



Karlsruher Institut für Technologie

FRAUNHOFER INSTITUT FÜR Optronik, SYSTEMTECHNIK UND
BILDAUSWERTUNG

MARIO KAUFMANN
PASCAL BIRNSTILL
ERIK KREMPEL

PFLICHTENHEFT

VERSION 1.0

Privacy Crash Cam App für Android

FABIAN WENZEL
GIORGIO GROSS
CHRISTOPH HÖRTNAGL
DAVID LAUBENSTEIN
JOSH ROMANOWSKI

6. Dezember 2016

Inhaltsverzeichnis

1 Zielbestimmung	4
1.1 Musskriterien	5
1.1.1 App	5
1.1.2 Web-Dienst	6
1.1.3 Web-Interface	6
1.2 Wunschkriterien	7
1.2.1 App	7
1.2.2 Web-Dienst	7
1.2.3 Web-Interface	8
1.3 Abgrenzungskriterien	8
2 Produkteinsatz	9
2.1 Zielgruppe	9
2.2 Einsatz	10
3 Produktumgebung	11
4 Funktionale Anforderungen	12
4.1 App	12
4.2 Web-Dienst	15
4.3 Web-Interface	17
5 Produktdaten	20
5.1 App	20
5.2 Web-Service	20
5.3 Web-Interface	20
6 Nichtfunktionale Anforderungen	21
6.1 App	21
6.2 Web-Dienst	21
6.3 Web-Interface	22
7 Globale Testfälle	23
7.1 Erklärung zur Qualitätssicherung	23
7.1.1 Komponenten-Tests	23
7.1.2 Integration-Tests	23
7.1.3 System-Tests	23

7.2	Testszenarien	23
7.2.1	Komponenten-Tests	23
App	23	
Web-Dienst	25	
Web-Interface	25	
7.2.2	Integration-Tests	25
App <-> Web-Dienst	25	
Web-Interface <-> Web-Dienst	25	
7.2.3	Systemtests	26
8	Systemmodelle	27
8.1	Anwendungsfälle	27
8.1.1	Bedienung der Android App	27
8.1.2	Bedienung der Website	28
8.2	Aktivitätsdiagramm	29
8.2.1	Vom Appstart bis zur Videofreigabe	29
9	Entwicklungsumgebung	31
9.1	Entwicklungstools	31
9.2	Verwendete Technologien	31
9.3	Beschreibung	31
10	Anhang	33
10.1	UI-Demos	33
10.2	Verschlüsselung	35

1 Zielbestimmung



Das Produkt ermöglicht es seinen Nutzern ihre Autofahrten zu überwachen, indem es durch die Smartphonekamera den Straßenverkehr verfolgt und relevantes Videomaterial persistent abspeichert. Dieses wird bei Bedarf verwendet, um Unfallhergänge im Straßenverkehr zu dokumentieren. Dabei gilt es, dem deutschen Datenschutzrecht gerecht zu werden, indem Personen und personenbezogene Daten, wie zum Beispiel Autokennzeichen, unkenntlich gemacht werden. Die Anwendung bietet dem Nutzer dafür eine moderne und intuitive Bedienoberfläche.

Zur Realisierung kann das Produkt in drei Hauptbestandteile aufgegliedert werden: Die Android App, den Web-Dienst und das Web-Interface. Diese Aufteilung wird in diesem Heft, um eine Übersicht zu schaffen, auch in nachfolgenden Kapiteln beibehalten.

1.1 Musskriterien

1.1.1 App

- PK1000** Nutzer müssen sich anmelden, um die App zu verwenden.
- PK1010** Nur registrierte Nutzer können die App verwenden.
- PK1020** Der Straßenverkehr wird durch die Smartphonekamera beobachtet.
- PK1030** Relevante Videodaten werden verschlüsselt abgespeichert.
- PK1040** Relevante Daten werden durch Auswertung der Sensordaten des Smartphones erkannt. Hierbei werden die Werte des G-Sensors ausgewertet.
- PK1050** Die Aufnahme kann manuell gestartet werden, auch wenn der G-Sensor des Smartphones keinen Anlass dazu gibt.
- PK1060** Während der Aufnahme werden sämtliche Nutzereingaben und G-Sensordaten ignoriert.
- PK1070** Es werden relevante Metadaten mit den Videodaten abgespeichert.
- PK1080** Es wird ab dem Appstart mit dem Beobachten des Straßenverkehrs begonnen.
- PK1090** Es wird nur das Hochformat unterstützt.
- PK1100** Die Beobachtung läuft nur während sich die App im Vordergrund befindet.
- PK1110** Videodaten werden verschlüsselt, sobald sie persistiert werden.
- PK1120** Verschlüsselte Videodaten werden aufgelistet.
- PK1130** Verschlüsselte Videodaten können gelöscht werden.
- PK1140** Vom Nutzer ausgewählte verschlüsselte Videodaten werden an einen Webdienst gesendet, der diese anonymisiert.
- PK1150** Geräte, auf denen Android API Level 19 (Android 4.4) und höher läuft werden unterstützt.
- PK1160** Die Benutzeroberfläche wird für Geräte ab einer Displaydiagonale von 4 Zoll optimiert.
- PK1170** Wenn verschlüsselte Videodaten lange Zeit nicht zum Anonymisieren ausgewählt wurden, wird der Nutzer benachrichtigt, dass er diese löschen kann.
- PK1180** Die aufnahmespezifischen Einstellungen werden angezeigt.
- PK1190** Die Standardsprache ist Deutsch.

1.1.2 Web-Dienst

PK2000 Es existiert eine Schnittstelle, um Videodaten hochzuladen.

PK2010 Von der App gesendete Videodaten werden anonymisiert.

PK2020 Nach Abschluss der Anonymisierung wird der Nutzer per E-Mail benachrichtigt.

PK2030 Es existiert eine Schnittstelle, um Nutzeraccounts anzulegen.

PK2040 Es existiert eine Schnittstelle, um Nutzeraccounts zu verwalten.

PK2050 Es existiert eine Schnittstelle, um die Videodaten eines Nutzers verwalten zu können.

PK2060 Nutzer müssen ihre E-Mail-Adresse verifizieren, um sich anmelden zu können.

PK2070 Die Kommunikation zwischen App und Web-Dienst wird durch eine REST-API realisiert.

PK2080 Die Kommunikation zwischen Web-Interface und Web-Dienst wird durch eine REST-API realisiert.

PK2090 Es existiert eine obere Schranke für die Anzahl der Videodaten, die ein Nutzer zur gleichen Zeit auf seinem Nutzeraccount online speichern kann.

PK2100 Passwörter werden nur als Hash-Code abgespeichert.

PK2110 Es wird Jetty verwendet.

1.1.3 Web-Interface

PK3000 Es können Nutzeraccounts angelegt werden.

PK3010 Es können Nutzeraccounts verwaltet werden.

PK3020 Es können Videodaten verwaltet werden.

PK3030 Es können Videodaten heruntergeladen werden.

PK3040 Nur eingeloggte Nutzer haben Zugriff auf ihre Nutzerdaten.

PK3050 Es können Passwort und E-Mail-Adresse geändert werden.

PK3060 Die Standardsprache ist Deutsch.

1.2 Wunschkriterien

1.2.1 App

WK1000 Falls es Android zulässt, wird die Beobachtung auch ausgeführt, wenn sich die App im Hintergrund befindet.

WK1010 Sowohl Quer- als auch Hochformat werden unterstützt.

WK1020 Die Beobachtung kann manuell gestartet und gestoppt werden.

WK1030 Während der Aufnahme wird eine Möglichkeit angeboten, die Aufnahme abzubrechen.

