PRIVACY BY DESIGN FOR BIOMETRIC AUTHENTICATION SOLUTIONS

Philip Schütz and Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research
The MARS Project

- MARS = Mobile Authentication via Retina Scanner
- Main goal: Preparing the grounds for a mobile retina scanner technology with **privacy by design** features
- Funded by the German Federal Ministry of Education and Research (Civil Security Research Programme)
- Project duration: 01/2012 until 12/214
- Interdisciplinary research project (11 partners)
What’s a retina (scan)?
Location of the retina
Different imaging techniques

Source: http://www.stlukeseye.com/anatomy/retina.html

Source: Department of Ophthalmology at the Technical University of Munich
The MARS technology

- Authentication through the retina’s unique structure of blood vessels
- Miniaturisation and the integration of the technology into mobile devices

Fields of applications:
- Online-banking
- Access control in security contexts
- ...
Scan process

• First scan (enrolment)
  – Infrared laser scan (unperceivable)
  – Image and template creation
  – Template stored locally or on service provider’s server

• Further scans (authentication)
  – Infrared laser scan with mobile device
  – Matching of the scan’s image against the template either on the mobile device or by the service provider
  – Communication (scan image/control template or authentication results) with the service provider
What has TA and privacy to do with that?
Technology assessment and user acceptance

- Medical evaluation (Medical eye specialists from TU Munich)

- Privacy considerations
  - Informational privacy: Legal analysis of retina scans with the focus on data protection (Centre for Applied Law (ZAR) at the Karlsruhe Institute for Technology)
  - Bodily privacy
  - Privacy Impact Assessment

- Economic evaluation

- User acceptance
  - Ergonomics and added security value
  - Focus groups
Main challenges towards privacy

• Surplus data
  – Retinal data can contain highly sensitive information such as health data (e.g. hints to diabetes, hypertension or drug abuse)
  – Dual use

• System architecture
  – Centralised vs. decentralised storage and processing of biometric data
  – Communication of more (images) or less (templates) sensitive data over public networks

• Retina as an internal biometric feature
  – The body as an extremely intimate sphere
  – Scanning perceived as an intrusion into the body
Privacy by design approaches

• Use of an **internal** biometric feature (needs co-operation)
• Design of scan engine (images contain less sensitive information)
• Immediate deletion of the retinal image (raw data)
  – No communication or storage of raw data (especially not on third party computers)
  – “De-specialisation” of the retinal data --> limiting legal requirements for data protection
• Maximum decentralised architecture
  – Reference template under the control of the user
  – Use of encapsulated and tamper-proof hardware
• BUT: elements need to be balanced against other requirements (e.g. burden of proof)
Initial conclusions

- Privacy by design is possible!
- Not necessarily a trade-off between privacy and security
- Interdisciplinary research is challenging but crucial
- Vigilance towards only fostering additional legitimacy
Outlook

• Acceptance research
  – Ergonomics and added security value
  – Focus groups

• Economic evaluation

• Data Protection and Privacy Impact Assessment