Customer Contract Partners zugeordnet, nicht dem Dienstleister (Service-Operator). Die SPEC-SO-RT sieht für das Dienstleister-Terminal keine Anwendungsfälle des Aktionsmanagements vor. Für die reine Kontrolle ergeben sich daraus keine zusätzlichen Anforderungen. Übernimmt dieselbe Hardware jedoch auch die Rolle eines ausführenden Customer Contract Partners, sieht die (((etiCORE-Spezifikation dafür eine eigene Ausbauvariante vor, die den Dienstleister mit der Aktionsausführung kombiniert (SPEC-MAIN Kap. 6.5). In diesem Fall wird empfohlen, die Aktionsausführung gleich mit zu beauftragen, da sie dieselben Geräte betrifft. Zu beachten ist, dass die Aktionsausführung ein Hardware-SAM voraussetzt (siehe Anforderung LF-09).

3.1 Meilenstein 01.05.2028

Für diesen Meilenstein müssen für die Kontrolle die Funktionen aus der Ausbauvariante (Deployment Variant) „D-Ticket Full“ umgesetzt werden. In erster Linie geht es um das Deutschlandticket oder ähnliche interoperable Tickets.

Hintergrund ist, dass erst nach Erreichen dieses Meilensteins interoperable Tickets im (((etiCORE-Format Erst nach Erreichen dieses Meilensteins können interoperable Tickets im (((etiCORE-Format ausgegeben werden, weil sie erst dann flächendeckend kontrolliert werden können.

Aufgrund der Funktionalität in dieser Ausbauvariante ergeben sich bestimmte Anforderungen in den Systemkomponenten, die nachfolgend aufgeführt sind.

Die Ausbauvariante „D-Ticket Full" enthält neben der Kontrolle von Berechtigungen auf Chipkarten auch die Kontrolle statischer Berechtigungen, mit und ohne MOTICS-Kopierschutz. Über welchen Übertragungsweg der Kopierschutz geprüft wird, gibt die Ausbauvariante nicht vor (siehe Kapitel 4).

3.1.1 Allgemeine Anforderungen an Dienstleister-Terminal

Die folgenden Anforderungen gelten für alle Terminals in (((etiCORE unabhängig von der Ausbauvariante. Sie betreffen Hardware, Konformität und Zertifizierung und sind damit Voraussetzung für die funktionalen Anforderungen des folgenden Abschnitts.

ID	Anforderung	Stufe	Grundlage
SO-T-01	Das Terminal muss über ein Zertifikat zum Nachweis seiner (((etiCORE-Funktionalität verfügen, ausgestellt durch das von VDV-ETS akkreditierte Prüflabor.	M	SPEC-SO-RT Kap. 3.2
SO-T-02	Das Terminal muss über geeignete Schnittstellen für die Datenver- und -entsorgung aus seinem Hintergrundsystem verfügen. Der Datenaustausch muss gemäß den in (((etiCORE spezifizierten Schnittstellen gesichert stattfinden. Wird die Ausführungseinheit getrennt von der Steuerungseinheit betrieben, gilt an dieser Schnittstelle zusätzlich SPEC-EUI.	M	SPEC-SO-RT Kap. 3.2.1
SO-T-03	Für das Terminal muss eine Konformitätsbescheinigung zur Typenprüfung nach dem Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) vorliegen. Der Hersteller muss eine EU-Konformitätserklärung nach Artikel 18 der RE Directive (2014/53/EU) beibringen, die für RFID-Komponenten mindestens ETSI EN 300 330, ETSI EN 301 489-1 und -3 sowie EN 60950 bzw. EN 62368 umfasst.	M	SPEC-SO-RT Kap. 3.2.2
SO-T-04	Das Terminal muss die Installation von Hardware-SAMs ermöglichen, sofern nicht ausschließlich ein Light-SAM verwendet wird, und mindestens zwei Steckplätze für Hardware-SAMs bereitstellen. Die Terminal-Software muss die SAMs entsprechend steuern können.	M	SPEC-SO-RT Kap. 3.2.3
SO-T-05	Die Manipulationssicherheit gemäß ISO 13491 muss gewährleistet sein, insbesondere Spannungs- und damit Datenverlust beim Entfernen des SAM.	M	SPEC-SO-RT Kap. 3.2.3
SO-T-06	Das Terminal muss über eine Leseeinrichtung verfügen, die alle Anforderungen gemäß ISO/IEC 14443 erfüllt. Es müssen Kommunikationsschnittstellen sowohl für Typ-A- als auch für Typ-B-Medien bereitgehalten werden. Die Mindest-Lesereichweite beträgt 1 cm. Mit Hilfe von Kollisionserkennung sollen Probleme mit mehreren Medien im Lesefeld vermieden werden.	M	SPEC-SO-RT Kap. 3.2.4
SO-T-07	Das Nutzermedium kann während der Startphase WTX-Kommandos absetzen, die das Terminal berücksichtigen muss. Bei Kommunikationsproblemen darf der Kartenleser während des WTX-Zeitfensters keinen erneuten Verbindungsaufbau versuchen, sondern soll die Kommunikation wiederherstellen und die Applikation ausführen.	I	SPEC-SO-RT Kap. 3.2.4 (dort als Hinweis gekennzeichnet)
SO-T-08	Für den Leser muss ein beglaubigtes Gutachten einer akkreditierten Zertifizierungsstelle vorliegen, das die standardgerechte Ausführung gemäß ISO/IEC 14443 nachweist.	M	SPEC-SO-RT Kap. 3.2.4