WK1040 Es können Nutzeraccounts angelegt werden.

WK1050 Es können Nutzeraccounts verwaltet werden.

WK1060 Anonymisierte Videodaten können vom Server gelöscht werden.

WK1070 Push-Benachrichtigungen vom Web-Dienst werden angezeigt.

WK1080 Es können Hilfestellungen für die Bedienung der App angezeigt werden.

WK1090 Anonymisierte Videodaten können heruntergeladen werden.

WK1100 Anonymisierte Videodaten die zum Download bereit stehen und sich nicht auf dem Smartphone befinden werden aufgelistet.

WK1110 Anonymisierte Videodaten, die sich auf dem Smartphone befinden, werden aufgelistet.

WK1120 Anonymisierte Videodaten können vom Speicher des Smartphones gelöscht werden.

WK1130 Anonymisierte Videodaten, die sich auf dem Smartphone befinden, können angesehen werden.

WK1140 Die aufnahmespezifischen Einstellungen können bearbeitet werden.

WK1150 So lange der G-Sensor des Smartphones Anlass zur Aufnahme gibt wird weiter aufgenommen.

1.2.2 Web-Dienst

WK2000 Die Zeit, die die Anonymisierung in Anspruch nehmen wird, wird geschätzt und an den Nutzer weitergeleitet.

WK2010 Es wird eine Push-Benachrichtigung an das Smartphone gesendet, sobald die Anonymisierung der Videodaten abgeschlossen ist.

WK2020 Videodaten werden maximal vier Wochen gespeichert.

WK2030 Der Nutzer erhält eine Woche bevor ein Video gelöscht wird eine E-Mail-Banchrichtigung.

1.2.3 Web-Interface

WK3000 Das Produkt wird neuen Nutzern präsentiert.

WK3010 Nutzer können ihre anonymisierten Videos online ansehen.

1.3 Abgrenzungskriterien

AK1000 Das Betrachten nicht anonymisierter Videodaten ist nicht möglich.

AK1010 Videodaten werden nicht automatisch persistiert, sobald die Beobachtung läuft.

AK1020 Livestreams werden nicht unterstützt.

AK1030 Die Anonymisierung findet nicht auf dem Smartphone statt.

AK1040 Der Web-Dienst speichert Videodaten nicht auf unbegrenzte Zeit und in unbegrenzter Anzahl.

AK1050 Vom Speicher des Smartphones werden Videodaten nicht automatisch gelöscht.

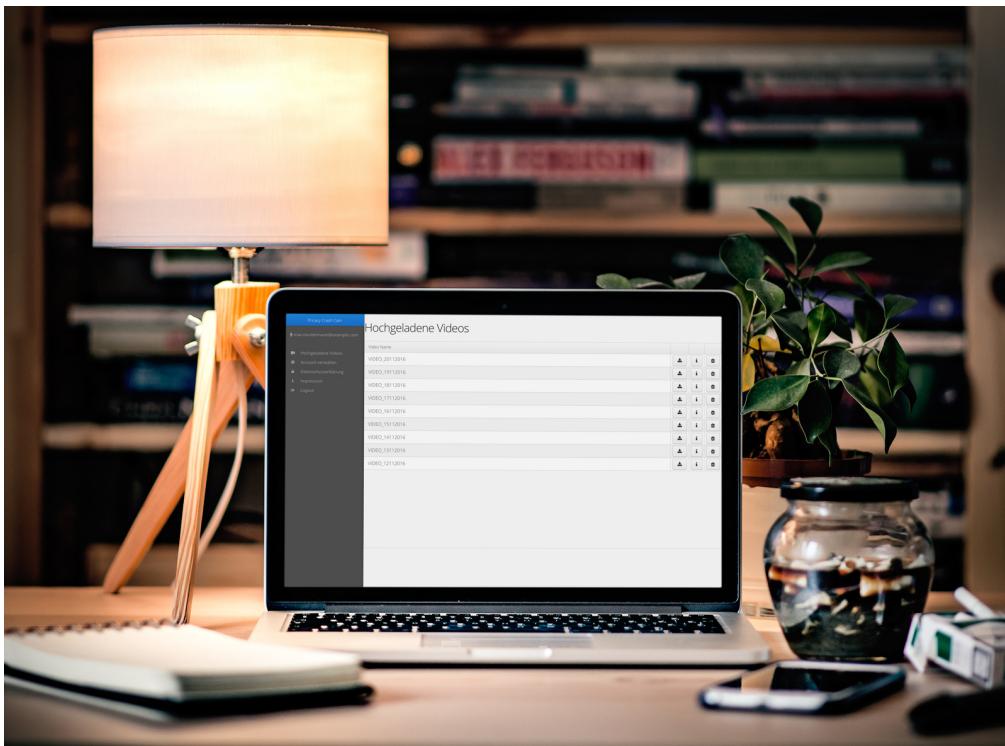
AK1060 Von Nutzern zurückgelegte Wege und besuchte Orte werden nicht aufgezeichnet.

AK1070 Die App ist nicht mit Windows Phone und iOS kompatibel.

AK1080 Die App wird nicht für Tablets optimiert.

AK1090 Ein Account ist nicht für die Nutzung durch mehrere Nutzer gedacht.

2 Produkteinsatz



2.1 Zielgruppe

Die Privacy Crash Cam verfolgt zwei grundlegende Ziele: Eine Crash Cam für das Smartphone anzubieten und ihren Einsatz mit dem deutschen Datenschutzrecht in Einklang zu bringen. Daraus lässt sich eine eindeutige Zielgruppe ableiten, die sich aus in Deutschland und Österreich ansässigen Auto-, LKW- und Motorrad-Fahrern zusammensetzt. Dabei haben sowohl Viel- als auch Gelegenheitsfahrer Bedarf an der Privacy Crash Cam. Darüber hinaus müssen Nutzer ein Smartphone besitzen, welches den Geräteanforderungen der App gerecht wird. Weiterhin werden Kenntnisse über die Benutzung des Smartphones, Verständnis der deutschen Sprache und ein Internetzugang für die Verwendung des Produktes vorausgesetzt.

2.2 Einsatz

Nachdem die App auf einem kompatiblen Smartphone installiert und ein Nutzeraccount erstellt wurde, findet sie ihren Einsatz im Straßenverkehr. Der Nutzer platziert dazu sein Smartphone mithilfe einer speziellen Halterung an der Frontscheibe seines Kraftfahrzeugs und ermöglicht so der Kamera ein deutliches Bild auf die Straße vor ihr. Darüber hinaus wird das Smartphone nach dem Aufzeichnen von relevantem Videomaterial verwendet, um besagtes Material dem Webservice zum Anonymisieren zu senden.

Das Web-Interface stellt die zweite Instanz dar, mit der der Nutzer direkt interagieren kann. Mit Hilfe dieser kann der Nutzer seinen Account verwalten und das vom Web-Dienst anonymisierte Videomaterial herunterladen.

3 Produktumgebung

	App	Web-Interface	Web-Dienst
Software	Android Version 19 (KitKat 4.4) oder höher	Betriebssystem mit Internetverbindung Browser (min): <ul style="list-style-type: none">• Google Chrome 23• Safari 6• Mozilla Firefox 17	Linux-Betriebssystem (Debian 8) Java Web-Dienst (min): <ul style="list-style-type: none">• Jetty, v5.0• Jersey, v2.x Java in Version 8 Datenbank: PostgreSQL in Version 9.5.5
Hardware	Android Smartphone mit: <ul style="list-style-type: none">• G-Sensor• Kamera• Internet-Verbindung	Computer mit Betriebssystem und Internetverbindung	Ein aus dem Internet erreichbarer Server

4 Funktionale Anforderungen

4.1 App

FA1000 Anzeigen der Anmeldeansicht

Öffnet der Benutzer die App und sind keine Nutzerdaten gespeichert (FA1020), so gelangt er in die Anmeldeansicht, in der er sich anmelden kann. Das Erstellen von Benutzeraccounts ist hier **nicht** möglich.

