Zuletzt bearbeitet: 11.06.18

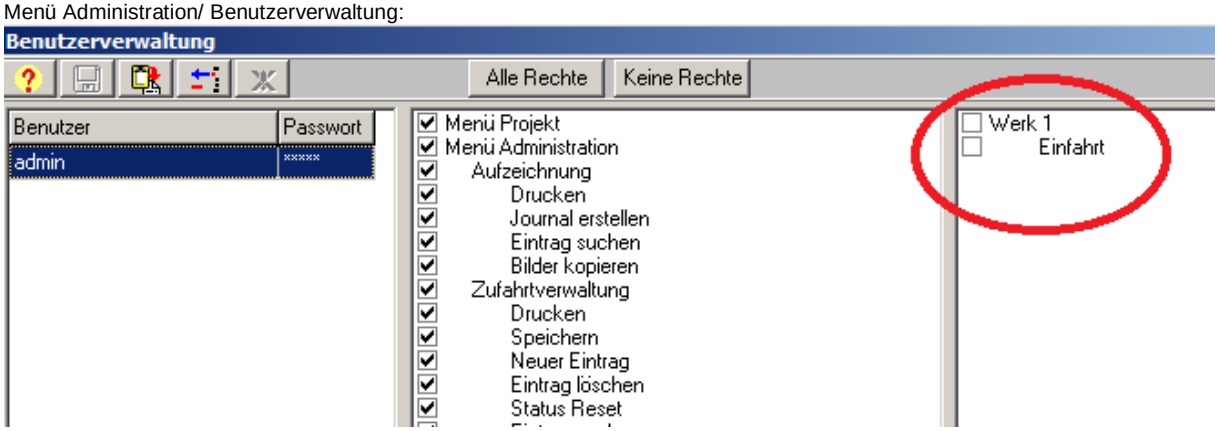
Datenschutz

Mit dem Inkrafttreten der europäischen Datenschutzgrundverordnung DSGVO am 25. Mai 2018 tritt das Thema in den Fokus der Öffentlichkeit.

Das CAR-READER-System ist davon in doppelter Weise betroffen. Zum einen werden Videokameras eingesetzt, die evtl. dazu dienen könnten, um Personen zu beobachten bzw. Bilder von ihnen zu speichern. Zum anderen werden Fahrzeugkennzeichen automatisiert gelesen und verarbeitet.

Das Thema Videoüberwachung wird hier ausgespart, da die eingesetzten Kameras vom CAR-READER-System nicht für diesen Zweck vorgesehen sind. Die Ausgabe des Livebildes kann vom User im CAR-READER gesperrt werden, was wir zur Einhaltung der Vorgaben zur Videoüberwachung empfehlen würden.

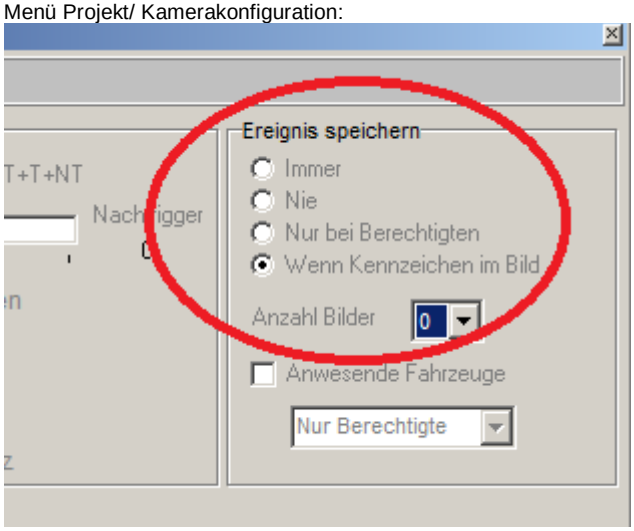
Menü Administration/ Benutzerverwaltung:



Hierzu wird in der Benutzerverwaltung der Zugriff auf die Fahrspurfenster gesperrt.
Der Zugriff per Browser auf die Kameras sollte ebenfalls mit einem geeigneten Passwort geschützt werden.

