BLIKSUND

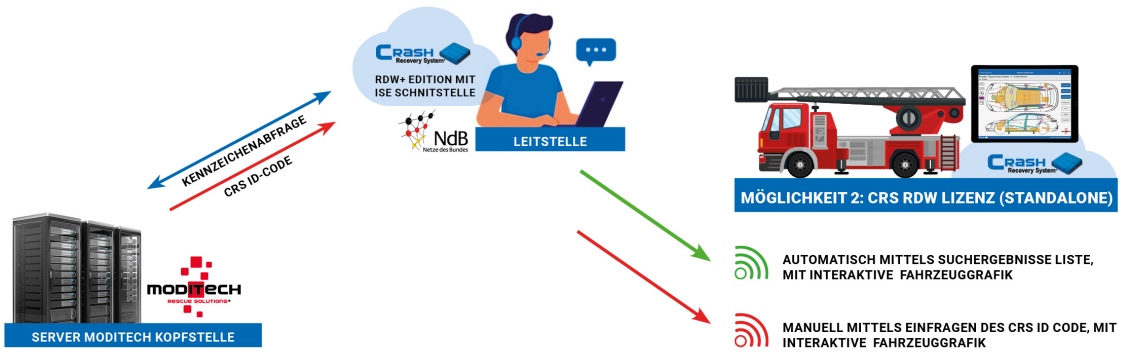
Sicherheitsrelevante Fragestellungen und technische Belange bei der Einführung neuer Verfahren

Version: 3. Juli 2025

1. **Dokumentation/Beschreibung des Verfahrens:** Die Dokumentation enthält eine umfassende Beschreibung des einzusetzenden Verfahrens. Sie enthält grundlegende Informationen über den Zweck und das Anwendungsgebiet des Verfahrens und beschreibt die Regeln, Arbeitsabläufe und Vorgänge des Verfahrens. Darüber hinaus sind dort die Schnittstellen von und zu anderen internen und externen Verfahren zu nennen.

Das Crash Recovery System ist auf allen gängigen mobilen Plattformen und über ein Online-Portal verfügbar. Das CRS bietet interaktive und modellspezifische Ansichten von Fahrzeugen aus der Vogelperspektive und von der Seite mit Deaktivierungsverfahren. Diese Informationen werden in einem standardisierten, ISO-formatierten Rettungsdatenblatt bereitgestellt. Ein Fahrzeug kann manuell nach Fahrzeugmodell oder automatisch nach Kennzeichen, VIN oder QR-Code ausgewählt werden. Jedes Fahrzeugrettungsdatenblatt enthält Standorte und Deaktivierungsverfahren für alle rettungsrelevanten Komponenten im Fahrzeug.

Um den Fahrzeugauswahlprozess zu automatisieren und zu vereinfachen, hat Bliksund Zugang zu den Kennzeichenregisterbehörden in mehreren europäischen Ländern. In Deutschland umfasst dies das Kraftfahrt-Bundesamt (KBA). Aufgrund der datenschutzrechtlichen Natur der Fahrzeugregisterinformationen ist es den deutschen Feuerwehren nicht gestattet, Kennzeichenregisterinformationen direkt vom KBA zu erhalten. Nur Notrufzentralen („Leitstellen“) sind berechtigt, Fahrzeuginformationen auf Basis eines Kennzeichens beim KBA anzufordern. Aufgrund dieser Einschränkung wird die Kennzeichenabfrage von der Online-Version des CRS durch die Notrufzentrale durchgeführt. Nach dieser Abfrage wird das richtige Rettungsdatenblatt automatisch im CRS ausgewählt und an die Einsatzkräfte am Unfallort übermittelt, damit sie basierend auf den bereitgestellten Anweisungen sicher arbeiten und wertvolle Zeit sparen können.

