

# Master project “Identity management for experience sharing”

## 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 networking sites like MySpace or Facebook) and sharing experiences (consider e.g. sharing what you are doing via Twitter or location via Socialight).

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 through consumer electronics devices.

For this assignment, consider the experience sharing application where a portable device automatically determines the user’s activity and location, and shares this identity information with people in the user’s social network rendering the information on the recipient’s device. The difference with e.g. Twitter is that this application automates observations and sharing and brings experiences to devices in people’s surroundings.

This experience sharing application raises privacy and security issues. Consider for example the desired level of detail of daily activities and locations particular recipients should be able to receive. This suggests some kind of policy driven approach. Unfortunately current solutions do not offer sufficient privacy and security in combination with being sufficiently user-friendly and practical.

## Assignment

Analyse, design and evaluate the privacy preserving experience (activity and location) sharing system with attention for user-friendly control, privacy and policy management. Consider technical aspects like a policy model and policy management. Potential directions to explore may include community based policy assistants, the fit it in identity management standards, the link to social networks, how to conveniently support multiple experience sharing devices in a home network, 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))  
Philips Research, Information & System Security department  
Location: Eindhoven, The Netherlands