Das Abspeichern von Bildern, die beim Triggern von Fahrzeugen entstehen, kann im CAR-READER ebenfalls deaktiviert werden.

Menü Projekt/ Kamerakonfiguration:



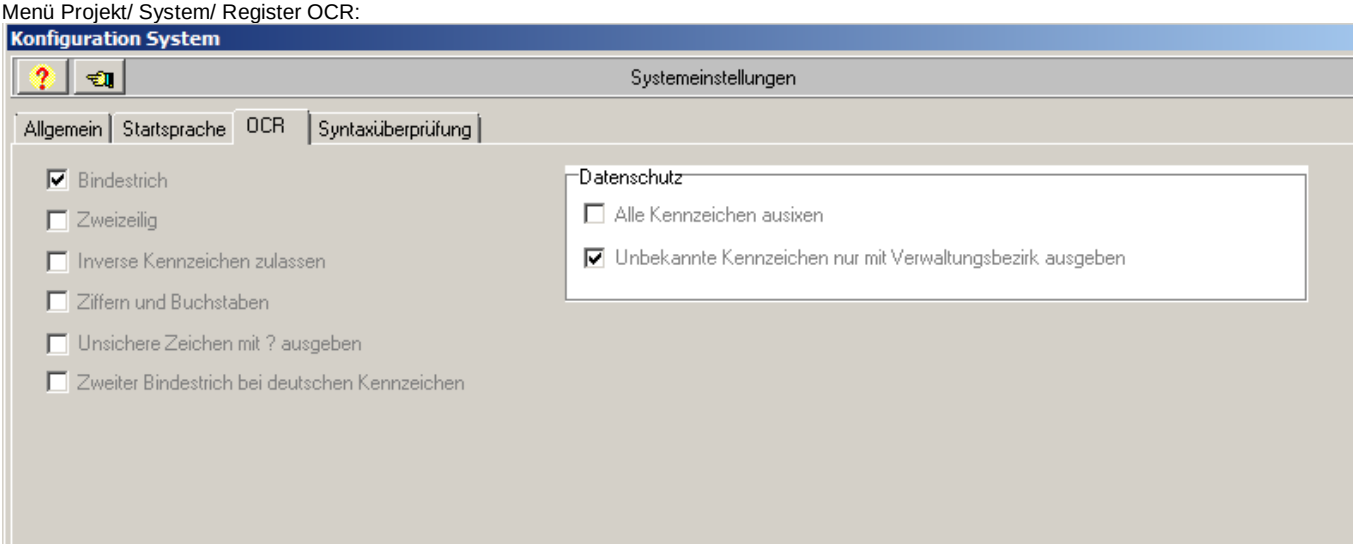
Braucht man dennoch die Bilder, lassen sich diese mit der Verschlüsselungskomponente auf Dateiebene verschlüsseln. Als Verfahren wird das Advanced Encryption System mit einem 256-Bit-Schlüssel verwendet. Näheres dazu findet sich unter:
https://de.wikipedia.org/wiki/Advanced_Encryption_Standard
und dem Dokument CR3_Verschlüsselungskomponente.pdf
Sollten Bilder (verschlüsselt) gespeichert werden, ist bei der Ausrichtung der Kamera darauf zu achten, dass keine Personen erfasst werden. Bei ordnungsgemäßer Installation ist nur die Fahrzeugfront mit Kennzeichen im Bild sichtbar um Belange der Videoüberwachung entgegen zu treten.