FA1010 Anmelddaten speichern

Anmelddaten bestehen aus der E-Mail-Adresse und dem Passwort des Nutzers und werden lokal auf dem Gerät abgespeichert. Das Passwort wird als Hash-Code gespeichert.

FA1020 Anmelden in der App

Beim Appstart muss sich der Nutzer zunächst anmelden. Zum Anmelden müssen die Anmelddaten (FA1010) des Nutzers korrekt in die entsprechenden Felder eingetragen sein. Nur verifizierte Nutzer (FA3010) können sich anmelden. Bei falschen Eingaben erhält der Nutzer eine Fehlermeldung. Hat sich ein Nutzer bereits zuvor angemeldet, ohne sich wieder abzumelden, gelangt der Nutzer direkt zur Kamera-Ansicht. Die Überprüfung der gespeicherten Anmelddaten erfolgt erst beim Hochladen von Videodaten auf den Server (FA1160).

FA1030 Abmelden von einem Benutzeraccount

Klickt ein Benutzer im Menü auf "abmelden", so wird er auf die Anmeldeansicht (FA1000) geleitet und seine lokalen Anmelddaten (FA1010) vom Gerät gelöscht.

FA1040 Ausführen des Beobachtungsmodus

Die Kamera kann sich bei aktiver Kamera in zwei Modi befinden: Im Beobachtungsmodus oder im Aufnahmemodus (FA1090). Im Beobachtungsmodus werden Kamerabilder nichtpersistiert (FA1110) sondern nur der Ringpuffer (FA1100) beschrieben. Die G-Sensor-Daten werden ausgewertet und es wird auf einen charakteristischen Ausschlag des G-Sensors (FA1070), oder manuelles Auslösen (FA1080) gewartet.

FA1050 Anzeigen des Statussymbols

Der aktuelle Kameramodus wird dem Nutzer durch ein blinkendes Statussymbol am Bildschirmrand visualisiert. Im Beobachtungsmodus hat es eine grüne Farbe, im Aufnahmemodus hat es eine rote Farbe.

FA1060 Stoppen der Beobachtung

Wenn der Benutzer die Kamera-Ansicht (FA1140) während der Beobachtung verlässt, oder die App schließt, wird die Beobachtung automatisch beendet.

FA1070 Durch G-Sensor ausgelöster Übergang in den Aufnahmemodus

Werden die in (NA1020) - (NA1040) definierten Richtwerte des G-Sensors überschritten, während die App die Kamera-Ansicht (FA1140) anzeigt, geht die Kamera in den Aufnahmemodus über (FA1090).

FA1080 Manueller Übergang in den Aufnahmemodus

Befindet sich die Kamera im Beobachtungsmodus (FA1040), geht sie nach doppeltem Tippen auf die Vorschaufläche der Kamera-Ansicht (FA1140) in den Aufnahmemodus (FA1090) über.

FA1090 Ausführen des Aufnahmemodus

Im Aufnahmemodus wird der Ringpuffer zunächst für 30 Sekunden beschrieben (FA1100) und anschließend der komplette Inhalt des Puffers im Hintergrund persistiert (FA1110). Weitere G-Sensor-Ausschläge, sowie Nutzereingaben werden während sich die Kamera im Aufnahmemodus befindet ignoriert. Die Messwerte des G-Sensors, Zeit und Auslöseart ((FA1070), (FA1080)) werden in die Metadaten der Videodatei geschrieben. Nach Ablauf der erwähnten 30 Sekunden wechselt die Kamera wieder zurück in den Beobachtungsmodus (FA1040).

FA1100 Ringpuffer beschreiben

Im Beobachtungsmodus (FA1040) wird der Ringpuffer mit den Videodaten der Kamera beschrieben. Die Tonspur wird verworfen. Die auf dem Ringpuffer vorhandenen Daten sind nicht verschlüsselt und daher dem Benutzer auch nicht zugänglich. Der Ringpuffer hält bis zu einer Minute Videomaterial (NA1000).

FA1110 Video persistieren

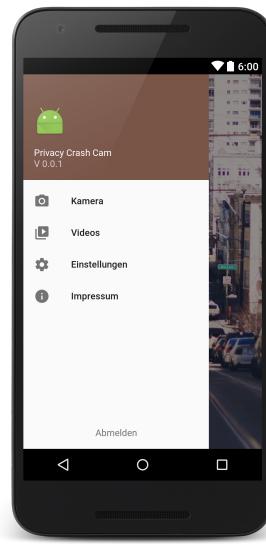
Beim Persistieren, werden die Videodaten zunächst verschlüsselt (FA1120) und daraufhin auf dem internen Speicher hinterlegt.

FA1120 Verschlüsseln eines Videos

Dem Nutzer zugängliche Videodaten werden durch das unter 10.2 beschriebene hybride Verschlüsselungsverfahren verschlüsselt.

FA1130 Anzeigen des Menüs

Drückt der Benutzer den “Menü-Button” in der oberen linken Ecke des Bildschirms, so öffnet sich das Menü. Wenn sich die Kamera im Beobachtungsmodus befindet, während das Menü geöffnet wird, wird die Aufnahme nicht gestoppt. In dem Menü hat der Benutzer die Möglichkeit zwischen den verschiedenen App-Ansichten Kamera-Ansicht (FA1140), Liste der persistierten Videos (FA1150), Einstellungs-Ansicht (FA1200) und Impressum-Ansicht (FA1210) zu wählen, oder sich abzumelden (FA1030).

**FA1140 Anzeigen der Kamera-Ansicht**

Wenn sich ein Benutzer gerade angemeldet hat oder im Menü die Option “Kamera” wählt, so gelangt er zur Kamera-Ansicht. Dort sieht er die Vorschau seines Kamerabildes. Zudem gelangt er automatisch in den Beobachtungsmodus (FA1040).

FA1150 Anzeigen der Liste der persistierten Videos

Wählt der Benutzer im Menü die Option “Videos”, so gelangt er zu einer Ansicht, in dem ihm seine persistierten (FA1110) Videos chronologisch aufgelistet werden. Der Nutzer kann dort Videos hochladen (FA1160), löschen (FA2070), oder Videoinformationen einsehen (FA1190).

FA1160 Hochladen von gespeicherten Videos

Wenn der Nutzer auf den “Upload-Button” klickt, so wird ein Bestätigungsdialog geöffnet. Falls der Benutzer bestätigt, schickt die App eine Anfrage an den Server (FA1160) das Video hochzuladen. Bricht der Benutzer den Dialog ab, bleibt er in der Listenansicht seiner Videos. Falls beim Hochladen ein Fehler auftritt, wird eine Fehlermeldung der App bzw. die vom Server gesendete Fehlermeldung angezeigt.

FA1170 Löschen von gespeicherten Videos

Klickt der Benutzer auf das “Löschen-Symbol”, so wird ein Bestätigungsdialog geöffnet. Falls der Benutzer bestätigt, wird das Video aus der Liste seiner persistierten (FA1110) Videos entfernt und vom Gerät gelöscht. Bricht der Benutzer den Dialog ab, bleibt er in der Listenansicht seiner Videos.

