Datenschutzmechanismen für Gesundheitsspiele am Beispiel von Secure Candy Castle

Corinna Giebler[1], Christoph Stach[1]

Abstract: Smartphones sind mittlerweile ein fester Bestandteil des modernen Lebens. Sie erzeugen, speichern und verarbeiten eine Vielzahl an privaten Daten. Auch im Gesundheitssektor werden sie zunehmend eingesetzt; die dabei entstehenden Daten sind besonders schützenswert. In dieser Arbeit werden daher Konzepte eingeführt, die Nutzern die Kontrolle über ihre Gesundheitsdaten geben. Zu diesem Zweck wird *Secure Candy Castle*, ein Spiel für Kinder mit einer Diabeteserkrankung, das mit einem Berechtigungsmanagementsystem verbunden ist, vorgestellt. Der Nutzer kann den Funktionsumfang des Spiels einschränken, wodurch die App weniger Berechtigungen erhält. Zusätzlich werden für SCC Komponenten entwickelt, die die Interoperabilität von Smartphones mit medizinischen Messgeräten verbessert. Die Evaluation zeigt, dass mit SCC alle aktuellen Probleme von Gesundheits-Apps adressiert werden. Die Konzepte sind generisch und lassen sich auf beliebige andere Gesundheits-Apps anwenden.

Keywords: mHealth-Apps; Datensicherheit; Datenschutz; Datenintegration; Interoperabilität.

1 Motivation

Im Zeitalter der Smartphones werden Daten mobil. Smartphones und Tablets sind fest in den modernen Alltag integriert. Nachrichten, Dokumente und auch Fotos können überall abgerufen, bearbeitet und gespeichert werden. Sensorik ermöglicht es, die Umwelt eines Nutzers zu erfassen und zu verarbeiten. Hierfür werden auf mobile Applikationen – kurz *Apps* – zurückgegriffen. Diese erlauben es, Daten verschiedenster Art zu generieren, anzuzeigen und zu verändern.

Zu diesen Daten gehören inzwischen auch Gesundheitsdaten. Das Stichwort *mHealth* beschreibt eine Form der Gesundheitsfürsorge, bei der Patienten mittels mobiler Technologien, wie beispielsweise Smartphones oder portablen Messgeräten, weitgehend selbstständig die Diagnostik und Therapie durchführen [KP12; Ma16]. Der Patient kann angeleitet von Apps Messwerte erheben, Aktivitäten und Mahlzeiten protokollieren und mithilfe der im Smartphone vorhandenen Sensorik weitere Umwelteinflüsse erfassen. Der so gewonnenen Selbstverantwortung der Patienten wird dabei viel Bedeutung beigemessen [KP12]. Ärzte können entlastet werden und Patienten entwickeln selbst ein Gefühl dafür, was ihnen gut tut und was schadet. Diese Art der Gesundheitsfürsorge eignet sich besonders bei chronischen Krankheiten, wie Diabetes oder Asthma [AM16]. Auch Kinder können von diesem Effekt profitieren [Mi13]. Mithilfe von *Serious Games* kann sowohl Wissen vermittelt als auch Verhalten trainiert werden und so Kinder dazu ermutigt werden, auf sich zu achten und Umwelteinflüsse korrekt einzuschätzen [Wi10]. Martin Knöll hat den Erfolg solcher Spiele evaluiert [Kn10; Kn14].

[1] Universität Stuttgart, Universitätsstraße 38, D-70569 Stuttgart, Vorname.Nachname@ipvs.uni-stuttgart.de

Durch mHealth-Apps werden jedoch sensible Gesundheitsdaten verarbeitet und gespeichert. Für den Nutzer ist oftmals unersichtlich, wie mit diesen Daten verfahren wird. Ein Grund hierfür ist, dass Datenschutzerklärungen oft fehlen [Hü15]. Auch sind viele Apps überprivilegiert, wodurch sie Zugriff auf Daten erhalten können, die für ihre Funktion unerheblich sind [Fe11]. Darum sind Datensicherheit und Datenschutz wichtige Themen bei der Verwendung von Apps – besonders im Bereich der Gesundheitsfürsorge [Ba14]. Dabei bedeutet Datenschutz die Freiheit des Nutzers, über die Verwendung seiner Daten selbst zu entscheiden, während Datensicherheit die technische Sicherheit von Daten bezeichnet, erreichbar durch beispielsweise Verschlüsselung.