Fahrzeugkennzeichen werden vom Datenschutz als personenbezogene Daten interpretiert, auch wenn auf den ersten Blick nicht einsehbar ist, dass man von einem Fahrzeug auf eine Person, die das Fahrzeug fährt, schließen kann. Theoretisch könnte ja jeder beliebige hinter dem Steuer sitzen.
Es besteht jedoch die Möglichkeit mit vertretbarem Aufwand z.B. durch eine Halterabfrage bei der Zulassungsstelle eine Person über ein Fahrzeugkennzeichen zu identifizieren, so dass Kennzeichen genauso wie IP-Adressen von Rechnern unter die Datenschutzgrundverordnung fallen.

Die Nutzung und Verarbeitung von Kennzeichen in der CAR-READER Zufahrtsverwaltung (White- oder Blackliste) muss deshalb durch jeweilige Einverständniserklärungen der Fahrer/Halter abgedeckt sein. Wir gehen davon aus, dass bei Kennzeichen, die im CAR-READER eingetragen werden, eine entsprechende Erlaubnis eingeholt worden ist. Dies betrifft z.B. Mitarbeiter von Firmen, für die eine automatische Schrankenöffnung erfolgen soll. Diese Kennzeichen werden im CAR-READER deshalb NICHT codiert oder verschlüsselt dargestellt.

Anders verhält es sich bei Kennzeichen die nicht im System hinterlegt und deshalb unbekannt sind. Die Erfassung und Verarbeitung dieser Kennzeichen unterliegt abhängig von der jeweiligen Anwendung verschiedenen Prozessen.
Zunächst kann die Anzeige im Fahrspurfenster und in der Aufzeichnung durch eine Konfigurationseinstellung unterdrückt werden:

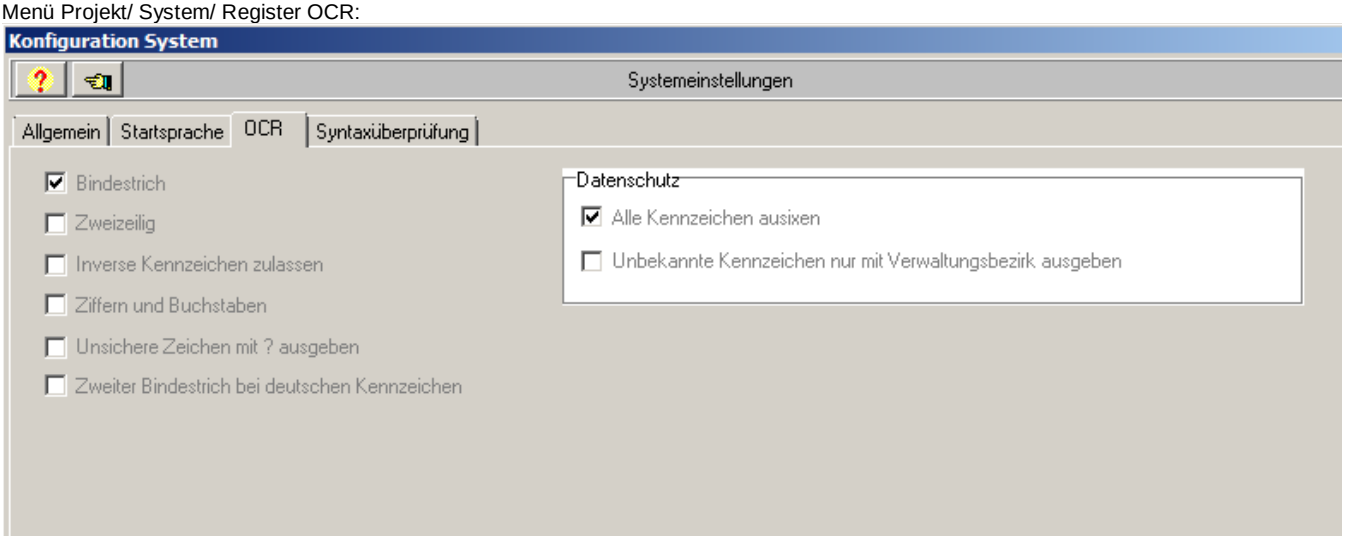
Menü Projekt/ System/ Register OCR:



Statt dem kompletten Kennzeichenstring wie etwa R-AB123 wird dann im Fahrspurfenster, in der Hauptmaske und in der Aufzeichnungsdatenbank nur R-XXXXX ausgegeben.