FA1180 Anzeigen einer Benachrichtigung zum Löschen von Videos

Beim Anmelden und bei jedem Appstart wird geprüft, ob persistierte (FA1110) Videos bereits seit über 4 Wochen auf seinem Gerät gespeichert

sind. Ist dies so, wird ihm ein Dialog angezeigt, der ihn auf diesen Umstand hinweist. Dort wird ihm angeboten, das Video zu löschen (FA1170). Bricht er den Dialog ab, gelangt er wie üblich in die Kamera-Ansicht (FA1140).

FA1190 Einsehen von Video-Daten der verschlüsselten Videos

Klickt der Benutzer lange auf ein Video, wird ein Fenster geöffnet, das dem Benutzer die Video-Metadaten (Erstellungsdatum, Größe, Auflösung, Dauer, Auslösseart, G-Sensor-Daten) als Dialog anzeigt. Schließt der Nutzer den Dialog, kehrt er zu der Liste seiner Videos (FA1150) zurück.

FA1200 Anzeigen der Einstellungen

Wählt der Benutzer im Menü die Option "Einstellungen", so werden dem Nutzer die Einstellungen (Auflösung, Bildwiederholrate, Größe Ringpuffer) angezeigt. Diese sind mit Standardparametern festgelegt.

FA1210 Anzeigen rechtlicher Informationen

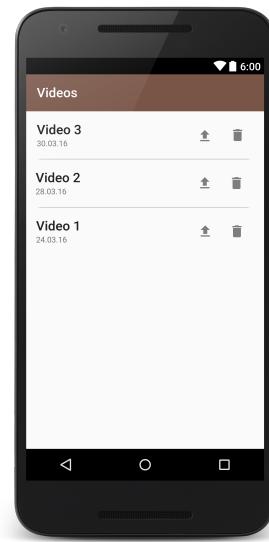
Wählt der Benutzer im Menü die Option "Impressum", gelangt er zur Impressums-Ansicht. Von dort kann er sich das Impressum (FA1220) und die Datenschutzerklärung (FA1230) anzeigen lassen.

FA1220 Anzeigen des Impressums

Wählt der Benutzer "Impressum" auf der Impressum-Ansicht, wird ein Dialog angezeigt, der das Impressum anzeigt.

FA1230 Anzeigen der Datenschutzerklärung

Wählt der Benutzer "Datenschutzerklärung" auf der Impressum-Ansicht, wird ein Dialog angezeigt, der die Datenschutzerklärung anzeigt.



4.2 Web-Dienst

FA2000 Empfangen eines Videos von der App

Bekommt der Web-Dienst eine Anfrage von der App, ein Video hochzuladen, so überprüft er zunächst, ob er die Anfrage bearbeiten kann, oder ob bereits zu viele andere Anfragen gestellt wurden (NA2000). Ist dies nicht der Fall, so entschlüsselt er das Video (FA2010) und beginnt die Anonymisierung (FA2020). Bei Fehlern bei der Anfrage bzw. wenn der Server die Anfrage annimmt, beantwortet der Server die Anfrage mit einer Fehlermeldung bzw. Erfolgsmeldung.

FA2010 Entschlüsseln eines empfangenen Videos

Bevor der Web-Dienst die Bearbeitung des Videos beginnt, entschlüsselt er das empfangene verschlüsselte Video 10.2. Das entschlüsselte Video wird lokal temporär gespeichert.

FA2020 Anonymisierung des Videos

Der Web-Dienst analysiert zunächst das Video (FA2030). Die dadurch gefundenen, für die Anonymisierung relevanten Bildbereiche werden mithilfe von Bildfiltern unkenntlich gemacht.

FA2030 Identifizieren der relevanten Bildbereiche

Der Web-Dienst nimmt das entschlüsselte Video und lässt einen Bildfilter über das Video laufen, der die für die Anonymisierung relevanten Bildbereiche (Gesichter, Nummernschilder, etc.) erkennt.

FA2040 Abspeichern eines anonymisierten Videos

Nachdem das Video anonymisiert wurde, wird es auf dem Server gespeichert und alle temporären Dateien werden gelöscht. Das gespeicherte Video wird zur Videoverwaltung hinzugefügt, damit es vom Benutzer eingesehen und bearbeitet werden kann. Wenn ein Benutzer die maximale Anzahl Videos pro Account (NA2030) überschreitet, wird automatisch das älteste Video des Accounts auf dem Server gelöscht.

FA2050 Speichern eines Accounts

Wenn ein Nutzer sich registriert (FA3010), werden seine Accountdaten auf dem Server gespeichert. Passwörter werden ausschließlich als Hash-Code abgelegt. Zusätzlich wird hinterlegt, dass der Account noch nicht verifiziert wurde.

FA2060 Video herunterladen

Möchte ein Nutzer ein anonymisiertes Video herunterladen (FA3050), so stellt der Server die Videodaten bereit und startet das Herunterladen.

FA2070 Video löschen

Möchte ein Nutzer eines seiner hochgeladenen Videos löschen (FA3060), so werden die Videodaten vom Server gelöscht.

FA2080 Versenden einer Bestätigungsmail

Hat ein Benutzer das Anmeldeformular (FA3010) ausgefüllt, so versendet der Web-Dienst eine Bestätigungsmail. Klickt der Benutzer auf den dort vorhanden Bestätigungslink, so wird der Account verifiziert.

FA2090 Löschen eines Accounts

Wenn der Nutzer seinen Account löschen will, werden zunächst alle von ihm hochgeladenen Videos vom Server gelöscht. Wird gerade ein Video des Benutzers anonymisiert, so wird dieses nach der Anonymisierung nicht gespeichert. Danach werden die Accountdaten des Nutzers gelöscht.

FA2100 Accountdaten ändern

Hat der Nutzer seine Accountdaten geändert (FA3100), so werden die Änderungen entsprechend auf dem Server hinterlegt.

FA2110 Abspeichern eines anonymisierten Videos

Nachdem das Video anonymisiert wurde, wird es lokal auf dem Server gespeichert und alle temporären Dateien gelöscht. Das gespeicherte Video wird der Videoverwaltung hinzugefügt damit es vom Benutzer eingesehen und bearbeitet werden kann. Wenn ein Benutzer die maximale Anzahl Videos pro Account (NA2030) überschreitet, wird automatisch das älteste Video des Accounts auf dem Server gelöscht.

FA2120 Fehlerbehandlung für nicht mehr existierende Daten

Werden bei einer Anfrage Daten angefragt, die nicht mehr existieren, so wird ein Fehler zurückgegeben.

4.3 Web-Interface

FA3000 Anzeigen der Anmeldeansicht

Ruft der Nutzer die Privacy-Crash-Cam-Webseite auf, so gelangt er zu der Anmeldeansicht. Dort kann sich der Benutzer anmelden (FA3020) oder sich registrieren (FA3010).

FA3010 Erstellen eines Benutzeraccounts

Klickt der Benutzer auf "Account erstellen" so öffnet sich der Registrierungsdialog. Dort wird der Nutzer gebeten eine E-Mail Adresse anzugeben. Zudem muss er ein Passwort auswählen und bestätigen. Klickt der Nutzer auf "Registrierung abschließen", werden die Eingaben überprüft. Schlägt dies fehl, bleibt der Benutzer in dem Registrierungsdialog. Nach dem Erstellen eines Benutzeraccounts (FA2050) sendet der Server eine Bestätigungsmail (FA2080).

FA3020 Anmelden auf der Webseite

Zum Anmelden auf die Webseite müssen Benutzername und Passwort korrekt in die entsprechenden Felder eingetragen sein. Nur verifizierte Nutzer (FA2080) können sich anmelden. Bei falschen Eingaben kehrt er zur Anmeldeansicht zurück und erhält eine Fehlermeldung.