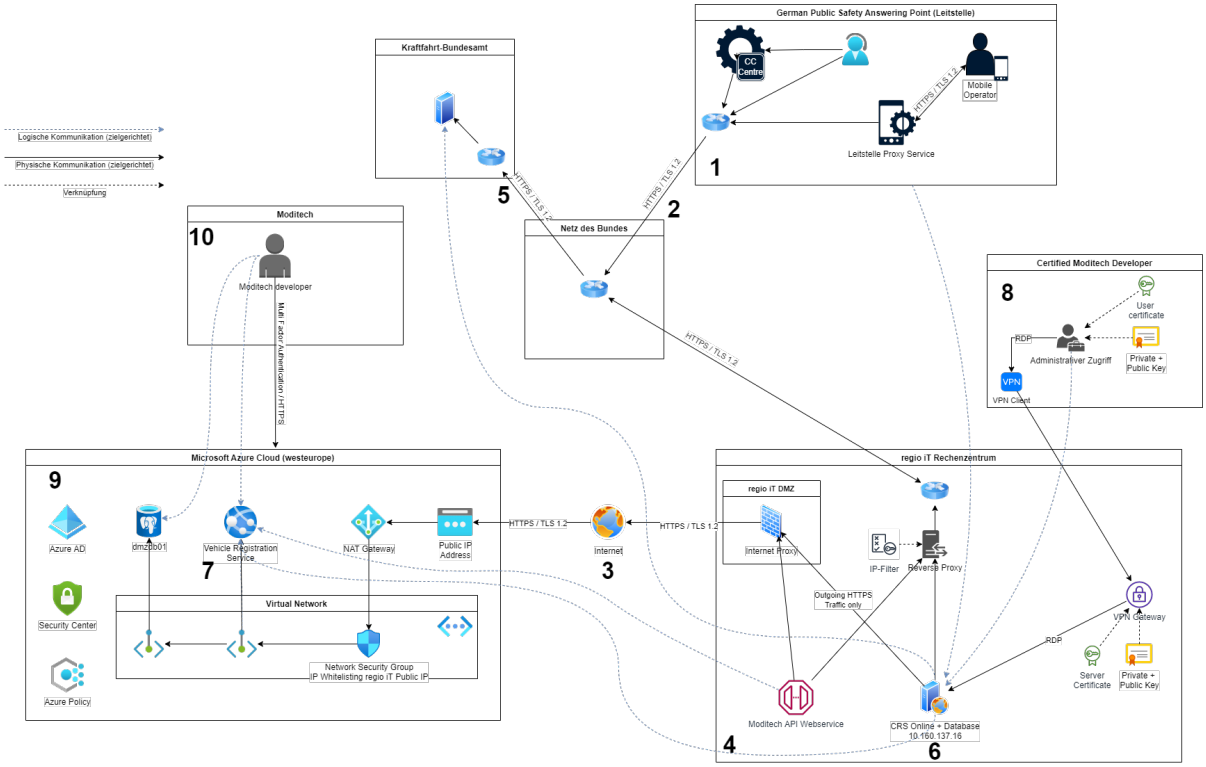


2. Schnittstellen von und zu anderen internen und externen Verfahren

In Deutschland wird die Online-CRS-Anwendung („Anwendung“) von den PSAPs („Leitstellen“) verwendet, um die Fahrzeugdaten zu erhalten. Es gibt zwei Möglichkeiten, die KBA-Datenbank abzufragen: nach Kennzeichen oder nach der VIN des Fahrzeugs. Die vom KBA zurückgegebenen technischen Informationen werden dann verwendet, um das richtige Fahrzeug in der CRS-Datenbank zu finden und das Rettungsdatenblatt anzuzeigen. Während dieses Prozesses sieht der Bediener nur die Modellbeschreibung des Fahrzeugs ohne technische Details.

Wenn eine PSAP eine Anfrage nach Fahrzeuginformationen startet, greift der Bediener mit einem Webbrowser innerhalb des NdB-VN-Netzwerks auf die CRS Online-Anwendung zu.

Die CRS Online-Anwendung befindet sich im NdB-VN-Netzwerk und wird von einem zertifizierten Anbieter, Regio-IT, gehostet. Regio-IT ist ein deutscher Internetdienstanbieter, der autorisiert ist, Zugang zum NdB-Netzwerk zu bieten.