ID	Anforderung	Stufe	Grundlage
SO-T-09	Ist die Eingabe des persönlichen Passworts zum Lesen persönlicher Daten erforderlich, muss die Tastatur die Ziffern 0 bis 9 enthalten. Es muss verhindert werden, dass ein Angreifer die Tastatur manipulieren und das Passwort während der Eingabe abhören kann.	M	SPEC-SO-RT Kap. 3.2.6
SO-T-10	Ändert sich die Terminalbezeichnung, der Typ oder die Einbauposition des Nutzermedium-Lesers, das SAM-Interface oder die (((etiCORE-Version einschließlich Funktionserweiterungen aus der Releasefortschreibung, ist eine erneute Zertifizierung erforderlich.	M	SPEC-SO-RT Kap. 3.2.5
SO-T-11	Bei Software-Updates, die keinen (((etiCORE-Anwendungsfall betreffen, muss der Hersteller eine Eigenerklärung vorlegen, dass die Änderungen die im Prüflabor geprüften (((etiCORE-Anwendungsfälle nicht beeinträchtigen. Diese Eigenerklärung ist dem Verkehrsunternehmen bei Kauf oder Update unaufgefordert vorzulegen.	M	SPEC-SO-RT Kap. 3.2.5
SO-T-12	Tritt im Betrieb eines bereits zertifizierten Terminals ein Fehler auf, ist eine Nachprüfung erforderlich. Dabei wird immer der bei der Erstprüfung zugrunde gelegte (((etiCORE-Funktionsumfang erneut geprüft.	M	SPEC-SO-RT Kap. 3.2.5
SO-T-13	Bei Zusammenbruch der Spannungsversorgung muss das Terminal alle Aktionen unterbrechen, seinen aktuellen Status speichern und bei Wiederinbetriebnahme mit dem gespeicherten Datenbestand aufsetzen; der Vorgang ist zu protokollieren. Treten Fehler oder Beschädigungen auf, muss die Rekonstruktion der Zählerstände aus der letzten Datenübernahme möglich sein. Der Anbieter hat hierzu ein Konzept zu erläutern und zu realisieren.	M	SPEC-SO-RT Kap. 3.2.7
SO-T-14	Die Bediener- und Kundenschnittstelle muss in Aufbau, Optik und Bedienung dem Kapitel „Terminal-Benutzer-Schnittstelle“ entsprechen und auch für Hör- und Sehgeschädigte sichergestellt sein. Das Piktogramm für die Antennenfläche ist so auf der Leserfläche aufzubringen, dass die optimale Leseposition des Nutzermediums gekennzeichnet ist.	M	SPEC-SO-RT Kap. 3.2.8 und Kap. 4
SO-T-15	Das Terminal muss über eine Echtzeituhr einschließlich Datumsfunktion verfügen; die Zeitabweichung darf 2 Minuten pro Jahr nicht überschreiten.	M	SPEC-SO-RT Kap. 3.2.8
SO-T-16	Die zyklische Aktualisierung der Hotlists muss gewährleistet sein, in der Regel mindestens einmal täglich.	M	SPEC-SO-RT Kap. 3.2.8

3.1.2 Funktionale Anforderungen an Dienstleister-Terminal

Für die Kontrolle von Berechtigungen auf Chipkarten gelten die folgenden Anforderungen an das Dienstleister-Terminal:

ID	Anforderung	Stufe	Grundlage
SO-T-17	Das Terminal muss für (((etiCORE konfigurierbar sein. Dazu gehören insbesondere das CA-Zertifikatsrepository und die Revocationliste für CV-Zertifikate.	M	SPEC-SO-RT Kap. 6.2.1, 6.2.7, 6.2.8
SO-T-18	Das Terminal muss erkennen, ob eine KA- oder eine (((etiCORE-Berechtigung vorliegt, und intern die zugehörige Software-Komponente sowie das zugehörige SAM ansprechen.	M	(((etiCORE Leitfaden Kap. 4.1, 7.2; (((etiCORE Migration und Parallelbetrieb, Kap. 2.3.10
SO-T-19	Das Terminal muss die KA-Sperrlisten und die (((etiCORE-Hotlisten verarbeiten und in der Vorprüfung anwenden. Bei einem Treffer muss es die Applikation oder Berechtigung ablehnen oder sperren können.	M	SPEC-SO-RT Kap. 3.2.8, 6.2.4, 9.2.1
SO-T-20	Das Terminal muss Sperrnachweise für Applikationen und Berechtigungen erzeugen und an das zuständige Hintergrundsystem übermitteln.	M	SPEC-SO-RT Kap. 8.2.5, 8.2.6
SO-T-21	Das Terminal muss die Kontrolle einer (((etiCORE-Berechtigung unter Verwendung eines (((etiCORE-SAM durchführen und die Kommunikation zwischen Chipkarte und SAM nach (((etiCORE unterstützen.	M	SPEC-SO-RT Kap. 9.2.1, 10.2.1; SPEC-SAM Kap. 5
SO-T-22	Das Terminal muss Kontrollnachweise im (((etiCORE-Format erzeugen und an das zuständige Hintergrundsystem übermitteln.	M	SPEC-SO-RT Kap. 10.2.2

Für die Kontrolle statischer Berechtigungen gelten die folgenden Anforderungen:

ID	Anforderung	Stufe	Grundlage
SO-T-23	Das Terminal muss beide Formate der statischen Berechtigung verarbeiten können: den 2D-Barcode über die optische Schnittstelle und die binäre Struktur über NFC.	M	SPEC-MAIN Kap. 9.2.21
SO-T-24	Das Terminal muss statische Berechtigungen und MOTICS-Applikationen gegen die Hotlisten prüfen und bei einem Treffer ablehnen.	M	SPEC-SO-RT Kap. 6.2.4, 17.2.1; SPEC-MAIN Kap. 9.2.21
SO-T-25	Das Terminal muss ein Nutzermedium ohne Chip-Applikation prüfen. Dazu gehören die Prüfung der MOTICS-Anforderungen, soweit zutreffend, und die Prüfung der statischen Berechtigungen.	M	SPEC-SO-RT Kap. 17.2.1
SO-T-26	Das Terminal muss den MOTICS-Kopierschutz prüfen. Der Übertragungsweg ist durch die Ausbauvariante nicht vorgegeben; die Prüfung über NFC behandelt Kapitel 4.	M	SPEC-SO-RT Kap. 17.2.4
SO-T-27	Das Terminal muss Kontrollnachweise für statische Berechtigungen an das zuständige Hintergrundsystem übermitteln.	M	SPEC-SO-RT Kap. 17.2.2, 17.2.3

Übergreifend gilt für beide Kontrollarten:

ID	Anforderung	Stufe	Grundlage
SO-T-28	Bei nutzermediumbasierten Prozessen muss das Terminal die Prozessinstanz-ID vergeben und in der Nachricht an	M	SPEC-ION Kap. 7.4.1.3

ID	Anforderung	Stufe	Grundlage
	das Hintergrundsystem übertragen. Das Hintergrundsystem verwendet sie für alle weiteren Nachrichten desselben Prozesses.		

3.1.3 Hintergrundsystem des Dienstleisters

Für das Hintergrundsystem des DIenstleisters gelten die folgenden Anforderungen:

ID	Anforderung	Stufe	Grundlage
SO-S-01	Das Hintergrundsystem muss für (((etiCORE konfigurierbar sein, einschließlich Hotlisten und Zertifikaten.	M	SPEC-SO-RS Kap. 5.2.5, 5.2.6, 5.2.16, 6.2.3
SO-S-02	Das Hintergrundsystem muss Sperrnachweise entgegennehmen und auswerten.	M	SPEC-SO-RS Kap. 8.2.3, 8.2.4
SO-S-03	Das Hintergrundsystem muss Kontrollnachweise entgegennehmen und auswerten.	M	SPEC-SO-RS Kap. 9.2.1, 16.2.1
SO-S-04	Das Hintergrundsystem muss Sperr- und Kontrollnachweise über das ION im neuen Nachrichtenformat an das zuständige Product-Owner-System weiterleiten.	M	SPEC-SO-RS Kap. 9.2.1, 16.2.1; SPEC-ION Kap. 7.4.1

3.1.4 Anbindung an das ION

Sperr- und Kontrollnachweise werden über das Interoperabilitätsnetzwerk (ION) ausgetauscht. Die folgenden Anforderungen gelten für das Hintergrundsystem des Dienstleisters an dieser Schnittstelle.