Sollen alle gelesenen Kennzeichen irreversibel geschützt werden, wählt man in der Konfiguration den Punkt „Alle Kennzeichen ausixen“.

Menü Projekt/ System/ Register OCR:

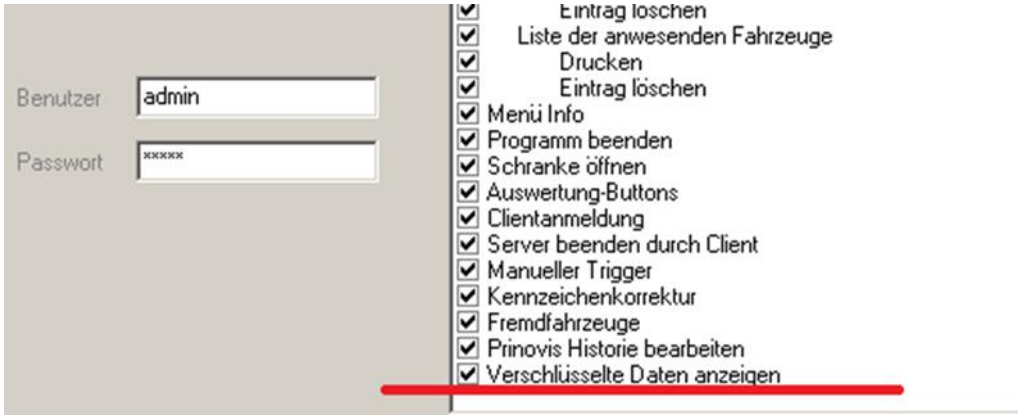


Die gelesenen Kennzeichen sind dann auch tatsächlich für Niemanden mehr einsehbar.

Will man die aufgezeichneten Bilder und Daten auf Betriebssystems Ebene schützen, bedarf es der Verschlüsselungskomponente. Diese garantiert, dass außerhalb des CAR-READER-Programms Niemand auf Windowsebene die Bilder und Daten einsehen kann.

Die Eigenschaft im CAR-READER-Programm die Bilder anschauen zu können, kann wiederum in der Benutzerverwaltung aktiviert werden:

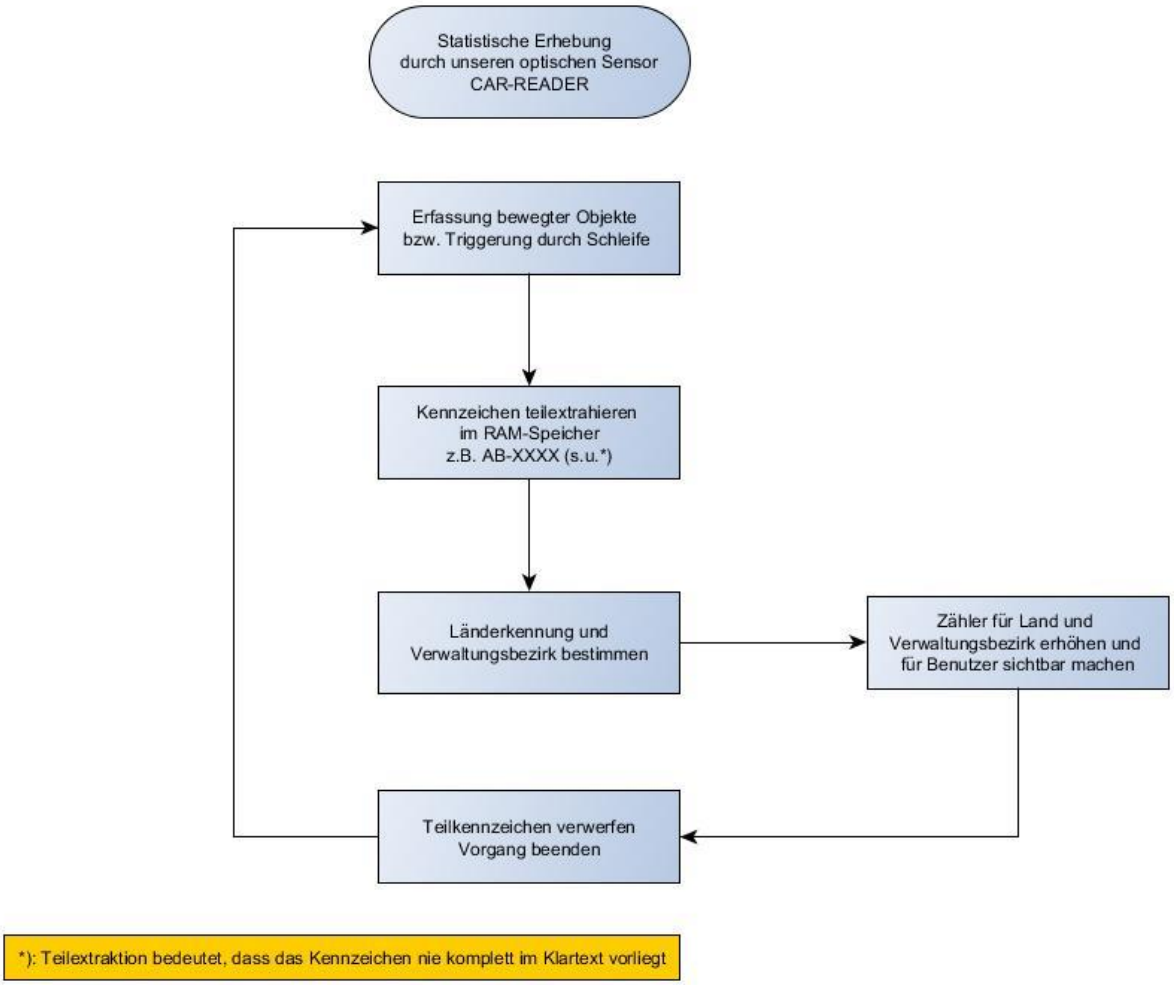
Menü Administration/ Benutzerverwaltung:



Typische Anwendungen der CAR-READER-Kennzeichenerkennung, die datenschutz-konform im Programm abgebildet werden können.