Ein weiteres Problem stellt die Interoperabilität zwischen App und externen Datenquellen, wie beispielsweise Messgeräten, dar [Ch12]. Um verschiedene Patienten gleichermaßen unterstützen zu können, muss eine Vielzahl von Messgeräten, beispielsweise Blutzuckermessgeräte, mit der App verknüpfbar sein. Hierfür müssen genormte Schnittstellen geschaffen werden, die eine Einbindung beliebiger Geräte ermöglichen.

In dieser Arbeit wird daher ein Konzept vorgestellt, wie einerseits Datensicherheit und Datenschutz gewährleistet und andererseits die Interoperabilität verbessert werden. Hierfür wird die mHealth-App *Candy Castle* [Kn10] mit einem Datenschutzsystem (in diesem Fall die *Privacy Management Platform*, kurz *PMP* [SM13]) verbunden, welches Mechanismen zur feingranularen Berechtigungsvergabe zur Verfügung stellt. Durch diese Verbindung kann der Nutzer selbst entscheiden, welche Daten er mit der App teilen will und die App passt ihren Funktionsumfang entsprechend an. Mit diesem Konzept wird das Problem der Datensicherheit und des Datenschutzes auf Mobilgeräten direkt adressiert. Zudem werden Erweiterungen für die PMP vorgestellt, die über eine vereinheitlichte Schnittstelle die Integration unterschiedlicher medizinischer Datenquellen (z. B. verschiedene Blutzuckermessgeräte) unterstützen. Eine weitere Erweiterung der PMP führt eine Analyse der medizinischen Daten durch, um so neues Wissen aus gesammelten Daten ableiten zu können und als Grundlage für Therapie und Behandlung genutzt werden. Die vorliegende Arbeit basiert auf den Ergebnissen meiner Bachelorarbeit [Gi16] und erweitert diese um einige Aspekte.

Der Rest dieser Arbeit ist wie folgt aufgebaut: In Abschnitt 2 werden zunächst verschiedene Gesundheitsspiele und ihr Umgang mit sensiblen Daten betrachtet. Die PMP ist in Abschnitt 3 näher beschrieben. In Abschnitt 4 werden anhand des Ablaufes einer überarbeiteten Version von Candy Castle die verwendeten Daten analysiert und die benötigten Schutzmechanismen ausgearbeitet. Die erarbeiteten Konzepte werden anschließend in Abschnitt 5 evaluiert. In Abschnitt 6 folgt eine Zusammenfassung und ein Ausblick auf zukünftige Arbeiten.

2 Verwandte Arbeiten

Mobile Geräte und Apps können für alle Arten von Gesundheitsthemen genutzt werden [Si12]. Dadurch sind mHealth-Apps in der Lage, die gesamte Spannbreite der ärztlichen Aufgaben unterstützend zu begleiten: Prävention, Diagnose, Therapie und Nachsorge. Speziell im Bereich der Diabetesfürsorge gibt es hier bereits verschiedene Apps.

In den Bereich der Prävention und Nachsorge gehören dabei Apps, die eine aufklärende Rolle übernehmen und zu den wichtigsten Fragen bezüglich Diabetes eine Antwort liefern können (z. B. *Making Chocolate-covered Broccoli* [Gl10] oder *Power Defense* [Ba12]). Bei diesem App-Typ spielen Datenintegration oder -schutz keine Rolle, da hier nur informative Lerninhalte weitergegeben und keine nutzerbezogenen Daten verarbeitet werden. Externe Geräte müssen daher nicht angebunden werden, wodurch keine Interoperabilität nötig ist.

Für Diagnose-Apps werden Gesundheitsdaten benötigt. Dadurch können weitere Einsichten in den Krankheitsverlauf gewonnen werden, z. B. um das Essverhalten eines Patienten zu analysieren [Or13]. Hier werden viele gesundheitsbezogene Daten mit der App und gegebenenfalls anderen externen Instanzen ausgetauscht. Daher sollte der Datenschutz hier eine besonders wichtige Rolle einnehmen. Auch die Interoperabilität spielt hier eine Rolle, da aus Gründen der Nutzerfreundlichkeit eine Anbindung von Messgeräten von Vorteil sein kann.