ID	Anforderung	Stufe	Grundlage
SO-S-05	Die Transportsicherung zwischen Teilnehmersystem und zentraler Vermittlungsstelle muss über TLS mit beidseitiger Authentifizierung erfolgen. Eingesetzt werden X.509v3-Zertifikate mit dem Schlüsselalgorithmus RSASSA-PSS und einer Schlüssellänge von 2048 Bit.	M	SPEC-ION Kap. 7.4.1.1.6
SO-S-06	Zusätzlich zur Transportsicherung müssen die Nachrichteninhalte im SOAP Body zwischen Sender- und Empfängerorganisation Ende-zu-Ende signiert und verschlüsselt werden.	M	SPEC-ION Kap. 7.5
SO-S-07	Als Algorithmensuite der Webservice Security ist Basic256Sha256 einzusetzen.	M	SPEC-ION Kap. 7.5.2.1
SO-S-08	Das System muss strikt entweder für Level-2 (Integrationstest) oder für Level-3 (Produktion) konfiguriert und in Betrieb sein. Schlüssel und Zertifikate der jeweils anderen Umgebung dürfen nicht verwendet werden.	M	SPEC-ION Kap. 7.5.1.1
SO-S-09	Die verwendeten Zertifikate müssen regelmäßig gegen die Sperrlisten der PKI geprüft werden, einschließlich der zugehörigen Sub-CA- und Root-CA-Zertifikate.	M	SPEC-ION Kap. 7.4.1.1.5
SO-S-10	Bei sicherheitsrelevanten Fehlern darf das System keine internen Informationen liefern, die auf Sicherheitsprobleme hinweisen. Das Verhalten muss	M	SPEC-ION Kap. 7.4.1.1.7

ID	Anforderung	Stufe	Grundlage
	ressourcenschonend sein, in der Regel Log-Eintrag, gegebenenfalls Alarm und HTTP-Fehlercode.		
SO-S-11	Die automatische Schemavalidierung muss für eingehende und für ausgehende Nachrichten aktiviert sein. Eine ausgehende Nachricht mit fehlerhafter Syntax darf nicht gesendet werden.	M	SPEC-ION Kap. 7.4.1.9 bis 7.4.1.11
SO-S-12	Das System muss die Übereinstimmung von Kommunikations-Header und Transaktions-Header prüfen. Absender-ID, Rolle des Senders, Transaktions-ID und Zeitstempel der Transaktion müssen denselben Wert haben.	M	SPEC-ION Kap. 7.4.1.12
SO-S-13	Jede ION-Nachricht muss in der gesamten ION-Umgebung eindeutig sein. Die Kennung setzt sich zusammen aus Organisations-ID und Rollen-ID des Systemeigentümers, dem Namen des implementierten Dienstes und einer fortlaufenden Nummer.	M	SPEC-ION Kap. 7.4.1.15
SO-S-14	Das System muss asynchrone Nachrichten annehmen, solange sie authentisch, entschlüsselbar und syntaktisch korrekt sind. Fachliche Fehler sind als BusinessException in der Antwort zu übermitteln, nicht als SOAP-Fault.	M	SPEC-ION Kap. 7.4.1.7
SO-S-15	Das System muss die Rollenautorisierung sicherstellen und dazu die Zuordnung von Organisation und Rollen regelmäßig vom Registrar anfordern.	M	SPEC-ION Kap. 7.4.1.14
SO-S-16	Die maximale Größe von Nachrichten, die in eine Queue gestellt werden können, darf 16 MB nicht überschreiten.	M	SPEC-ION Kap. 7.4.1.5
SO-S-17	Wo die Spezifikation es vorsieht, muss das System Listeninhalte nach dem ZIP-Standard komprimieren und Base64-kodiert übertragen sowie empfangene Listen entsprechend dekodieren und entpacken.	M	SPEC-ION Kap. 7.4.1.6
SO-S-18	Für alle geschäftlichen Anfragen und Antworten mit Webservice Security ist MTOM verpflichtend. Als SOAP-Version wird SOAP 1.1 verwendet.	M	SPEC-ION Kap. 7.4.1.16, 7.4.1.17

3.1.5 Hintergrundsystem des Produktverantwortlichen

Die folgenden beiden Abschnitte betreffen Systeme anderer Rollen. Sie sind nachrichtlich aufgeführt, weil die Nachrichten des Dienstleisters dort weiterverarbeitet werden, und begründen keine Anforderungen an das Verkehrsunternehmen in der Rolle des Dienstleisters.

Das Hintergrundsystem des Produktverantwortlichen muss im Rahmen der Kontrolle folgende Grundfunktionen erfüllen:

- Grundkonfiguration für (((etiCORE inklusive Hotlists und Zertifikaten
- Entgegennahme und Auswertung von Sperrnachweisen
- Entgegennahme und Auswertung von Kontrollnachweisen
- Sperrwesen und Sperranforderungen für (((etiCORE-Hotlists im Rahmen des Monitorings

- Weiterleitung von Sperr- und Kontrollnachweisen an das zuständige Customer Contract Partner System über das ION mit neuem Nachrichtenformat

3.1.6 Hintergrundsystem des Kundenvertragspartners

Das Hintergrundsystem des Kundenvertragspartners (Customer-Contract-Partners muss im Rahmen der Kontrolle folgende Grundfunktionen erfüllen:

- Grundkonfiguration für (((etiCORE inklusive Hotlists und Zertifikaten
- Entgegennahme und Auswertung von Sperrnachweisen
- Entgegennahme und Auswertung von Kontrollnachweisen
- Entgegennahme von Sperranforderungen für (((etiCORE-Hotlists im Rahmen des Monitorings
- Aufträge und Freigaben für Hotlisteinträge von Applikationen und Berechtigungen

4 MOTICS-NFC

4.1 Gegenstand und Verbindlichkeit

MOTICS (Mobile Ticketing Crypto Service) bindet eine statische Berechtigung kryptographisch an das Endgerät, auf dem sie ausgegeben wurde. Die Bindung wird bei der Kontrolle automatisiert nachgewiesen. Damit entfällt die zwingende Prüfung eines Ausweisdokumentes um den Kopierschutz sicherzustellen. Im Sinne einer tarifliche Prüfung bleibt der Abgleich mit einem Ausweisdokument bei personengebundenen Tickets erhalten, kann aber auf Stichproben reduziert werden.

Die Kontrolle des MOTICS-Kopierschutzes ist Bestandteil der Ausbauvariante „D-Ticket Full" und damit Pflicht (Anforderung SO-T-26). Nicht vorgegeben ist der Übertragungsweg. Die Spezifikationen zur Prüfung über NFC hat die Teilnehmerversammlung beschlossen; ein verbindlicher Umsetzungstermin besteht nicht (siehe Kapitel 2.5).

4.2 Wirkung der Übertragungswege

Eine statische Berechtigung kann als 2D-Barcode über die optische Schnittstelle oder über NFC übertragen werden. Für die Schutzwirkung kommt es darauf an, ob die Berechtigung mit MOTICS-Kopierschutz ausgegeben wurde und über welchen Weg sie kontrolliert wird:

Merkmal	VDV-Barcode ohne MOTICS	MOTICS-Barcode (optisch)	MOTICS-NFC
Träger	Papier oder Display	Display des Smartphones	Smartphone
Bindung an das Endgerät	Keine	Über sceId und SCE-Zertifikat	Über sceId und SCE-Zertifikat
Dynamisches Element	Keines	Zeitstempel mit Toleranzfrist	Frisches Challenge des Dienstleister-Terminal an das Smartphone
Weitergabe per Screenshot oder Bildübertragung	möglich	innerhalb der Toleranzfrist möglich	nicht möglich
Prüfung des ID-Mediums	Erforderlich	Nicht zwingend	Nicht zwingend
Kontrollablauf	Scannen und Sichtprüfung	scannen	tappen

4.3 Nachweise und Abnahme

ID	Nachweis	Stufe	Grundlage
NW-01	Der Hersteller weist die Zertifizierung der Terminal-Software einschließlich der MOTICS-Funktionalität nach.	S	SPEC-SO-RT Kap. 3.2; (((etiCORE Leitfaden Kap.

ID	Nachweis	Stufe	Grundlage
			2.2 ((((eTicket-Regelwerk, Anlage 1)
NW-02	Die Kontrolle einer MOTICS-Berechtigung über NFC wird im Rahmen der Abnahme gegen ein Testnutzermedium nachgewiesen.	S	–

4.4 Begründung der Aufnahme in den Beauftragungsumfang

MOTICS-NFC ist keine eigene Systemkomponente, sondern eine Erweiterung derselben Geräte und derselben Software, die bis Mai 2028 ohnehin angepasst werden. Entwicklung, Zertifizierung und Rollout fallen bei gemeinsamer Beauftragung einmal an. Eine spätere separate Beauftragung löst denselben Zyklus ein zweites Mal aus.

Hinzu kommt die Wirkung im Betrieb: Der Nutzen entsteht erst, wenn die Geräteflotte durchgängig ausgestattet ist, da Tickets bis dahin weiterhin, als Barcode kontrolliert werden und das Zeitfenster des Zeitstempels bestehen bleibt.

5 Beauftragung und Projektdurchführung

Hier gibt es mehrere Migrationsansätze. Dabei kommt es sehr auf die aktuelle Situation beim Verkehrsunternehmen an.

Grundsätzlich zu empfehlen bzw. notwendig:

- **Service-Operator-Terminal:** muss mit allen Varianten umgehen können und braucht dabei die Unterstützung für KA und (((etiCORE inklusive der notwendigen SAMs und Konfigurationen und Sperrlisten/Hotlisten.
- **Service-Operator-System:** separates System nur für (((etiCORE. Weiterbetreiben des bisherigen Dienstleister-Hintergrundsystems für KA bis zur Ablösung.
- **Customer Contract Partner Terminal / Motics-Ausgabe:** „Big Bang"-Ansatz: Ab einem bestimmten Zeitpunkt werden nur noch (((etiCORE-Berechtigungen / Applikationen verwendet. Das spart die Software-Weiche und einen Betrieb mit verschiedenen SAMs.
- **Customer Contract Partner System:** eigenes Modul für (((etiCORE mit größtmöglicher Trennung. Zusammenführung nur über Kundenverwaltung. Bei Ablauf von Berechtigungen / Applikationen wird nur noch (((etiCORE verwendet. Alternativ: „Big Bang" Ansatz: Alle Kunden erhalten zu einem gewissen Zeitpunkt nur noch (((etiCORE-Berechtigungen / Applikationen. Dafür muss parallel ein (((etiCORE-System in Betrieb genommen werden mit den Kundendaten sowie den neuen Applikationen und Berechtigungen.
- **Product Owner System:** möglichst separates System für (((etiCORE, Weiterbetreiben des bisherigen PV-Systems für KA bis zur Ablösung. Alternativ: Zusammenführung der Datenbestände nur an ganz bestimmten Punkten, z.B. bei Suche und Monitoring-Klärfällen. Grundsätzlich empfehlen wir den Anschluss an das neue, mandantenfähige MPS für (((etiCORE. Damit kann eine eigene Umsetzung entfallen.

5.1 Unternehmensspezifische Angaben

Die folgenden Angaben sind unternehmensspezifisch und vom Verkehrsunternehmen zu ergänzen. Ohne sie kann der Hersteller kein belastbares Angebot erstellen.

- ORG_ID und wahrgenommene Rolle (SO/CCP/PO)
- Anzahl der Dienstleister-Terminal, gegliedert nach Gerätetyp
- Gerätetypen mit Baujahr und Stand des Betriebssystems
- NFC-Unterstützung nach ISO/IEC 14443 je Gerätetyp
- Anzahl freier SAM-Steckplätze je Gerätetyp

- Terminal-Management-System (Hersteller, Version)
- Dienstleister-Hintergrundsystem (Hersteller, Version)
- Bestehende Anbindung an das ION (ja / nein)
- Verbund- und Kooperationspartner mit gleichem Hersteller
- Geplanter Termin der Inbetriebnahme der Kontrollfähigkeit
- Umfang der Beauftragung (nur Kontrolle / Kontrolle und Vertrieb)
- Vorgesehener Umgang mit MOTICS-NFC (siehe Kapitel 4)
- Einsatz der Dienstleister-Terminal auch als Terminal eines ausführenden Customer Contract Partners (ja / nein, je Gerätetyp)

5.2 Anforderungen an Lieferumfang und Leistungen

ID	Anforderung	Stufe	Grundlage
LF-01	Die eingesetzten Komponenten müssen für (((etiCORE zertifiziert sein. Liegt die Zertifizierung bei Angebotsabgabe nicht vor, ist sie als Vertragsbestandteil zu vereinbaren.	M	(((etiCORE Leitfaden Kap. 2.2 (zitiert (((eTicket-Regelwerk, Anlage 1); SPEC-SO-RT Kap. 3.2, 3.2.5
LF-02	Das Terminal-Management-System muss während der Übergangszeit beide Standards unterstützen sowie die Konfiguration von SAMs und die Erneuerung von Zertifikaten ermöglichen.	M	(((etiCORE Leitfaden Kap. 2.3, 2.4
LF-03	Der Hersteller muss einen Migrationsplan mit Terminen, Abhängigkeiten und benötigten Beistellungen vorlegen.	M	(((etiCORE Leitfaden Kap. 2.4
LF-04	Der Hersteller muss das Verkehrsunternehmen beim Anschalttest (Level 2) unterstützen. Der Anschalttest ist auch dann erforderlich, wenn bereits eine Anbindung nach KA 1.X besteht.	M	(((etiCORE Leitfaden Kap. 2.5
LF-05	Der Hersteller muss ein Rollout-Konzept für die Geräteflotte vorlegen, einschließlich Software-Verteilung und Rückfallebene.	M	–
LF-06	Für reine Dienstleister-Terminal ohne freien SAM-Steckplatz muss der Einsatz eines Light-SAM (im (((etiCORE Leitfaden als Software-SAM bezeichnet) unterstützt werden.	S	SPEC-SO-RT Kap. 3.2.3; (((etiCORE Leitfaden Kap. 2.6
LF-07	Der Hersteller muss je Gerätetyp nachweisen, ob die vorhandene Hardware für (((etiCORE und für MOTICS-NFC aufrüstbar ist.	S	–
LF-08	Dokumentation und Schulung für Betrieb und Kontrollpersonal müssen Bestandteil der Lieferung sein.	S	–
LF-09	Werden Dienstleister-Terminal zugleich als Terminal eines ausführenden Customer Contract Partners eingesetzt, soll die Aktionsausführung in den Lieferumfang aufgenommen werden. Die betroffenen Geräte benötigen dafür ein Hardware-SAM.	S	SPEC-MAIN Kap. 6.5; (((etiCORE Leitfaden Kap. 2.6

