OPTIMOS 2.0

OPTIMOS 2.0

Plattform für sichere Identitäten auf Smartphones

1 Förderprojekt vom BMWi
Zusammenarbeit namhafter Industrie- und Forschungseinrichtungen

2 Sicherheit
Nutzung von Hardware-Sicherheitselementen in mobilen Endgeräten

3 Datensouveränität
Unabhängigkeit von Sicherheitsmechanismen der Betriebssysteme und Smartphone-Hersteller

4 Nutzerfreundlichkeit
Einfache Online-Identifikation und Authentifikation mit dem Smartphone

5 Offenes Ökosystem
Nutzung und Weiterentwicklung von Standards und offenen Schnittstellen

6 Vielseitige Anwendung
Sichere Identitäten u. a. für E-Government, Internet of Things und Mobilität

22 namhafte Unternehmen sind bereits an OPTIMOS 2.0 beteiligt

BUNDESDRUCKEREI (Konsortialführer)

8 Projektpartner

14 Assoziierte Projektpartner

Digitale Dienste mit hohen Sicherheitsanforderungen werden mobil

Wir bewegen uns heute in einer digitalen Netzwelt, deren Basis die universelle Präsenz des Smartphones ist – es beschleunigt die Digitalisierung von Dienstleistungen, die vor wenigen Jahren noch in der analogen Welt zuhause waren: Viele Bankdienstleistungen sind ohne Smartphone kaum noch zu erledigen, Smartphone-Dienste haben Stadtpläne und Landkarten für die Navigation verdrängt. Verwaltungsleistungen und hoheitliche Dienste können sich diesem Trend zur „Mobitalisierung" nicht entziehen. Auf internationaler Ebene werden bereits digitale Formate für Führerschein und Reisepass standardisiert. Dies sind die sichtbarsten Beispiele zukünftiger hoheitlicher Anwendungen, die mit Hilfe des Smartphones das grenzüberschreitende Reisen oder die Verkehrsüberwachung vereinfachen werden. Nur durch den Schutz und die Integrität der eigenen mobil genutzten digitalen Identität kann das nötige Vertrauen in innovative mobile Dienstleitungen gewährleistet werden. Dabei darf sich ein mobiles System nicht auf herstellerabhängige Ökosysteme beschränken, sondern muss auf offenen Schnittstellen beruhen. Nur so wird ein Zugang für alle Bürger ermöglicht.

Um das Smartphone für hoheitliche Dienste zu qualifizieren, sind „State-of-the-Art"-Sicherheitstechnologien erforderlich. Sie sollen die Verfügbarkeit von persönlichen Daten und den Schutz der Privatsphäre garantieren. Anwendungen für ein hoheitliches Identitätsmanagement benötigen eine sichere digitale Infrastruktur für sensible personenbezogene Daten.

OPTIMOS entwickelt Sicherheits-architektur für hoheitliche Anwendungen auf Smartphones

Im Rahmen des Förderprojekts OPTIMOS arbeiten namhafte Industrieunternehmen und Forschungseinrichtungen an der Definition einer offenen Sicherheitsarchitektur für mobile Dienste. Gemeinsam realisieren sie auf dem Smartphone eine Plattform für das Daten- und Anwendungsmanagement für Dienste mit hohem Schutzbedarf. Im Projekt entstehen Identitätsdienste zum Beispiel für das E-Government, Carsharing-Dienste und E-Ticket-Anwendungen für den öffentlichen Nahverkehr.