Im Bereich der Therapie werden Gesundheitsdaten analysiert, um Gegenmaßnahmen einzuleiten. Ein Beispiel hierfür ist eine automatisch gesteuerte Insulinpumpe [Cu11]. Je mehr Kontextdaten dieser zur Verfügung stehen, desto besser kann die Insulinmenge bestimmt und gegebenenfalls auf Veränderungen reagiert werden. So kann beispielsweise durch hohe Lautstärken auf einen erhöhten Stresslevel geschlossen werden, welcher sich direkt auf die benötigte Insulinmenge auswirken kann. Um möglichst genaue Diagnosen stellen zu können, werden große Mengen an Gesundheitsdaten benötigt und Datenmanipulation muss ausgeschlossen werden, da dies schwerwiegende gesundheitliche Folgen haben kann. Außerdem müssen Daten korrekt in die Analyse einfließen und Analyseergebnisse korrekt an externe Geräte weitergeleitet werden. Daher ist die Lösung des Interoperabilitätsproblems hier von enormer Wichtigkeit.

Es zeigt sich, dass Datenschutz bei Diagnose- und Therapie-Apps besonderer Aufmerksamkeit bedürfen. *mySugr*[2] ist dabei eine der wenigen Apps, die dies konsequent umsetzt und dafür zertifiziert wurde. Jedoch hat auch hier der Nutzer keine Kontrolle über seine Daten und muss darauf vertrauen, dass die App sich an die gemachten Versprechen hält. Im Folgenden wird daher beschrieben, wie die PMP erweitert werden kann, damit sie als Basis für mHealth-Spiele fungiert, den Datenschutz und die Datensicherheit gewährleistet und das Interoperabilitätsproblem löst.

Dabei ist der Anwendungsfall „Diabetes-App“ beispielhaft gewählt. Auch für andere chronische Krankheiten gibt es mHealth-Apps, z. B. für Asthma [Ni12] oder Parkinson [Sa13]. Die präsentierten Konzepte lassen sich auch auf diese Bereiche anwenden.

3 Die PMP

Mit der PMP können Apps feingranular eingeschränkt werden. Beispielsweise kann ein Nutzer so festlegen, ob und wie eine App GPS-Daten sammeln und verarbeiten kann. Möchte er nicht, dass diese Daten gesammelt werden, kann er die entsprechende Funktion über die PMP deaktivieren. Ebenso ist es möglich, Daten mit reduzierter Genauigkeit an eine App weiterzugeben. Dies

[2] https://mysugr.com/apps

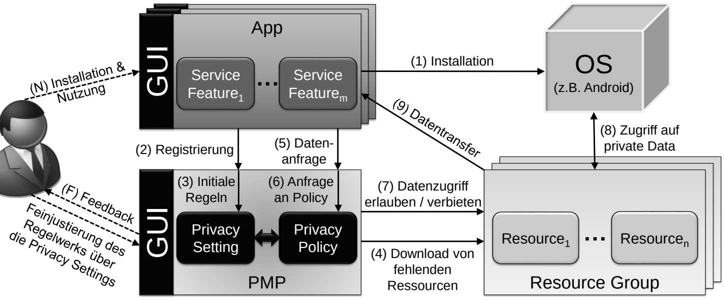


Abb. 1: Die Arbeitsweise der PMP [SM15]

schränkt die Servicequalität der App zwar ein, der Nutzer weiß allerdings jederzeit, welche Daten von welcher App wie verwendet werden können.

Abb. 1 stellt die Arbeitsweise der PMP dar. Damit Apps mit der PMP zusammenarbeiten können, müssen sie sich zunächst bei der PMP registrieren (1 & 2). Mithilfe von so genannten *Privacy Settings* kann der Nutzer nun beliebige Funktionen der App aktivieren, deaktivieren oder auch einschränken (3). Zu diesem Zweck bietet die App ihre grundlegenden Funktionen als *Service Features* an. Diese werden mit der PMP auf so genannte *Ressourcen* abgebildet. Ressourcen stellen dabei Schnittstellen zu Systemfunktionen oder -daten dar. Ressourcen und PMP stammen dabei aus einer vertrauenswürdigen Quelle. Zusätzliche Ressourcen können bei Bedarf nachinstalliert werden (4). Will die App ein durch die PMP verwaltetes Service Feature verwenden, muss sie die passende Methode der zugehörigen Ressource aufrufen (5). Bei einem solchen Aufruf prüft das Managementsystem der PMP, welche Privacy Settings gesetzt sind. Dies geschieht mithilfe der *Privacy Policy*, dem Regelwerk der PMP (6). Je nachdem wird die geforderte Funktion ausgeführt, Filter zur Reduktion der Datengenauigkeit angewandt oder aber Dummy-Daten an die App gesendet (7 – 9). Dies verhindert einen Absturz der App, sollte ein Nutzer die angefragten Daten nicht mit der App teilen wollen. Informationen zur PMP finden sich in der Literatur [SM13; SM14; St15a].