FA3030 Anzeigen der Menüleiste

Befindet sich der Nutzer in einer anderen Ansicht als der Anmeldeansicht, so befindet sich am linken Rand der Webseite die Menüleiste. Dort kann der Nutzer die Liste der anonymisierten Videos (FA3040) in seinem Account bearbeiten (FA3080), die Datenschutzerklärung einsehen (FA3120), das Impressum einsehen (FA3110), oder sich abmelden (FA3130).

FA3040 Anzeigen der Liste der anonymisierten Videos

Hat sich ein Benutzer eingeloggt, wird er automatisch auf diese Ansicht weitergeleitet. Hier werden die, vom Nutzer hochgeladenen Videos chronologisch aufgelistet. Der Nutzer kann Videos herunterladen (FA3050), löschen (FA3060), oder die Videoinformationen einsehen (FA3070).

FA3050 Herunterladen von anonymisierten Videos

Durch einen Klick auf das “Herunterlade-Icon” wird ein Speicherdialog geöffnet. Nachdem der Nutzer einen Speicherort ausgewählt hat, wird das Video heruntergeladen (FA2060). Bricht der Benutzer den Dialog ab, bleibt er in der Listenansicht seiner Videos.

FA3060 Löschen eines anonymisierten Videos

Durch den Klick auf das “Löschen-Symbol” wird ein Bestätigungsdialog geöffnet. Falls der Benutzer bestätigt, wird das Video aus der Liste seiner hochgeladenen Videos entfernt und vom Server gelöscht (FA2070). Bricht der Benutzer den Dialog ab, bleibt er in der Listenansicht seiner Videos. Videos werden auch gelöscht nachdem der Nutzer mehr Videos hochgeladen hat als zulässig (NA2030) ist. Dabei wird das älteste Video zuerst gelöscht.

FA3070 Einsehen von Video-Daten der anonymisierten Videos

Klickt der Benutzer auf das “Info-Symbol”, so wird ein Fenster geöffnet, das dem Benutzer die Video-Metadaten (Erstellungsdatum, Datum der Anonymisierung, Größe, Auflösung, Dauer) anzeigt.

FA3080 Bearbeiten eines Benutzeraccounts

Klickt ein Benutzer in der Menüleiste auf “Account bearbeiten”, so wird ein Fenster geöffnet, in dem der Nutzer auswählen kann, ob er seine Accountdaten ändern oder seinen Account löschen will.

FA3090 Account löschen

Klickt der Benutzer im Fenster (FA3080) auf “Account Löschen”, so öffnet sich ein Bestätigungsdialog, in dem der Benutzer gefragt wird, ob er wirklich seinen Account löschen will. Bestätigt dieser, so gelangt er zu der Anmeldeansicht (FA3000) und sein Account wird gelöscht (FA2090).

FA3100 Accountdaten bearbeiten

Klickt der Benutzer in dem Fenster (FA3080) auf “Accountdaten ändern”, so kann er sein Passwort ändern. Dies macht er, indem er zunächst in ein Feld sein altes Passwort und danach in zwei Felder sein neues gewünschtes Passwort eingeht. Stimmt das alte Passwort und stimmen die zwei Felder für das neue Passwort überein, so werden die Daten auf dem Server entsprechend geändert (FA2100).

FA3110 Anzeigen des Impressums

Klickt der Benutzer in der Menüleiste auf “Impressum”, so wird eine Sicht geöffnet, in der der Nutzer das Impressum einsehen kann.

FA3120 Anzeigen der Datenschutzerklärung

Klickt der Benutzer in der Menüleiste auf “Datenschutz”, so wird eine Sicht geöffnet, in der der Nutzer die Datenschutzerklärung und die AGB einsehen kann.

FA3130 Anmelden von der Webseite

Klickt ein Benutzer in der Menüleiste auf “Abmelden”, so wird er auf die Anmeldeansicht (FA3000) zurückgeleitet. Schließt ein Nutzer die Webseite, so wird er automatisch ausgeloggt.

5 Produktdaten

Bei der Verwendung des Produktes werden vom jeweiligen Teil der Software Daten erhoben und entsprechend auf dem Server oder dem Smartphone abgelegt.

5.1 App

PD1000 Kundendaten

Es wird die E-Mail Adresse des Kunden abgelegt.

PD1010 Einstellungen

Es werden Einstellungen der Kamera, die aus Auflösung, Bilder pro Sekunde und Ringpufferlänge bestehen, gespeichert.

PD1020 Ringpuffer

Es wird eine Minute Videomaterial im Ringpuffer gespeichert.

PD1030 Videodaten

Neben den aufgezeichneten Videodaten werden Zeit und Auslöseart in die Metadaten des Videos gespeichert.

5.2 Web-Service

PK2000 Videodaten

Es werden neben den Videodaten Zeit und Auslöseart in die Metadaten des Videos gespeichert. Die Daten werden nach einer bestimmten Zeit wieder gelöscht.

PK2010 Nutzerdaten

Es werden die E-Mail-Adresse und der Hash-Code des Passwortes des Nutzers in einer Datenbank gespeichert. Jeder Nutzer bekommt eine einzigartige ID zugewiesen.

5.3 Web-Interface

PK3000 Daten

Es werden keine Daten auf dem Web-Interface gespeichert. Alle Informationen werden mit REST-Anfragen vom Web-Dienst abgerufen.

6 Nichtfunktionale Anforderungen

6.1 App

NA1000 Ringpuffer-Kapazität

Der Ringpuffer speichert eine Minute an Video-Daten.

NA1010 Zusatzspeicher nach Auslösen

Nach Auslösen des G-Sensors/Speicherbutton werden die folgenden 30 Sekunden aufgenommen und danach der volle Inhalt des Ringpuffers persistiert.

NA1020 G-Sensor Empfindlichkeit frontal

Der G-Sensor soll bei einer Vorwärts-/Rückwärts-Bewegung beim überschreiten von 3 G auslösen.

NA1030 G-Sensor Empfindlichkeit horizontal

Der G-Sensor soll bei einer Links-/rechts Bewegung beim Überschreiten von 3 G auslösen.

NA1040 G-Sensor Empfindlichkeit vertikal

Der G-Sensor soll bei einer Auf-/Ab Bewegung beim Überschreiten von 4 G auslösen.

NA1050 Videokapazität der App

Ein Benutzer kann beliebig viele Videos in der App speichern und verwalten.

NA1060 Benachrichtigung zum Löschen

Die Benachrichtigung zum Löschen eines Videos soll 10 Tage nach dessen Speicherung erfolgen.

6.2 Web-Dienst

NA2000 Parallelle Zugriffe

Es sollen bis zu 4 Videos parallel anonymisiert werden können.

NA2010 Gleichzeitiger Zugriff auf den Web-Dienst

Es sollen bis zu 10 Anfragen gleichzeitig vom Web-Dienst bearbeitet werden können. Dabei werden Anfragen zur anonymisierung in (NA2000) getrennt betrachtet.

NA2020 Benutzerkontenkapazität

Es sollen bis zu 100 Benutzerkonten verwaltet werden können.

NA2030 Videokapazität der Website

Ein Benutzer kann bis zu 10 Videos auf der Website speichern und verwalten.

6.3 Web-Interface

NA3000 Größenanpassung

Die Website soll Responsive-Design umsetzen.

NA3010 Gleichzeitiges Benutzen der Website

Es sollen 10 Benutzer gleichzeitig in der Lage sein, die Website zu benutzen.

