

# Master project “Identity management for shared devices”

## Introduction

Digital identity plays an increasingly bigger role in today’s (online) world. It enables personalization, targeting of content, services and advertisements, connecting to other people (consider e.g. social network sites like MySpace and Facebook) and sharing experiences.

Also identity management technology is being developed rapidly. For example, concepts and technology for identity federation and single sign on have been developed resulting in standards and solutions like SAML, OpenID and CardSpace. These standards have in common that they are PC and web-services focussed. Typically, they do not target typical consumer electronics devices, which have different user interaction and usage patterns. However, it is expected that in the near future identity driven applications will not just live on the PC and online, but will also enter the living room via consumer electronics devices.

For this assignment, consider the application where an Internet connected TV on which multiple people together may enjoy content and (online) services. The TV, service portal and services use identity management solutions like identity federation and single sign on for user convenience. Personalization of content, services and advertisements in this case should be based on multiple user profiles contrary to typical PC scenarios where there is just a single user present. However, this combination is currently not supported by identity management protocols.

This application raises security and privacy issues. This includes the aforementioned protocols, privacy for building the profiles based on user behaviour and managing user profiles for shared devices, but also accountability of individuals and correlation of identities. Although users value their privacy they are preferably not bothered too much with security like authentication, managing many individual access control settings, etc. Unfortunately current solutions do not offer the required privacy and security while also being user-friendly and practical enough.

## Assignment

Analyse the connected TV application and relevant identity management protocols, develop an identity architecture and design (extend) identity management protocols to support sessions with multiple users, and evaluate the result for its privacy and security properties. Besides multi-user support in identity protocols for service personalization, one may consider fast identity and role switching for e.g. payment or content publishing where an individual must be held accountable, etc.

## Candidate

Candidate profile: master student computer science, telecommunications, etc., with interest in security

## Information

Duration: 6 months

Contact person: Paul Koster ([r.p.koster \(AT\) philips.com](mailto:r.p.koster(AT)philips.com))

Location: Philips Research, Information & System Security department  
Eindhoven, The Netherlands