4 Secure Candy Castle

Als Grundlage für den Forschungsprototypen von Secure Candy Castle (SCC), einem sicheren Gesundheitsspiel, dient das Spiel *Candy Castle* [Kn10; SS12]. Es handelt sich dabei um ein mobiles Diabetestagebuch für Kinder. Die Aufgabe des Spiels ist es, den Nutzer dazu zu motivieren, regelmäßig Messungen an möglichst verschiedenen Orten vorzunehmen. Die Verbindung zwischen Messwerten und GPS-Koordinaten kann anschließend für die Analyse von Umwelteinflüssen auf die Behandlung von Diabetes verwendet werden [KM12]. Da es für Kinder gedacht ist, ist Candy Castle übersichtlich und verständlich gestaltet. Jede Eintragung einer Messung gibt Punkte, die den Spieler motivieren sollen. Um allerdings eine Motivation für

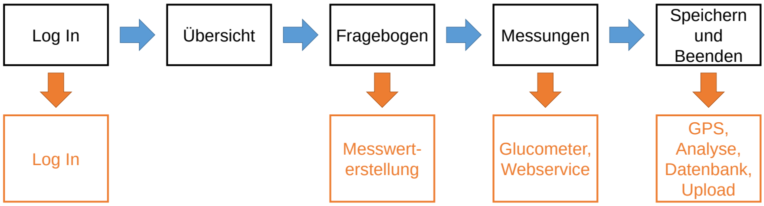


Abb. 2: Ein exemplarischer Ablauf einer Gesundheits-App

regelmäßige Messungen zu bieten, greifen einmal täglich *dunkle Mächte* an, die dem Spieler Punkte abziehen und so neue Messungen erforderlich machen.

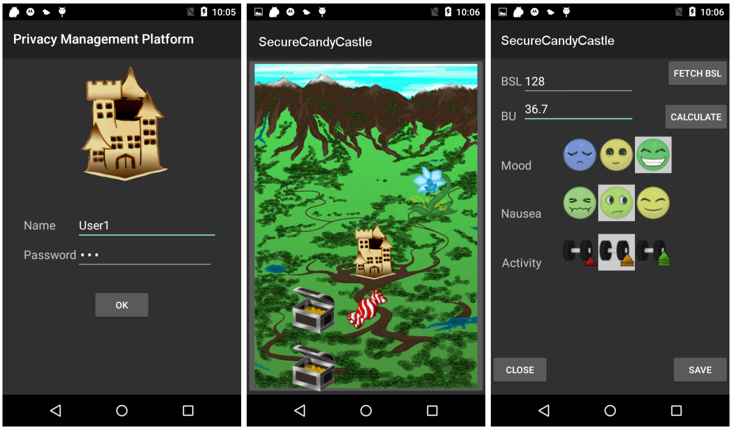
Da in einem solchen Tagebuch viele sensible Daten verwaltet werden, bietet sich der Einsatz der PMP hier an. Eltern können gemeinsam mit ihrem Kind auswählen, welche Funktionen der App erlaubt sein sollen. So kann beispielsweise die Sammlung von GPS-Daten eingeschränkt oder ganz abgeschaltet werden. Auch Berechtigungen wie zur Verbindung mit dem Internet können über die PMP bequem erteilt oder entzogen werden.