7 Globale Testfälle

7.1 Erklärung zur Qualitätssicherung

Wir teilen die Testphase in mehrere Teilphasen ein, um sowohl Komponenten für sich, als auch ihr Zusammenarbeiten separat zu testen. Automatisierte Tests werden das Backend und Frontend testen. Zudem werden manuelle Tests zur Überprüfung der Bedienbarkeit durchgeführt. Das Ziel ist, 80 Prozent des geschriebenen Codes ausführlich zu testen.

7.1.1 Komponenten-Tests

In den Komponenten-Tests werden wir unsere drei Komponenten, die App, das Web-Interface und den Web-Dienst, unabhängig voneinander testen.

7.1.2 Integration-Tests

In den Integration-Tests wird die Kommunikation zwischen den Komponenten getestet. In dieser Phase wird die korrekte Implementierung und Funktion der Schnittstellen sichergestellt.

7.1.3 System-Tests

Die Software wird in einer realen Umgebung installiert und dort unter realen Bedingungen von uns getestet.

7.2 Testszenarien

7.2.1 Komponenten-Tests

App

TK1000 Erstmaliges Starten der App

Beim ersten Start der App wird die Anmeldeansicht angezeigt.

TK1010 Accountanmeldung

In der Anmeldeansicht wird der Benutzer aufgefordert, sich anzumelden. Nach erfolgreicher Anmeldung geht die App in den Beobachtungsmodus über.

TK1020 Menü öffnen

Die App befindet sich im Beobachtungsmodus. Nach Klicken des Menü-buttons wird das Menü angezeigt.

TK1030 Accountabmeldung

Die App zeigt das Menü. Klickt der Benutzer auf “abmelden”, werden die Benutzerdaten von der App gelöscht und er gelangt zur Anmeldeansicht.

TK1040 Starten der App nach Erstanmeldung

Bei Start der App wird die Kameraansicht gezeigt, und die App befindet sich im Beobachtungsmodus.

TK1050 Beobachtungsmodus

Im Beobachtungsmodus wird der Ringpuffer beschrieben.

TK1060 Stoppen des Beobachtungsmodus

Die App befindet sich im Beobachtungsmodus. Wird die App geschlossen oder die Kameraansicht beendet, so wird der Beobachtungsmodus beendet.

TK1070 Aufnahmemodus manuell starten

Die App befindet sich im Beobachtungsmodus. Durch doppeltes Drücken des Bildschirms wird in den Aufnahmemodus gewechselt.

TK1080 Auslösen der Aufnahme

Die App befindet sich im Beobachtungsmodus. Überschreitet die durch den G-Sensor gemessene Beschleunigung, so wird in den Aufnahmemodus gewechselt.

TK1090 Aufnahmemodus

Die App wechselt gerade in den Aufnahmemodus. Nach 30 Sekunden wird der Inhalt des Ringpuffers verschlüsselt auf dem internen Speicherbereich abgelegt. Zudem wird das gespeicherte Video nun unter “Videos” angezeigt.

TK1100 Testen der Verschlüsselung

Es wird die Korrektheit der Ver- bzw. Entschlüsselung der Videos überprüft.

TK1110 Ansicht gespeicherter Videos

Die App befindet sich in der Menüansicht. Nach dem Klicken des “Video”-Feldes werden alle gespeicherten Videos angezeigt.

TK1120 Löschen gespeicherter Videos

Die App zeigt die gespeicherten Videos. Nach dem Klicken des Löschen-Symbols wird ein Bestätigungsdialog gezeigt. Akzeptiert der Nutzer, wird das Video gelöscht.

TK1130 Einstellungen

Die App befindet sich in der Menüansicht. Durch Klicken des Feldes “Einstellungen” werden die Einstellungen angezeigt.

Web-Dienst**TK2000 Anonymisierung des Videos auf dem Web-Dienst**

Der Web-Dienst hat ein zu verarbeitendes Video. Das Video wird zunächst entschlüsselt und anonymisiert, anschließend gespeichert und mit dem Benutzeraccount verknüpft.

Web-Interface**TK3000 Account erstellen**

Beim Öffnen der Anmeldeseite besteht die Option, einen Account zu erstellen. Nach Eingabe gültiger Benutzerdaten wird ein Account angelegt.

TK3010 Anmelden

Durch das korrekte Eingeben existierender Benutzerdaten auf der Anmeldeseite, wird der Benutzer angemeldet und auf die Liste seiner Videos weitergeleitet.

TK3020 Account verwalten

Die Website zeigt die Accountverwaltung an. Der Benutzer führt eine Accountänderung durch. Beim nächsten Anmeldeversuch sind die geänderten Anmeldedaten ungültig.

7.2.2 Integration-Tests

App <-> Web-Dienst**TI1000 Anmelden in der App**

Die App zeigt das Anmeldefenster an. Der Benutzer gibt seine Anmelddaten ein. Die Daten werden an den Web-Dienst geschickt und verifiziert. Ist die Anmeldung erfolgreich, bestätigt der Web-Dienst dies.

TI1010 Video hochladen

Die App zeigt die gespeicherten Videos an. Nach Betätigen des “Hochladen”-Buttons wird das Video an den Web-Dienst gesendet, der es sichert und mit dem Benutzeraccount verknüpft.

Web-Interface <-> Web-Dienst**TI2000 Account erstellen**

Der Benutzer erstellt über das Web-Interface einen Account. Durch den Button “Account erstellen” wird eine Anfrage an den Web-Dienst gesendet, und der Account wird auf der Datenbank hinzugefügt.

TI2010 Accountänderung

Der Benutzer will seine Anmelde Daten ändern. Er gibt seine Änderungen ein und bestätigt diese. Daraufhin wird eine Anfrage des Web-Interface an den Server gesendet, der die Änderungen entsprechend übernimmt.

TI2020 Anzeigen hochgeladener Videos

Der Benutzer gelangt in zu der Liste seiner Videos. Es wird eine Anfrage an den Web-Dienst geschickt, die alle hochgeladenen Videos dieses Benutzers anfordert. Der Web-Dienst antwortet mit den hochgeladenen Videos des Benutzers, und die Videos werden in der Liste angezeigt.

7.2.3 Systemtests

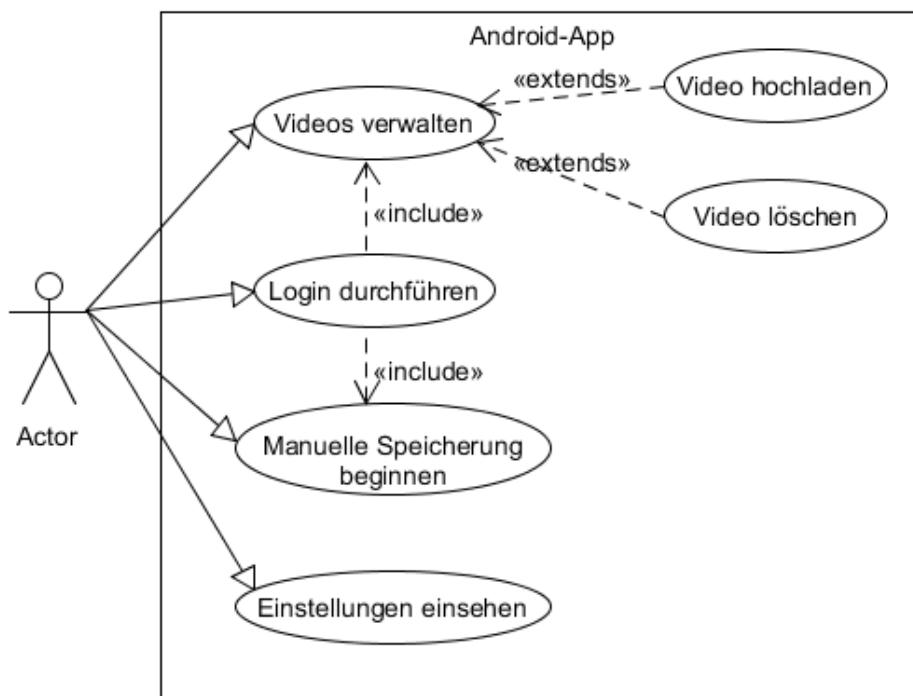
TS1000 Systemtest

Das System wird von uns durch Testen unter realen Bedingungen auf Vollständigkeit und Korrektheit der Funktionalität geprüft. Zudem erfolgt eine Überprüfung der Bedienbarkeit.