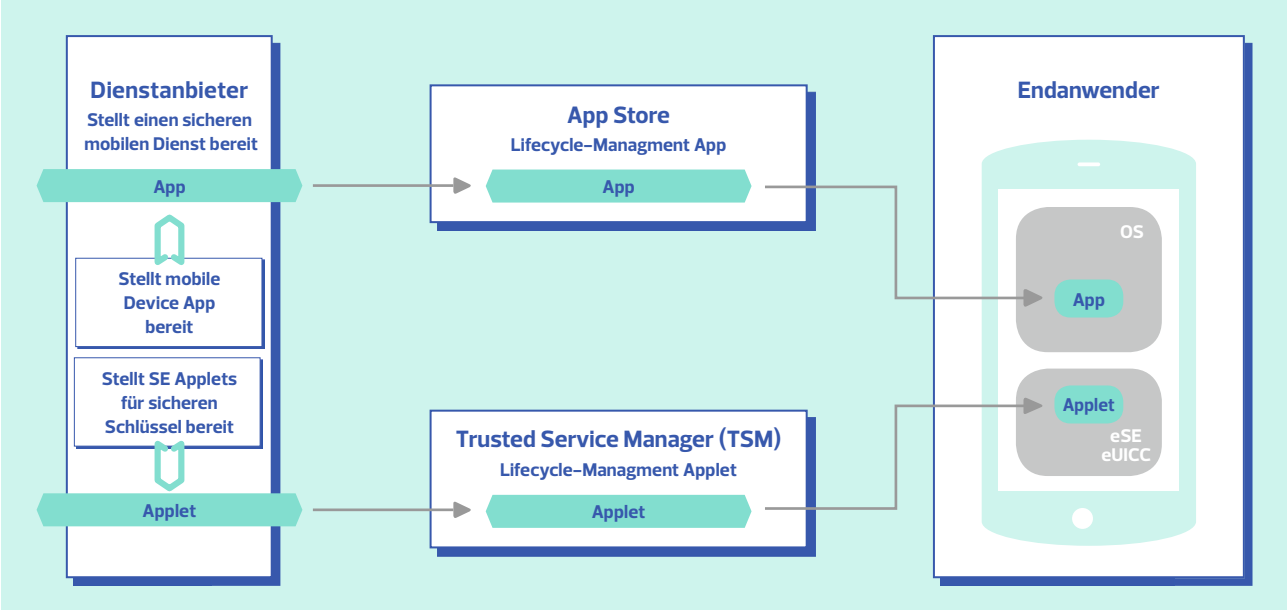
Die technologische Basis von OPTIMOS sind „sichere Zonen" im Smartphone wie das „embedded secure element" (eSE) oder die eSIM. Diese Sicherheitselemente sind gegen Manipulation geschützt und über kryptografische Schlüssel nur für autorisierte Dienste und Anwendungen zugänglich.

Zentrales Element der OPTIMOS-Sicherheitsarchitektur ist ein „Trusted Management System" (TSMS). Diese Plattform übernimmt das Life-Cycle-Management für die Anwendungen auf dem Secure Element und stellt hierzu u. a. einen sicheren Kommunikationskanal zwischen einem Diensteanbieter – z. B. einem E-Scooter-Betreiber – und dem Smartphone des Kunden her. Er prüft und initialisiert den Sicherheitsstatus des Smartphones und überträgt die sensiblen Kundendaten in die „sichere Zone".

Mit den Sicherheitstechnologien des Smartphones schaffen die OPTIMOS-Partner die Voraussetzung für digitale ID-Systeme, die auf europäischer Ebene das Sicherheitsniveau „substantiell" erreichen können. Die Partner bauen auf den digitalen Identitätsattributen des Personalausweises und weiterer europäischer ID-Systeme auf, die den Anforderungen der eIDAS-Verordnung genügen. Eine vom Personalausweis abgeleitete digitale Identität auf dem Smartphone ist für Konsumenten und Diensteanbieter, für Bürger und Verwaltung ein großer Schritt in Richtung Sicherheit und Komfort in der digitalen Netzwelt.

OPTIMOS entwickelt ein offenes Ökosystem

Hoheitliche Anwendungen erfordern eine herstellerunabhängige und diskriminierungsfreie Nutzung der OPTIMOS-Sicherheitstechnologie. Nur so ist die digitale Souveränität eines Staates als Aussteller von Identitätsdaten auf einem Smartphone gewährleistet. Standards und offene Schnittstellen zwischen Diensteportalen im Internet, Hintergrundsystemen und mobilen Endgeräten sind dafür die Grundlage. Nur Technologiehersteller, die mit ihrer Produktstrategie diese Ziele unterstützen, kommen für hoheitliche Anwendungen infrage. Die OPTIMOS-Technologie baut auf offenen Schnittstellen auf und entwickelt diese weiter. Standards für die Qualifikation von Smartphones und für den Zugang zu den „sicheren Zonen" werden zurzeit durch OPTIMOS-Partner und durch das BSI in die internationale Standardisierung eingebracht.



Ver. 01/2019