Dies bietet zwei große Vorteile: Zum einen kann die App auf den Nutzer angepasst werden. Ist z. B. die Sammlung von GPS-Koordinaten nicht erwünscht, kann diese Funktion deaktiviert werden. Auch die Verbindung zum Internet kann untersagt werden, um die Weitergabe von Daten zu verhindern. Zum anderen können potenziell bösartige Apps nicht ohne Verwendung der PMP unkontrolliert auf Daten zugreifen. Durch die Verbindung mit der PMP allerdings werden alle kritischen Funktionen, die mit sensiblen Daten arbeiten, in Ressourcen ausgelagert, die von vertrauenswürdigen Entwicklern stammen. So erhält eine App zu keinem Zeitpunkt Zugriff auf die Daten und kann auch keine Verbindung mit Dritten aufnehmen, da auch die Kommunikation mit externen oder internen Komponenten durch die PMP reglementiert wird.

Abb. 2 zeigt den Ablauf des Prototypen. Schwarz umrahmt sind die Aktivitäten der mHealth-App dargestellt, während verwendete Ressourcen in Orange abgebildet sind. Zunächst startet die App mit einem Log In Bildschirm (siehe Abb. 3a). Dadurch können mehrere Nutzer die App auf dem selben Gerät verwenden und es wird softwareseitig sichergestellt, dass nur autorisierte Instanzen Zugriff auf die gespeicherten Daten erhalten. Die Anmeldemaske ist als PMP-Ressource implementiert. Dies hat mehrere Vorteile: Einerseits erhält die App keinen Zugriff auf Anmeldedaten. Andererseits können Anmeldemaske und -daten dadurch in anderen Apps wiederverwendet werden, die die entsprechende Ressource einbinden. So muss sich der Nutzer nur einen Benutzernamen und ein Passwort merken, was besonders für Kinder sinnvoll ist. Dieser Ansatz ist an *OpenID*[3] angelehnt.

Nach der Anmeldung gelangt man auf den Kartenbildschirm, dargestellt in Abb. 3b. Hier erhält der Nutzer ein visuelles Feedback zu seinem Messverhalten. Dies geschieht mithilfe des Schlosses, das sich in der Mitte des Bildschirms befindet. Pro Messung erhält der Nutzer Punkte,

[3] http://openid.net/



(a) PMP-Login (b) Spielfeld von SCC (c) Fragebogen von SCC

Abb. 3: Screenshots von SCC

die täglich in einem Angriff der dunklen Mächte um einen bestimmten Betrag verringert werden. Abhängig von dieser Punktezahl, verändert sich die Darstellung des Schlosses. Zudem geben weitere Bilder (wie Blumen, Schätze oder Bonbons) Rückmeldung über die Orte, an denen bereits Messungen vorgenommen werden. Sie stehen dabei in Relation zum Schloss, für das beliebige Koordinaten gewählt werden können. Die Verknüpfung zwischen Blutzuckermesswerten und GPS-Koordinaten ist bereits Teil des Originalkonzepts von Candy Castle und bringt neue Erkenntnisse bezüglich Umwelteinflüssen auf die Gesundheit von Diabetespatienten [KM12; Kn10].

Um Messergebnisse eintragen zu können, stellt SCC einen kindgerechten Fragebogen zur Verfügung (siehe Abb. 3c). Der Nutzer kann hier seinen Blutzuckermesswert, die zu sich genommenen Broteinheiten sowie Laune, Übelkeit und Aktivität erfassen. All diese Werte ermöglichen es dem behandelnden Arzt, genaue Diagnosen und Prognosen zu erstellen; hierbei werden viele sensible Daten gesammelt. Dies ist durch eine sichere Messwertressource realisiert. Diese erfasst die eingetragenen Daten und fügt sie einem Messwertobjekt hinzu, welches verschlüsselt wird. Andere Ressourcen können dieses Objekt entschlüsseln und verarbeiten. Es ist somit sicher vor unbefugtem Zugriff durch die App; diese erhält ausschließlich abstrahierte Daten.

Aus dem Fragebogen heraus ist es dem Nutzer zudem möglich, ein Blutzuckermessgerät per Bluetooth zu verbinden oder sich Broteinheiten über einen Webservice berechnen zu lassen. Diese beiden Funktionen werden ebenfalls durch Ressourcen ausgeführt. Die Glucometer-Ressource regelt den Zugriff auf beliebige Bluetooth-fähige Blutzuckermessgeräte. Standardisierte Protokolle, wie das *Bluetooth SIG Health Device Profile* (siehe ISO/IEEE 11073-20601 Norm), werden von der Ressource direkt unterstützt. Für andere Messgeräte kann diese Ressource erweitert und ähnlich eines Gerätetreibers nachinstalliert werden. Der Abruf der Broteinheiten wird über eine Webservice-Ressource durchgeführt. In der Ressource ist explizit eine externe Datenquelle angegeben, in der diese Information zu unterschiedlichen Lebensmitteln hinterlegt ist. Dadurch ist sichergestellt, dass die App zu keiner anderen Adresse eine Verbindung aufbauen kann.