A) Statistische Erhebungen

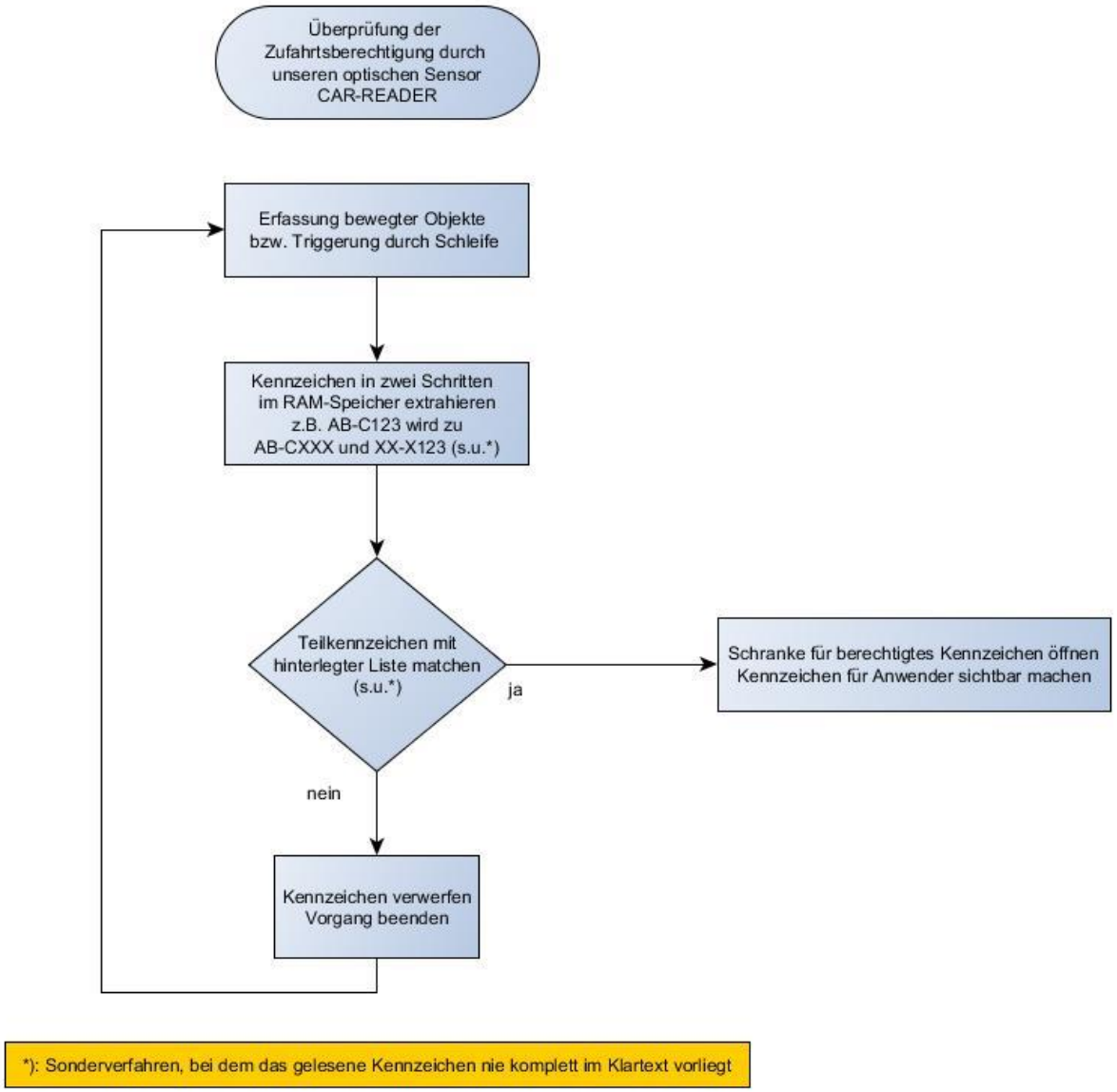
Zur Auswertung der Herkunft von Fahrzeugen wie z.B. Verwaltungsbezirke oder Länderzugehörigkeit läuft im CAR-READER folgender Prozess ab:



Für diesen Anwendungsfall werden zu keinem Zeitpunkt Kennzeichen vollständig erfasst. Notwendig dafür ist allerdings die Verschlüsselungskomponente, die die Teilextraktion der Kennzeichen im RAM zur Verfügung stellt.

