

Sichere nomadische Personalisierung in konvergenten Netzwerken

(Abstract)

Heinz-Josef Eikerling

Siemens SBS C-LAB
Fürstenallee 11
33 102 Paderborn
Heinz-Josef.Eikerling@c-lab.de

Hintergrund

Mobile Geräte und die dazugehörigen Services und Applikationen boomen und gewinnen nicht nur in der klassischen mobilen Telephonie, sondern auch verstärkt im mobilen Zugriff auf digitalisierte Informationsquellen zunehmend an Bedeutung. Nach heutigen Schätzungen wird es bereits in drei Jahren mehr Geräte geben, die drahtlos mit dem Internet verbunden sind (also im mobilen Einsatz verwendet werden können), als solche, die über das Festnetz angeschlossen sind. Hieraus werden sich zukünftig in nahezu allen Lebensbereichen und Umgebungen neue Geschäftsmodelle ergeben, die ortsabhängige und proaktive, personalisierte Dienste und die Konvergenz von Netzen, Geräten und Diensten nutzen werden.

Mobilität hat dabei verschiedene Ausprägungen, die jeweils den Einsatz spezieller Techniken erfordern. Sie kann sich auf Dienste, Geräte, Applikationen oder Nutzer beziehen. Eine alltägliche Anforderung ist z. B. die Sicherstellung der Portabilität der persönlichen Umgebung eines Nutzers bei einem Kontext-Wechsel (siehe Abbildung 1). Eine solche Umgebung besteht aus (nicht notwendigerweise mobilen) Geräten, entsprechenden Applikationen und darauf zugreifenden Diensten, die der Nutzer optimal auf die lokalen Gegebenheiten und seine persönlichen Präferenzen abgestimmt haben möchte. Eine solche Personalisierung und das Datenmanagement unterliegen dabei Sicherheitsanforderungen, speziell im Hinblick auf die Handhabung personenbezogener Daten.

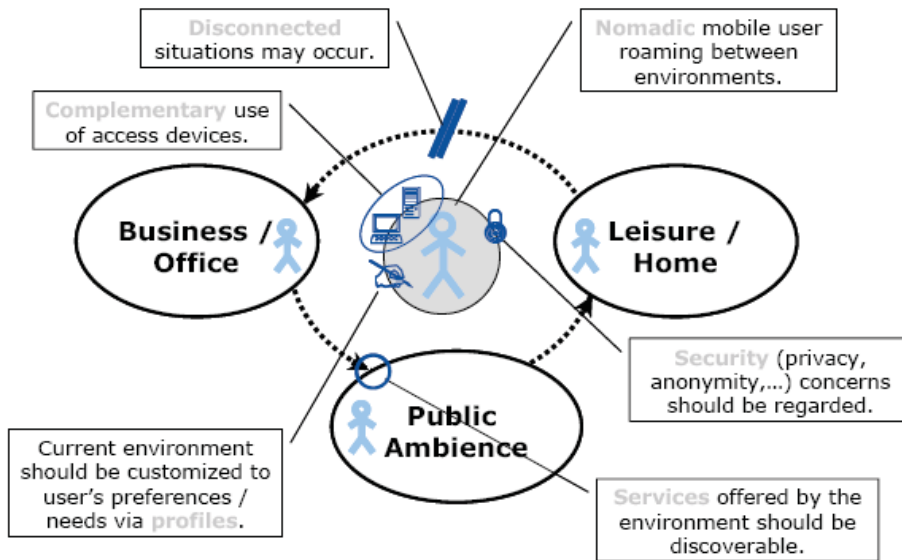


Abbildung 1: Anforderungen an nomadische Personalisierungskonzepte.

Ansatz

Im Rahmen des Projektes UBISEC¹ wurde an der Entwicklung der technischen Voraussetzungen zur umfassenden und sicheren Anwendung von Personalisierung für die Unterstützung nomadischer Nutzer gearbeitet. Die im Projekt entwickelten Konzepte (siehe Abbildung 2) berücksichtigen, dass Profildaten unabhängig vom aktuell verwendeten Speichermedium verlinkt werden können. Hierzu wird ein abgestufter Sicherheitsmechanismus auf Basis von Policies bereitgestellt, der die Nutzer authentifiziert sowie entsprechend Manipulationen an Profildaten autorisiert. Für die Umsetzung dieser Konzepte liegen die folgenden Aspekte speziell im Fokus:

- **Verteilung:** Im Hinblick auf physikalische Grenzen (Speichergröße) ist eine Föderation von Profilen und der Aspekt der Datenverteilung zu betrachten. Informationen zur Identität eines Nutzers können zur Wahrung der Integrität der Daten und der Privatsphäre des Nutzers auf einem speziellen Medium abgespeichert werden (z.B. Smartcard). Extern zu ändernde Daten (z.B. Daten zum Ortskontext des Nutzers) werden über eine Datenbank bereitgestellt.
- **Profile:** Die Personalisierung wird auf Basis von Profildaten (Attribute, Regeln etc.) für die zu personalisierenden Objekte vorgenommen. Die

resultierenden Profile werden bzgl. unterschiedlicher Domänen (Benutzer, Gerät, Kontext, Netzwerk, Dienst, Applikation,...) klassifiziert. Der Zugriff erfolgt über ein einfach adaptierbares, abgesichertes Protokoll (z.B. als zum Schutz vor unautorisierten Zugriffen). Das Profile-Management wurde als einfach retargierbarer Dienst (CMS, *Customisation Management System*) realisiert.

- *Sicherheit*: Bei einer übergangslosen (*seamless*) Mobilität kann die Handhabung von Sicherheitsaspekten durch ein kontinuierlich vorhandenes Netzwerk und darüber zugängliche Dienste geregelt werden. Die nomadische Nutzung stellt eine Herausforderung für das Sicherheitskonzept da, weil sicherheits-relevante Informationen für das Trust-Management auch in Offline-Situationen vorhanden sein müssen. Dafür wurde im Rahmen des Projektes eine ePKI (*Enhanced PKI*) entwickelt, die die Basis der *Access Control Engine* im CMS darstellt.

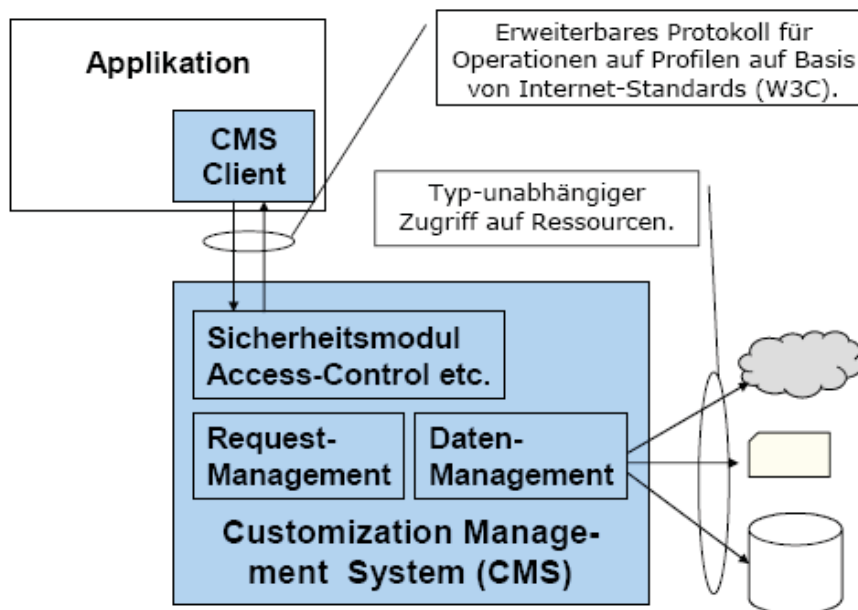


Abbildung 2: Konzept Customization Management System (CMS).

Ergebnisse

Im Rahmen von UBISEC wurde eine Struktur aus kooperierenden Diensten zur Profilverwaltung entwickelt, dessen Ziel die Unterstützung von konvergenten Zugriffsszenarien (B3G, *Beyond 3G*) auf Profildaten darstellt. Diese lassen sich als Softwarekomponenten leicht in Applikationen oder Dienste integrieren, die auf die Informationen zur Personalisierung zugreifen müssen. Das CMS ermöglicht die Verknüpfung von Profildaten über die Grenzen von Speichermedien hinweg.

Im Rahmen von Evaluierungen wurde der Einsatz des CMS für die Realisierung verschiedener Anwendungsfälle betrachtet and analysiert. Durch die Dezentralisierung (nicht nur der Nutzdaten, sondern z.B. auch der Autorisierungsinformation) haben wir insbesondere die Auswirkung der Access Control Engine auf die Zugriffszeiten des CMS untersucht. In typischen Fällen (Autorisierung von als XML-Dateien gespeicherte Profildaten) liegt dieser Overhead bei unter 10% für die Requestverarbeitung.

(Der Vortragstext wurde nicht eingereicht.)