3. **Aussagen zur Art der gespeicherten Daten im Verfahren bzw. bei der Durchführung der Dienstleistung:** Es ist vollständig und abschließend zu beschreiben, welche Daten von dem Verfahren bzw. bei Erbringung der Dienstleistung verarbeitet werden sollen. Es ist zu prüfen, ob es sich um perso-nenbezogene Daten handelt (ggf. um besonders schutzwürdige Daten gem. § 4 Abs. 3 DSG NRW) und auf welcher Rechtsgrundlage die Daten verarbeitet werden.

Die Online-CRS-Anwendung setzt, speichert, ändert oder überträgt keine KBA-informationen. Es werden keine KBA-Daten auf dem Computer des Benutzers angezeigt, gespeichert oder protokolliert. Es wird nur die allgemeine Fahrzeugbeschreibung mit einem Rettungsblatt bereitgestellt. **Dementsprechend verwaltet unser CRS keine personenbezogenen oder schutzwürdigen Daten.**

4. **Administrationshandbuch:** Das Administrationshandbuch enthält alle für den Betrieb des Verfahrens notwendigen Informati-onen. Hierzu gehören notwendige technische Voraussetzungen zum Betrieb, technische Be-schreibung aller beteiligten Systeme und der eingesetzten Hardware, Software (Betriebssystem, Middleware, Programmiersprachen, Module), sowie Datenbanken und evtl. mobile Systeme.

Um Fahrzeuginformationen basierend auf einem Kennzeichen oder einer VIN anzufordern, müssen die PSAPs mit dem NdB-VN-Netzwerk verbunden sein. Für eine Anfrage beim Anwendungsserver wird die HTTPS-Verbindung basierend auf dem TLS 1.2 Protokoll verwendet. Diese Verschlüsselung entspricht dem BSI TR-02102-2 Protokoll.

Alle Verbindungen zu und von dem CRS-Anwendungsserver sind HTTPS-Anfragen unter Verwendung des TLS 1.2 Protokolls (Abbildung 1&2).

Der CRS-Anwendungsserver bei Regio-IT ist in einem sicheren Netzwerk gehostet. Es ist nicht möglich, eine Anfrage aus der Bliksund Azure-Umgebung oder dem öffentlichen Internet an den CRS-Anwendungsserver zu senden. Aus Gründen der Netzwerksicherheit verfügt der Regio-IT-Server über einen Reverse-Proxy vor dem Anwendungsserver, der nur eingehende, auf die Whitelist gesetzte Anfragen aus dem NdB-VN-Netzwerk empfängt. Dieser Reverse-Proxy verwendet eine IP-Filterung, sodass nur auf die Whitelist gesetzte PSAPs auf den CRS-Anwendungsserver zugreifen können. Wenn der CRS-Anwendungsserver die Bliksund Azure-Umgebung anfragt, wird ein Internet-Proxy verwendet, der nur ausgehenden HTTPS-Verkehr zulässt. Die IP-Adresse des Regio-IT-Servers ist in der Bliksund Azure-Umgebung auf die Whitelist gesetzt.

5. **Sicherheitskonzept**: Das Sicherheitskonzept, dass durch die Hersteller von Verfahren bzw. durch die Anbieter einer Dienstleistung verfasst wird, ist als eine abstrakte Blaupause eines Sicherheitskonzeptes zu ver-stehen, welches zunächst das definierte Schutzniveau nach Art und Umfang der Datenverarbei-tung (zum Schutzniveau vgl. auch Handbuch des Bundesamtes für Sicherheit in der Datenverar-beitung BSI) beschreibt und die erforderlichen technischen Mittel für die Umsetzung liefert. Das Sicherheitskonzept muss schlüssig und nachvollziehbar Auskunft über technische und organisato-rische Maßnahmen zur Datensicherheit enthalten.