Zuletzt wird der eben erstellte Messwert gespeichert. Hierfür sind verschiedene Ressourcen eingebunden. Zunächst werden GPS-Koordinaten erfasst und in den Messwert eingefügt. Hierbei kann der Nutzer in der PMP eine Genauigkeit festlegen, mit der der Ort erfasst werden soll. Anschließend wird der eben erstellte Messwert analysiert und eine Meldung an eine angegebene Kontaktperson versandt, sollte der Blutzuckerwert eine bestimmte Grenze unterschreiten. Auch diese Analyse erfolgt in einer Ressource, so dass die App weder Zugang zu den Gesundheitsdaten noch auf die Kontakte benötigt.

Der Messwert wird auf dem Gerät gespeichert und an ein Analyse-Backend für medizinische Daten wie die *ECHO-Plattform* [St15b] übermittelt, auf das der behandelnde Arzt Zugriff hat. Da in einem solchen Backend sehr viele unterschiedliche Sensordaten akkumuliert werden, ist es möglich, dass aus der Kombination dieser Daten neue Informationen über die Patienten abgeleitet werden können. Beispielsweise lassen sich aus Bewegungsprofilen mehrerer Patienten Rückschlüsse auf deren soziale Beziehung ziehen. Um die Geheimhaltung derartiger privater Informationen kümmert sich das PATRON Projekt[4], weshalb mHealth-Apps wie SCC hierfür als idealer Anwendungsfall dienen.

Da all diese Funktionen in der PMP ausgeführt werden, hat die App keinen Zugriff auf sensible Daten wie Aufenthaltsort, Kontaktperson und medizinische Daten. Auch kann sie nicht auf gespeicherte Messwerte zugreifen. Diese werden durch Verwendung des *Secure Data Container (SDC)*, einem verschlüsselten Datencontainer für die PMP [SM15; SM16], geschützt. SCC wurde in Teilen auf der IEEE MDM 2016 demonstriert [St16].

5 Diskussion des Konzeptes von Secure Candy Castle

Nachdem SCC vorgestellt wurde, wird es in dem folgenden Abschnitt evaluiert. Hierfür wird ein Anforderungskatalog von Patienten an Diabetes-Apps herangezogen [Al15] und um die Punkte Datenschutz, Datensicherheit und Interoperabilität erweitert.

Datenschutz: Durch die PMP kann der Nutzer selbst entscheiden, welche Funktionen der App er zulässt und welche er verbietet. Da die App selbst über keine Berechtigungen verfügt und die Ressourcen der PMP aus vertrauensvollen Quellen stammen, kann er sich sicher sein, dass seine Daten nur wie von ihm gewünscht verwendet werden.
Datensicherheit: Mit verschiedenen Datensicherheitskonzepten kann die Datensicherheit gewährleistet werden. Durch die Nutzung des *SDCs* [SM15; SM16] und der Verschlüsselung von Datenobjekten können unautorisierte Instanzen nicht auf die Daten zugreifen.
Interoperabilität: Da in SCC jede Kommunikation mit externen Services über Ressourcen erfolgt, können diese einfach auf die verwendeten Technologien angepasst werden. So kann

