Long Term Cybersecurity research
Summaries of projects granted in the second NWO call for proposals (2014)

Project number	CYBSEC.14.024 / 628.001.014	
Main Applicant	Prof. dr. B.P.F. Jacobs	Radboud Universiteit Nijmegen Faculteit der Natuurwetenschappen, Wiskunde en Informatica Computer Science
Project title	Own Your Own Identity	

Scientific summary

Over the past fifteen years, research in cryptography has demonstrated that attribute-based credentials (ABCs) can be used for flexible, secure and privacy-friendly authentication. Such credentials may be either identifying or anonymous; they allow users to gain access to resources without revealing any information about themselves other than the fact that they are authorized, e.g. by only proving that they are over 21, or have such-and-such social security number. More recent research within the "IRMA project'' at Nijmegen has shown that the advanced cryptographic protocols supporting ABCs can actually run on modern smart cards. This non-trivial achievement forms a breakthrough towards an innovative eIdentity infrastructure.

A crucial aspect of ABCs is that they need to be closely bound to the user, via a secret cryptographic key. This key needs to be stored securely, under direct (physical) control of the user, in special hardware.

The project outlined in this proposal builds on this existing IRMA work and aims to make a next step, going outside academia into the world of eIdentity providers and customers. Together with project partners KPN and SURFnet this proposal aims to design and develop new realisations of ABCs in (secure hardware in) mobile phones and tablets that are so important in modern workflow.

The combined scientific and engineering challenges lie in integrating the subtle and computationally-intensive cryptographic protocols for ABCs in constrained environments like SIM cards, Trusted Execution Environments (TEEs) in mobile phones and tablets, and in a newly designed "homebox''.

Applicable NCSRA theme

- Identity, privacy and trust management