



TrUsted Revocable Biometric IdeNtitiEs

The TURBINE research project has received funding from the 7th Framework Programme of the European Community (FP7/2007-2013) under Grant Agreement n° ICT-2007-216339



Best Practices for privacy friendly biometric data processing

The present document summarises the TURBINE *practical guidelines* for the design, the development and the implementation of biometric identity management systems in the *private sector*. The full text of the guidelines is set out in the public TURBINE deliverable 1.4.3, available at www.turbine-project.eu

TURBINE partners received an opinion of the EDPS on 1 February 2011 about the project.

The EDPS acknowledged the relevance of the Best Practices and stated that *'developing the best practices (...) will help to implement appropriate measures for any biometric Identity Management System conducted in compliance with the EU regulatory framework. Such a check list could indeed allow development of more privacy friendly systems, if they are taken into account from the start of projects'*. The opinion is public and the text can be consulted on the website of the EDPS.^[1]

[1] EDPS, Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs), 14 p., also available at <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC/OC2011>

Important notice: The suggested Turbine Best Practices do not replace the privacy and data protection compliance measures. These remain required according to applicable national data protection legislation(s). v.1.0.

More information on the TURBINE project:

<http://www.turbine-project.eu>



For further information and contacting the partners, please visit the TURBINE website or send an email to: contact@turbine-project.eu

Project Coordinator: Nicolas DELVAUX (MORPHO) Tel: +33 (0)1 58 11 33 70
Email: nicolas.delvaux@morpho.com

Functionality of the biometric IdM system

Best Practice N°1 : Biometric data shall in principle only be used for verification and stored locally For most IdM systems, the security need is fulfilled if the (verification) comparison can confirm that the person is enrolled.

Design and Architecture

Best Practice N°2 : User control over biometric data by default

by storage of the collected biometric data locally on an object under the control of the individual, increasing in addition the transparency of the use of the biometric data.

Best Practice N°3 : Multiple identities and pseudonymity

because otherwise, biometric data could be used in an IdM system as unique identifiers.

Best Practice N°4 : Revocability of biometric identities and re-issuance

by using techniques, making it possible to issue various identities based on the same characteristics, allowing to revoke such identities.

Enrolment

Best Practice N°5 : Credential and/or identity check which is of crucial importance and shall be thorough and reliable for any biometric IdM systems to be trustworthy.

Best Practice N°6 : Deletion of the samples and of the original templates

Best Practice N°7 : The use of privacy-enhancing technologies to transform the original biometric data, allowing for multiple biometric identities which are irreversible and unlinkable across contexts.

Deployment

Best Practice N°8 : Transparency and additional information for the data subjects such as about the functioning of the system and the error rates.

Best Practice N°9 : Accuracy and specification of fall back and of the appeal procedure

Additional Best Practice N°10: Measures for the *organization*, the *security* and the *certification* of the biometric IdM system