5.3 Termine und Meilensteine

Der Stichtag im Mai 2028 bezeichnet den Zeitpunkt, zu dem die Kontrollsysteme im Feld einsatzfähig sein müssen. Die folgenden Meilensteine sind im Projekt zu vereinbaren und mit Terminen zu hinterlegen:

ID	Meilenstein	Termin
M1	Beauftragung	
M2	Bereitstellung der zertifizierten Software durch den Hersteller	
M3	Test und Abnahme im Testsystem	
M4	Anschalttest (Level 2) erfolgreich abgeschlossen	
M5	Verbundtest abgeschlossen	
M6	Beginn des Rollouts	
M7	Abschluss des Rollouts, Kontrollfähigkeit hergestellt (spätestens zum 01.05.2028)	

Zur Einordnung der Gesamtdauer: Der (((etiCORE Leitfaden enthält einen Referenzplan für den Umstieg. Er führt von der Kosten- und Aufwandsanalyse über Projektplanung, Ausschreibung, Beauftragung, Zertifizierung von Terminals und Hintergrundsystem, Test und Abnahme, Verbundtest und Migrationsplanung bis zur Pilotphase und zur Einführung der Kontrolle. Verbindlich ist dabei weniger die absolute Dauer der einzelnen Schritte als ihre Reihenfolge: Jeder Schritt setzt den vorangegangenen voraus.

Zwei Punkte bestimmen den Zeitbedarf maßgeblich. Die Zertifizierung obliegt dem Hersteller und sollte zum Zeitpunkt der Ausschreibung entweder bereits vorliegen oder als Vertragsbestandteil vereinbart werden. Sind die Produkte des Herstellers zum gewünschten Zeitpunkt noch nicht (((etiCORE fähig, verlängert sich der Einführungszeitraum deutlich; eine enge Abstimmung mit dem Hersteller ist dann im Vorfeld notwendig. Hinzu kommt, dass die Zertifizierung eines Hintergrundsystems einmalig je Hersteller und System vergeben wird, der Anschalttest dagegen für jedes in Betrieb genommene System einzeln erforderlich ist.

Erfahrungswerte aus der Einführung des Deutschlandtickets sind nur bedingt übertragbar. Nach dem Leitfaden kann eine Infrastruktur auf Basis des heutigen Standards KA 1.X in etwa vier bis neun Monaten eingeführt werden, dies allerdings nur für das tariflich einheitliche und leicht abbildbare Deutschlandticket. Für (((etiCORE ist ein längerer Zeitraum anzusetzen, insbesondere wenn eine ganze Palette lokaler Ticketprodukte anzupassen ist.[1]

[1] (((etiCORE Leitfaden Kap. 2, Kap. 2.2 und Kap. 3.1 einschließlich Referenzplan (Tabelle 1)

5.4 Kosten und Kalkulation

Die VDV-ETS hat die zu erwartenden Entwicklungskosten für die Umstellung auf (((etiCORE vorkalkuliert und die Ergebnisse anonym mit Richtpreisangaben der Hersteller verprobt. Referenzwerte für kleine, mittlere und große Verkehrsunternehmen, die zugrunde liegenden Annahmen sowie ein Berechnungsschema für die eigene Kalkulation stehen auf der Internetseite der VDV-ETS zur Verfügung:

www.eticket-deutschland.de/standard/eticore, Bereich „so viel kostet (((etiCORE“

Die Werte dienen der Plausibilisierung eines Angebots; sie sind keine Preisobergrenze und kein Richtwert für eine Vergabe. Es wird empfohlen, mit dem Angebot eine Urkalkulation zum Projekt anzufordern.

5.5 Gemeinsames Vorgehen mit anderen Verkehrsunternehmen

Da die Entwicklungskosten des Herstellers auf die Anzahl der Projekte und Geräte umgelegt werden, senkt jede zusätzliche Beauftragung beim selben Hersteller den Anteil aller Beteiligten. Anfragen und Verhandlungen sollten daher möglichst nicht einzeln geführt werden, sondern gemeinsam mit Unternehmen, die Produkte desselben Herstellers einsetzen. Innerhalb eines Verbundes bietet sich eine abgestimmte Projektplanung an.

Um solche Einkaufsgemeinschaften zu ermöglichen, besteht im (((efi die Gruppe der (((etiCORE-Koordinatoren. Dort wird eine Herstellerübersicht gepflegt, die Verkehrsunternehmen je Hersteller und Komponente gruppiert: Für jeden Hersteller ist erfasst, welche Verkehrsunternehmen welche Komponenten einsetzen, etwa Dienstleister-Terminal oder Dienstleister-Hintergrundsystem, mit Gerätetyp und ungefährer Stückzahl. Die Übersicht dient genau dem Zweck, Verkehrsunternehmen mit demselben Hersteller zusammenzubringen.