8 Systemmodelle

8.1 Anwendungsfälle

8.1.1 Bedienung der Android App



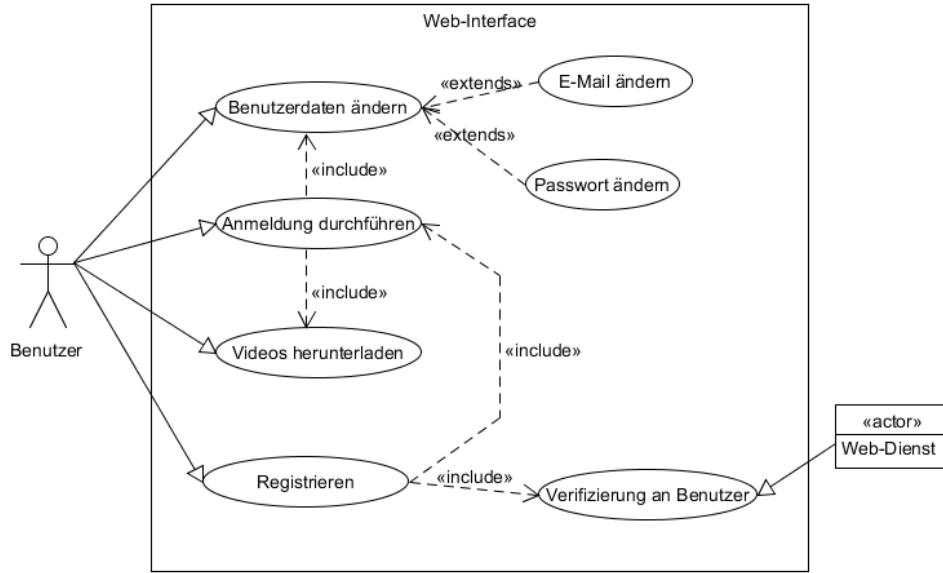
Dieser Anwendungsfall beschreibt die Bedienung der App. Der Benutzer kann hierbei mehrere Aktionen ausführen:

- Login durchführen
- Videos verwalten
- manuelle Speicherung beginnen
- Einstellungen einsehen

Um die App zu nutzen, muss sich der Benutzer zunächst auf der App einloggen. Nach dem Einloggen kann der Benutzer sein aufgenommenes Videomaterial verwalten. Er kann z.B. Videos löschen oder an den Web-Dienst senden. Ist er in

der Beobachtungsansicht, so ist es dem Nutzer möglich, die manuelle Speicherung des Videomaterials zu initialisieren. Außerdem ist es dem Benutzer möglich, die aufnahmespezifischen Einstellungen einzusehen.

8.1.2 Bedienung der Website



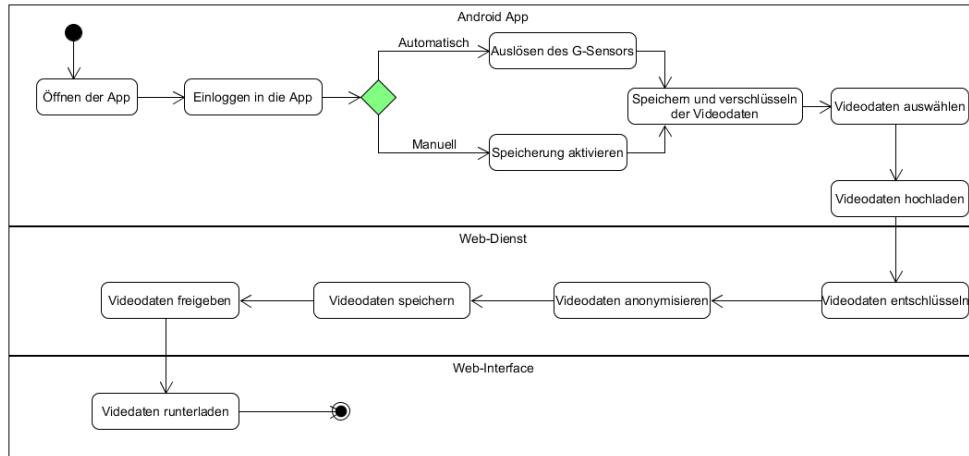
Dieser Anwendungsfall beschreibt die Bedienung der Website. Der Benutzer kann hierbei mehrere Aktionen ausführen:

- Anmelden
- Registrieren
- Benutzerdaten ändern
- Videos herunterladen

Um die Website zu nutzen, muss sich der Benutzer zunächst registrieren. Nach der Registrierung schickt der Web-Dienst eine Verifizierungs-E-Mail an den Benutzer. Nach der Bestätigung kann er sich auf der Webseite anmelden, um deren Funktionen zu nutzen. Ist der Benutzer eingeloggt, kann er seine Benutzerdaten ändern und zuvor hochgeladene, nun anonymisierte Videodateien herunterladen.

8.2 Aktivitätsdiagramm

8.2.1 Vom Appstart bis zur Videofreigabe



Dieses Aktivitätsdiagramm beschreibt den Ablauf vom Start der App, bis zur Freigabe und dem Herunterladen der Videodaten.

1. Öffnen der App
2. Anmelden in der App

Der Benutzer meldet sich mit seinen Anmelddaten in der App an um die Funktionen zu nutzen.

3. Speicherung beginnen

- a) Durch G-Sensor

Die vom G-Sensor gemessene Beschleunigung ist größer als der festgelegte Richtwert.

- b) Manuell

Der Benutzer fordert manuell die Speicherung an.

4. Speichern und verschlüsseln der Videodaten

Nach Beendigung der Aufnahme werden die Videodaten verschlüsselt und daraufhin auf dem Smartphone gespeichert.

5. Videodaten auswählen

6. Videodaten hochladen

Die ausgewählten Videodaten werden an den Web-Dienst gesendet.

7. Videodaten entschlüsseln

8. Videodaten anonymisieren

Nach der Entschlüsselung der Videodaten anonymisiert der Web-Dienst diese.

9. Videodaten speichern

10. Videodaten freigeben

Die Videodaten werden dem Benutzer über das Web-Interface zugänglich gemacht.

11. Videodaten herunterladen

Nun kann der Benutzer sich einloggen und die anonymisierten Videodaten herunterladen.

9 Entwicklungsumgebung

9.1 Entwicklungstools

Android IDE	Android Studio
Java IDE	IntelliJ IDEA
Projektmanagement	Atlassian JIRA
Textverarbeitung	LaTeX
TeX-Distribution	TeXLive
LaTeX Editor	TexMaker
UML Tool	Umlet
Versionskontrolle	Git

9.2 Verwendete Technologien

Programmiersprache (App, Web-Dienst und Web-Interface)	Java 8
Web-Framework	Vaadin 7
Java-Servlet und Http Server	Jetty 9.3.14
Serverkommunikation	RESTful
RESTful-Framework	Jersey 2.24.1
Datenbank	PostgreSQL
Videobearbeitung	OpenCV

9.3 Beschreibung

Android Studio

Für die Implementierung der Android App wird die offizielle Android-Entwicklungsumgebung Android Studio von Google verwendet.

