Protokoll

Mobile Sicherheit im Gesundheitswesen

Eine Applikation für mehrere Anwendungen auf mobile Endgeräten sollte auch auf 3 Betriebssystemen laufen können. Wir brauchen ein Architekturmodell darunter auch unser Frontend. Ein mobiles Endgerät kann über HTML5 Kameras und Sensoren nicht aufrufen. Native Applikationen laufen nicht auf einem Browser eines Rechners.

Eine Alternative für eine Anwendung wäre ein Hybridanwendung. Diese baut einen Rahmen auf der wir die Funktionen der mobilen Endgeräte nutzen und im Core auf unser HTMl zurückgreifen können.

Eindeutige Identifizierung der Nutzer zB mittels Handysignatur. Sicherheit in Mobilen Anwendungen muss vorher geplant werden mit den passenden Sicherheitsmechanismen darunter Kontrolle, ob Programm auf Gejailbreakten Geräten läuft. Ist dies der Fall oder das Betriebssystem des Geräts hat Sicherheitslücken weil es nicht aktuell ist, sollte der Zugriff auf unsere Applikation gesperrt werden. Für die Implementierung einer solchen Software sollte man spezielle Bibliotheken benutzen, welche unsere Sicherheitsmechanismen bereitstellen.

L1 sind Grundlegende Daten, die nicht hoch sicher sein müssen.

L2 ist sicher, sprich sichere Informationen Bankdaten oder Gesundheitsdaten.

Wir verfolgen somit die Sicherheitsstufe L2.

Wir sollten uns auch überlegen von wem die Mobilen Endgeräte gemanaged werden. Werden sie über ein MDM gemanaged?

Rahmenbedingungen

Bei mobilen Endgeräten kann es Probleme geben, wie z.B. das Verbreiten von sensiblen Daten zum Konzern des Geräts. Es ist keine gute Idee sensible Daten auf dem Gerät bzw auf dem Frontend selber zu speichern, da sie verschlüsselt werden müssen und eine Manipulationsgefahr darstellen. Eine Möglichkeit wäre eine Cloudlösung.

Cloudlösung:

Der Service sollte idealerweise bei uns selber gehostet werden. Externe Anbieter können auch genutzt werden, jedoch sollte man sich beqwusst sein, dass diese nicht immer sehr vertrauenswürdig sind. (SaaS).

Die Core Syteme sollten somit in unserem Wirkungsbereich liegen & die Funktion können wir extern hosten.

Unbehaftete & Behaftete Systeme:

Bsp: unbehaftet: NFC

Bsp: behfatet: Lesen des Chips einer Bankomatkarte

E-Card

E-Card ist jetzt Gino fähig Arzt braucht aber ein Gino fähiges Gerät GINA/GINO Box. Ohne diesem Gerät keinen Zugriff auf die Daten des Patienten kann keine Medikamente auf E-Card laden.

Nachteil der Lösung der SV:

Funktioniert nur bei Ärzten, die die Voraussetzungen und Hardware dafür haben

+ funktioniert nur in Ö (1/3 der Ärzte haben diese Möglichkeit nicht)

E-Government verifiziert User mit der Handysignatur. Die Handy Signatur ist eine Eindeutige Identifizierung des Nutzers. Man spricht dabei von EID die europaweite Gültigkeit hat und so ist auch der E Führerschein aufrufbar und überall nutzbar. E-Card enthält noch keine EID laut ELGA sollte sie dies aber noch können.