6 Anlagen und mitgeltende Dokumente

6.1 Hinweis zum Versionsstand

Die modellbasierten Spezifikationsdokumente des (((etiCORE-Standards liegen zum Zeitpunkt der Erstellung dieses Dokuments als Release Candidate 3.0.0-rc.6 vor. Maßgeblich ist stets die jeweils aktuelle veröffentlichte Fassung.

Die Spezifikationen der zweiten Generation der Sicherheitsinfrastruktur, darunter SPEC-UM und SPEC-SAM, tragen auf jeder Seite einen Vertraulichkeitsvermerk und dürfen ohne vorherige schriftliche Zustimmung der VDV-ETS nicht weitergegeben werden. Vor der Weitergabe von Spezifikationsunterlagen an Hersteller ist zu prüfen, welche Dokumente diesem Vermerk unterliegen.

6.2 (((etiCORE-Spezifikation

Die nachfolgend aufgeführten Dokumente sind für die Umsetzung der Kontrolle unmittelbar einschlägig.

Kurzform	Titel	Stand	Relevanz für die Kontrolle
SPEC-MAIN	Main Specification	3.0.0-rc.6	Rollenmodell, Ausbauvarianten, Elementarprozesse und Anwendungsfälle im Überblick
SPEC-SO-RT	Service Operator Reference Terminal Specification	3.0.0-rc.6	Anwendungsfälle des Dienstleister-Terminals einschließlich Funktionspaket statische Berechtigung
SPEC-SO-RS	Service Operator Reference System Specification	3.0.0-rc.6	Anwendungsfälle des Dienstleister-Hintergrundsystems
SPEC-ION	Interoperable Network Specification	3.0.0-rc.6	Nachrichtenaustausch im Interoperabilitätsnetzwerk, Webservice Security
SPEC-UM	User Medium Specification	1.0.13	Datenmodell und Befehlssatz der Chipkarten-Applikation
SPEC-SAM	Secure Application Module Specification	1.0.11	Datenmodell und Befehlssatz der SAM-Applikation
SPEC-CipherSuite	Cipher Suite Specification	1.0.1	Kryptographische Algorithmen für Nutzermedium, SAM und Signatur von Barcodes und MOTICS
SPEC-PKI-Setup	2GSI PKI Setup Specification	-	Parameter und Daten für die 2GSI Medien-PKI, die Zertifikate für SAM und Nutzermedien ausgibt
SPEC-M2MC	M2M Certificates Specification	2.0.3	Struktur und Inhalt der Machine-to-Machine-Zertifikate
User's Manual	User's Manual	3.0.0-rc.6	Lesehilfe für den Umgang mit dem Spezifikationsmodell

6.3 Weiterhin gültige Dokumente der VDV-KA

Der überwiegende Teil der KA-Spezifikationen entfällt mit (((etiCORE oder geht in den oben genannten Dokumenten auf. Für die Kontrolle bleiben relevant:

Dokument	Anmerkung
Anlage TLV EFS	Wird in (((etiCORE weiterverwendet. Der Referenz-EFS kann ebenfalls weiterverwendet werden, wird laut (((etiCORE Leitfaden aber nicht empfohlen.
KA-etiCORE-Glossar	Gegenüberstellung der Begriffe beider Standards; für beide Versionen gültig
KA MOTICS-Spec, Version 1.13.0	Beschreibt das MOTICS-Verfahren für Barcode und NFC. Grundlage der Erläuterungen in Kapitel 4.2

6.4 Unterstützende Dokumente der VDV-ETS

Dokument	Inhalt
(((etiCORE Leitfaden	Einstieg in (((etiCORE, Migrations- und Parallelbetriebsaspekte, Schritt-für-Schritt-Anleitung, Referenzplan für den Umstieg
Quick-Guide (((etiCORE	Zugänge zu ASM-Tool, (((efi und Online-Spezifikation
Was darf (((etiCORE kosten?	Vorkalkulation der Entwicklungskosten mit Referenzbeispielen für kleine, mittlere und große Unternehmen
(((etiCORE-Kalkulationstabelle	Berechnungsschema für die Eigenkalkulation, getrennt nach Rollen

6.5 Zugänge und Online-Quellen

Zweck	Zugang	Hinweis
Spezifikationsdokumente	asmtool.eticket-deutschland.de	Anmeldung erforderlich; Kategorie „etiCORE Spec“
Online-Spezifikationsmodell	modell.eticket-deutschland.de/LATEST	Jeweils letztes Release; Übersicht unter modell.eticket-deutschland.de
Forum, Migrationshilfen, Beispieldaten	efi.eticket-deutschland.de	Anmeldung erforderlich; Gruppe „(((etiCORE Forum“
Berechnungsschema Eigenkalkulation	eticket-deutschland.de	Paket „Infos zu Preisen und Kalkulation“ Zugang: https://www.eticket-deutschland.de/standard/eticore
Herstellerübersicht für Einkaufsgemeinschaften	efi.eticket-deutschland.de	Gruppe „(((etiCORE-Koordinatoren"; geschlossene Gruppe