[4] http://patronresearch.de/

beispielsweise für verschiedene Messgeräte je eine Ressource zur Verfügung gestellt werden, die eingebunden werden kann. Die App bleibt hiervon unbeeinträchtigt.
Automatischer Logging Prozess: Durch die Anbindung eines externen Messgerätes kann das Erfassen der Messwerte zu einem großen Teil automatisch ablaufen.
Vorhersagen: Die App bindet eine Analyse-Ressource ein, die ein direktes Feedback zu den eingegebenen Messwerten liefern kann. Zudem werden die Daten an einen externen Service weitergeleitet, in dem der behandelnde Arzt ebenfalls Analysen durchführen und Rückmeldungen an die Patienten geben kann.
Intuitive Navigation: Da es sich bei SCC um ein Kinderspiel handelt, wurde bei der Konzeption besonderes Augenmerk auf Verständlichkeit gelegt. Viele Bilder, wenig Text und klare Funktionen bieten intuitive Möglichkeiten, die App zu bedienen.
Unterstützung für neue Geräte und Frameworks: Durch die Nutzung von erweiterbaren Ressourcen zur Kommunikation mit externen Geräten kann die App mit beliebigen Messgeräten kommunizieren.
Verständliche Daten: In SCC werden dem Patienten keine medizinische Daten wie Blutzuckerwerte angezeigt. Diese Daten werden von speziellen Ressourcen analysiert und dem Nutzer wird eine zielgruppengerechte grafische Aufbereitung präsentiert.
Haptisches oder hörbares Feedback: Um diese Funktion zu SCC hinzuzufügen, kann eine Ressource eingebunden werden, die auf die Vibrationsfunktion des mobilen Gerätes zugreift, um so zusätzlich zum visuellen auch ein haptisches Feedback geben zu können.
Positive Ermutigung: Diese geschieht im vorgestellten Konzept mithilfe des Schlosses, welches durch regelmäßige Messung intakt bleibt, sowie durch Bilder, die auftauchen, wenn neue Orte erschlossen wurden.
Erinnerungen: Die Erinnerung geschieht in SCC durch den Verfall des Schlosses. Bricht das Schloss zusammen, muss dringend eine neue Messung erfolgen. Auch könnten Push-Menüs eingebaut werden, um den Nutzer an eine Messung zu erinnern.
Integration von Sensorik: In SCC können über die Ressourcen alle in Smartphones verbauten Sensoren angesprochen werden. Zusätzlich ermöglichen Ressourcen die Kommunikation mit externen Datenquellen, wie beispielsweise tragbare Sensoren.
Launen-Erfassung: Im Fragebogen von SCC können Laune, Übelkeit und Aktivität in jeweils drei Stufen erfasst werden.

SCC erfüllt somit alle Anforderungen an eine Gesundheits-App für Diabetiker.

6 Zusammenfassung

In dieser Arbeit wird das Konzept einer sicheren mHealth-App für Kinder vorgestellt. Durch die Verbindung des Spiels Candy Castle mit der Privacy Management Plattform entsteht eine sichere mHealth-App namens Secure Candy Castle, in welcher der Nutzer selbst entscheidet, welche Funktionen er verwenden möchte. Dadurch kann er selbstständig den Zugriff der App auf seine sensiblen Daten einschränken. Darüber hinaus kann durch die Nutzung der PMP die Interoperabilität mit externen Messgeräten sichergestellt werden, da diese über erweiterbare

Ressourcen ohne das Zutun der App angesprochen werden. Die Evaluation zeigt, dass SCC alle Anforderungen an Datensicherheit, -schutz und Interoperabilität sowie die allgemeinen Anforderungen an mHealth-Apps erfüllt.

Dieses Konzept ist auf andere mHealth-Apps anwendbar. Somit können durch die hier vorgestellte Verbindung zwischen App und PMP weitere sichere Gesundheitsanwendungen erstellt werden, die der Nutzer ohne Angst um seine Daten verwenden kann.

Danksagung. Die in diesem Beitrag vorgestellte Forschungsarbeit entstand aus dem PATRON-Forschungsauftrag, der von der Baden-Württemberg Stiftung finanziert wurde.

Literatur

[Al15] Alexander, S.: mHealth Technologies for the Self-management of Diabetes in the Older Population. SIGACCESS Access. Comput./111, S. 14–18, 2015.

[AM16] Alkhushayni, S.; McRoy, S.: mHealth Technology: Towards a New Mobile Application for Caregivers of the Elderly Living with Multiple Chronic Conditions (ELMCC). In: DH ’16. 2016.

[Ba12] Bassilious, E. et al.: Power Defense: A Serious Game for Improving Diabetes Numeracy. In: CHI EA ’12. 2012.

[Ba14] Bai, Y. et al.: Issues and Challenges in Securing eHealth Systems. Int. J. E-Health Med. Commun. 5/1, S. 1–19, 2014.