IntelliJ IDEA

IntelliJ IDEA ist eine Java Entwicklungsumgebung, die zusätzlich zu dem üblichen Umfang anderer gängiger IDEs Support für die Entwicklung mit Vaadin, Jetty und Jersey anbietet.

Atlassian JIRA

Atlassian JIRA bietet eine Webanwendung zur Projektverwaltung. Dort werden Aufgaben erfasst, verwaltet und dokumentiert.

LaTeX

Um eine einfache, einheitliche und stabile Formatierung zu gewährleisten wird zur Texterstellung LaTeX anstelle klassischer Texteditoren wie Word verwendet. Umgesetzt wird dies durch die Tex-Distribution TexLive und den Editor TexMaker.

Umlet

Zum einfachen Entwerfen von UML-Diagrammen wird das Tool Umlet verwendet.

Git

Git bietet ein teamfähiges (nicht-lineares) Versionskontrollsystem an, über das alle Daten des Projekts erfasst werden.

Java

Da alle verwendeten Technologien auf Java basieren, verwenden wir für alle Module (App, Web-Dienst und Web-Interface) Java.

Vaadin

Für die Realisierung des Web-Interface wird Vaadin verwendet. Vaadin ermöglicht die Weboberfläche vollständig in Java zu schreiben und bietet moderne responsive Layouts an.

Jetty

Für den Web-Dienst und das Web-Interface läuft auf dem Server Jetty. Jetty bietet eine Kombination aus Java-Servlet und Http Server.

RESTful

Um Anfragen zwischen den einzelnen Modulen zu vereinheitlichen verwenden wir die Kommunikationsschnittstelle RESTful.

Jersey

Für die Umsetzung eines RESTful Web-Dienstes in Java wird das Framework Jersey verwendet.

PostgreSQL

Zur Verwaltung der Nutzerdaten und der hochgeladen Videos wird das Datenbanksystem PostgreSQL eingesetzt.

OpenCV

Zur Erkennung der zu anonymisierenden Bildbereiche, sowie zur Anwendung der Anonymisierungsfilter werden OpenCV Algorithmen verwendet.

10 Anhang

10.1 UI-Demos

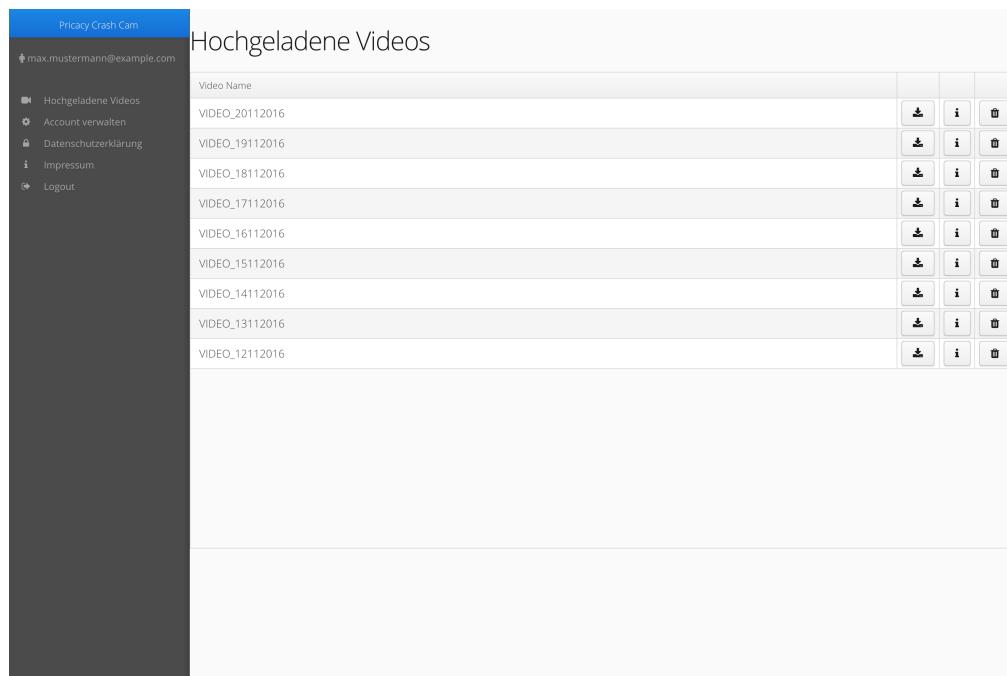


Abbildung 10.1: Web-Interface

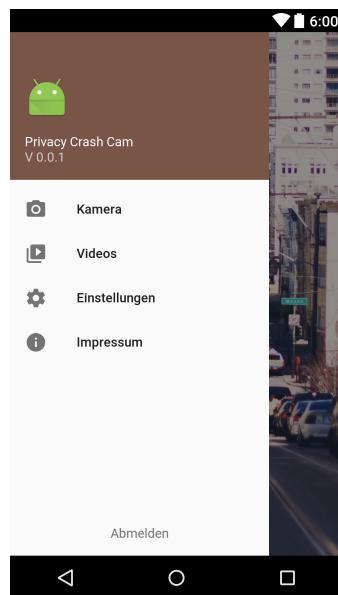


Abbildung 10.2: Menü

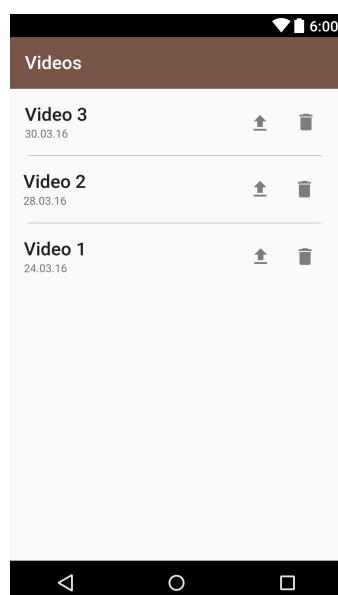


Abbildung 10.3: Videos

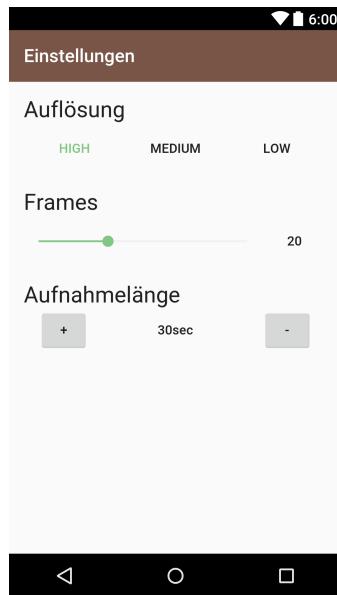


Abbildung 10.4: Einstellungen

10.2 Verschlüsselung

Um den Datenschutz zu gewährleisten, ist die Verschlüsselung eine zentrale Funktion der App und des Web-Dienst. Hierbei müssen die Videos vor der Anonymisierung verschlüsselt gespeichert werden. Dabei wendet die App beim Persisteren eine hybride Verschlüsselung an. Die hybride Verschlüsselung verbindet dabei die Geschwindigkeit von symmetrischer Verschlüsselung **mit der Sicherheit asymmetrischer Verschlüsselung.**

Zunächst wählt die App einen zufälligen symmetrischen Schlüssel. Mit diesem Schlüssel wird das Video symmetrisch verschlüsselt. Anschließend wird der Schlüssel asymmetrisch mit dem öffentlichen Schlüssel des Web-Dienst verschlüsselt. Als kryptographisches Verfahren werden hierbei AES für die symmetrische und RSA für die asymmetrische Verschlüsselung verwendet.