In Deutschland muss die Kommunikation mit allen Servern, an die die entsprechenden Daten gesendet werden, in Übereinstimmung mit den Mindestanforderungen an Organisation und Sicherheit gesichert werden, die durch die für Bundesbehörden verbindlichen Mindeststandards definiert sind.

Der CRS-Anwendungsserver bei Regio-IT ist in einem sicheren Netzwerk gehostet. Es ist nicht möglich, eine Anfrage aus der Bliksund Azure-Umgebung oder dem öffentlichen Internet an den CRS-Anwendungsserver zu senden. Aus Gründen der Netzwerksicherheit verfügt der Regio-IT-Server über einen Reverse-Proxy vor dem Anwendungsserver, der nur eingehende, auf die Whitelist gesetzte Anfragen aus dem NdB-VN-Netzwerk empfängt. Dieser Reverse-Proxy verwendet eine IP-Filterung, sodass nur auf die Whitelist gesetzte PSAPs auf den CRS-Anwendungsserver zugreifen können. Wenn der CRS-Anwendungsserver die Bliksund Azure-Umgebung anfragt, wird ein Internet-Proxy verwendet, der nur ausgehenden HTTPS-Verkehr zulässt. Die IP-Adresse des Regio-IT-Servers ist in der Bliksund Azure-Umgebung auf die Whitelist gesetzt. Mit diesen Sicherheitsmaßnahmen ist ein unbefugter Zugriff auf den CRS-Anwendungsserver sowohl aus dem Internet, der Bliksund Azure-Umgebung als auch aus dem internen NdB-VN-Netzwerk unmöglich. Die umgebende Infrastruktur und die unidirektionale Netzkommunikation verhindern dies durch ihr Design. Alle Verbindungen zur Außenwelt müssen vom CRS-Anwendungsserver ausgehen, und er akzeptiert keine nicht zugehörigen eingehenden Netzwerkverbindungen.

Azure Application Gateway Alle Bliksund-Dienste befinden sich innerhalb eines speziell konfigurierten Bliksund Azure VNet und sind von der Außenwelt nicht zugänglich. Aufgrund der Verwendung privater Endpunkte können nur das Azure Application Gateway und der API-Verwaltungsdienst Backend-Dienste in der Bliksund Azure-Infrastruktur verbinden. Wie oben erwähnt, ist ein Azure Application Gateway vor der Bliksund Azure-Infrastruktur platziert, das dafür verantwortlich ist, Angriffe auf die Bliksund Azure-Infrastruktur und Umgebung zu verhindern. Mit dem Application Gateway ist die Bliksund-Umgebung geschützt vor:

- SQL-Injection-Angriffen
- Cross-Site-Scripting-Angriffen
- Anderen häufigen Angriffen wie Befehlsinjektion, HTTP-Anfrageverfälschung, HTTP-Antwortspaltung und Remote-Dateieinbindung
- HTTP-Protokollverletzungen
- HTTP-Protokollanomalien wie fehlende Host-, User-Agent- und Akzeptanz-Header
- Bots, Crawler und Scanner
- Häufigen Anwendungsfehlkonfigurationen (z. B. Apache und IIS)

Dieses Application Gateway bietet folgende Optionen:

- Autoskalierung
- Zonenausfallsicherheit
- Statische VIP
- Azure Kubernetes Service (AKS) Ingress-Controller
- Azure Key Vault-Integration
- Umschreiben von HTTP(S)-Headern
- URL-basiertes Routing
- Hosting mehrerer Websites
- Verkehrsweiterleitung
- Web Application Firewall (WAF)
- WAF-Benutzerdefinierte Regeln
- WAF-Richtlinienassoziationen
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Termination
- End-to-End TLS-Verschlüsselung
- Sitzungsaffinität

- Benutzerdefinierte Fehlerseiten
- WebSocket-Unterstützung
- HTTP/2-Unterstützung
- Verbindungstraining

OWASP Das Open Web Application Security Project (OWASP) ist eine Online-Community, die frei verfügbare Artikel, Methoden, Dokumentationen, Werkzeuge und Technologien im Bereich der Webanwendungssicherheit produziert. Es wird von einer gemeinnützigen Organisation namens The OWASP Foundation geleitet. Das OWASP Top 10 - 2021 ist das veröffentlichte Ergebnis aktueller Forschungen, die auf umfassenden Daten basieren, die von über 40 Partnerorganisationen zusammengestellt wurden.