B) Überprüfung der Zufahrtsberechtigung

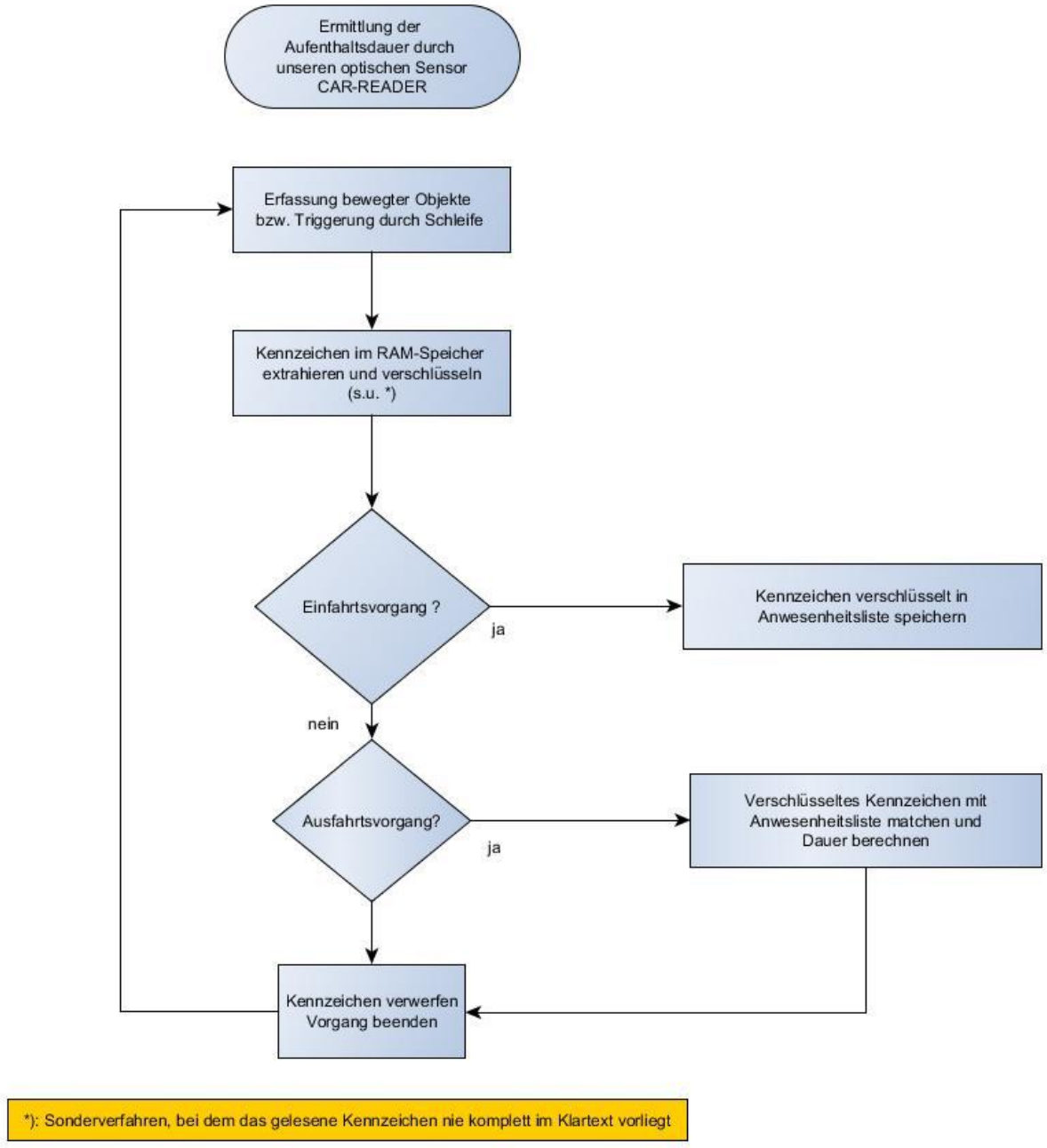
Berechtigte und mit der Kennzeichenverarbeitung einverstandene Fahrer werden wie folgt abgearbeitet:



Für diesen Anwendungsfall werden zu keinem Zeitpunkt unbekannte Kennzeichen vollständig erfasst. Notwendig dafür ist allerdings die Verschlüsselungskomponente, die die Aufspaltung der Kennzeichen im RAM zur Verfügung stellt.

C) Aufenthaltsdauer von Fahrzeuge bestimmen

In einem Parkhaus soll die Aufenthaltsdauer von Fahrzeugen über das Kennzeichen bestimmt werden, obwohl keine Einverständniserklärung der (unbekannten) Fahrer vorliegt.



Für diesen Anwendungsfall werden zu keinem Zeitpunkt Kennzeichen vollständig im Klartext erfasst. Notwendig dafür ist allerdings die Verschlüsselungskomponente, die die Verschlüsselung schon bei der Extraktion der Kennzeichen im RAM vornimmt.