[Ch12] Chan, M. et al.: Smart Wearable Systems: Current Status and Future Challenges. Artif. Intell. Med. 56/3, S. 137–156, 2012.

[Cu11] Cukierman-Yaffe, T. et al.: Key elements for successful intensive insulin pump therapy in individuals with type 1 diabetes. Diabetes Research and Clinical Practice 92/1, S. 69–73, 2011.

[Fe11] Felt, A. P. et al.: Android Permissions Demystified. In: CCS ’11. 2011.

[Gi16] Giebler, C.: Privatheit im Gesundheitsspiel Candy Castle, Bachelorarbeit, Universität Stuttgart, 2016.

[Gl10] Glasemann, M. et al.: Making Chocolate-covered Broccoli: Designing a Mobile Learning Game About Food for Young People with Diabetes. In: DIS ’10. 2010.

[Hü15] Hübner, M.: Gesundheits-Apps werden für Chroniker wichtig, Studie, Ärzte Zeitung online, Juni 2015, URL: `https://goo.gl/jUym5W`.

[KM12] Knöll, M.; Moar, M.: The Space of Digital Health Games. Int. J. Comp. Sci. Sport 11/1, 2012.

[Kn10] Knöll, M.: “On the Top of High Towers . . . ” Discussing Locations in a Mobile Health Game for Diabetics. In: MCCSIS ’10. 2010.

[Kn14] Knöll, M. et al.: Wo die Monster leben? Welche Orte und Begleitung haben Einfluss auf das Blutzuckermessen und können zur Entwicklung von Serious Games für Typ-1-Diabetiker beitragen. Diabetologie und Stoffwechsel 9/1, 2014.

[KP12] Klasnja, P.; Pratt, W.: Healthcare in the Pocket: Mapping the Space of Mobile-phone Health Interventions. J. of Biomedical Informatics 45/1, 2012.

[Ma16] Matusiewicz, D.: Mobile Health, Definition, Gabler Wirtschaftslexikon, 2016, URL: `https://goo.gl/AWQNJM`.

[Mi13] Miller, A. D. et al.: Design Strategies for Youth-focused Pervasive Social Health Games. In: PervasiveHealth '13. 2013.

[Ni12] Nikkila, S. et al.: Wind Runners: Designing a Game to Encourage Medical Adherence for Children with Asthma. In: CHI EA '12. 2012.

[Or13] Orji, R. et al.: LunchTime: A Slow-casual Game for Long-term Dietary Behavior Change. Personal Ubiquitous Comput. 17/6, S. 1211–1221, 2013.

[Sa13] Sanders, T. H. et al.: Remote Smartphone Monitoring for Management of Parkinson's Disease. In: PETRA '13. 2013.

[Si12] Siewiorek, D.: Generation smartphone. IEEE Spectrum 49/9, S. 54–58, 2012.

[SM13] Stach, C.; Mitschang, B.: Privacy Management for Mobile Platforms – A Review of Concepts and Approaches. In: MDM '13. 2013.

[SM14] Stach, C.; Mitschang, B.: Design and Implementation of the Privacy Management Platform. In: MDM '14. 2014.

[SM15] Stach, C.; Mitschang, B.: Der Secure Data Container (SDC) – Sicheres Datenmanagement für mobile Anwendungen. Datenbank-Spektrum 15/2, S. 109–118, 2015.

[SM16] Stach, C.; Mitschang, B.: The Secure Data Container: An Approach to Harmonize Data Sharing with Information Security. In: MDM '16. 2016.

[SS12] Stach, C.; Schlindwein, L. F. M.: Candy Castle — A Prototype for Pervasive Health Games. In: PerCom '12. 2012.

[St15a] Stach, C.: How to Deal with Third Party Apps in a Privacy System — The PMP Gatekeeper. In: MDM '15. 2015.

[St15b] Steimle, F. et al.: Design and Implementation Issues of a Secure Cloud-Based Health Data Management System. In: SummerSOC '15. 2015.

[St16] Stach, C.: Secure Candy Castle — A Prototype for Privacy-Aware mHealth Apps. In: MDM '16. 2016.

[Wi10] Wiemeyer, J.: Gesundheit auf dem Spiel? – Serious Games in Prävention und Rehabilitation. Deutsche Zeitschrift für Sportmedizin 61/11, 2010.