Das Azure Application Gateway kann OWASP-beschriebene Angriffe erkennen und verhindern. Basierend auf diesen Szenarien/Angriffen hat Microsoft spezifische Richtlinien erstellt, die für das Azure Application Gateway entwickelt wurden, um diese Angriffe zu verhindern, wenn sie in Ihrem Netzwerk auftreten. Das Application Gateway ist so eingestellt, dass es Angriffe basierend auf den OWASP 3.2-Richtlinien verhindert. Im Folgenden finden Sie eine Liste der Hauptkategorien, in denen das Application Gateway Angriffe verhindert. Für die vollständige Beschreibung der Anfragen siehe Anhang 1.

- KNOWN-CVES - Hilft, neue und bekannte CVEs zu erkennen
- REQUEST-911-METHOD-ENFORCEMENT - Methoden (PUT, PATCH) sperren
- REQUEST-913-SCANNER-DETECTION - Schutz vor Port- und Umgebungsscannern
- REQUEST-920-PROTOCOL-ENFORCEMENT - Schutz vor Protokoll- und Codierungsproblemen
- REQUEST-921-PROTOCOL-ATTACK - Schutz vor Header-Injektion, Anfrageverfälschung und Antwortspaltung
- REQUEST-930-APPLICATION-ATTACK-LFI - Schutz vor Datei- und Pfadangriffen
- REQUEST-931-APPLICATION-ATTACK-RFI - Schutz vor Remote-Dateieinbindung (RFI)-Angriffen
- REQUEST-932-APPLICATION-ATTACK-RCE - Schutz vor Remote-Code-Ausführungsangriffen
- REQUEST-933-APPLICATION-ATTACK-PHP - Schutz vor PHP-Injection-Angriffen
- REQUEST-941-APPLICATION-ATTACK-XSS - Schutz vor Cross-Site-Scripting-Angriffen
- REQUEST-942-APPLICATION-ATTACK-SQLI - Schutz vor SQL-Injection-Angriffen
- REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION - Schutz vor Sitzungsfixierungsangriffen
- REQUEST-944-APPLICATION-ATTACK-SESSION-JAVA - Schutz vor JAVA-Angriffen

LOG4J Die Application Gateway Firewall schützt die Azure Bliksund-Umgebung auch vor der kürzlich entdeckten Log4j-Sicherheitslücke CVE-2021-44228, CVE-2021-45046, wie unter den KNOWN-CVES beschrieben.

Bliksund API Manager Anfragen an die Bliksund Azure-Infrastruktur, die das Gateway und die Application Gateway Firewall passieren, werden vom Bliksund API Manager bearbeitet. Nur der Bliksund API Manager hat einen öffentlichen Endpunkt für spezifische Anfragen, der von außerhalb der Bliksund Azure-Umgebung zugänglich ist. Alle anderen Anwendungen haben nur private Endpunkte, die von außerhalb dieser Umgebung weder sichtbar noch zugänglich sind. Der API-Manager ruft die zugewiesenen privaten Endpunkte aller Backend-Dienste basierend auf der Anfrage auf.

Zusätzliche Sicherheit und Compliance Als zusätzliche Sicherheitsmethode verwendet die Bliksund Azure-Umgebung Microsoft Defender for Cloud, ein Tool zur Sicherheitsstatusverwaltung und Bedrohungsschutz (Anhang 2). Das gesamte Setup der Bliksund Azure-Umgebung schützt vor Angriffen.

Alle blockierten Angriffe werden protokolliert und im Logbuch registriert. Darüber hinaus überwacht der Bliksund-Support die Azure-Umgebung kontinuierlich. Der Bliksund-Support ist rund um die Uhr verfügbar.