

# **Working Group 5 Identity Management and Privacy Technologies within ISO/IEC JTC 1/SC 27 – IT Security Techniques**

**Joint Workshop  
of  
ISO/IEC JTC 1/SC 27/WG 5, ITU-T SG17/Q.6, and FIDIS  
on  
Identity Management Standards  
Lucerne, Switzerland, 2007-09-30**

**Kai Rannenberg (WG5 Convener)  
Christophe Sténuit (Co-editor 24760)  
Asahiko Yamada (Editor 24761)  
Stefan Weiss (Editor 29100/29101)**





# Agenda

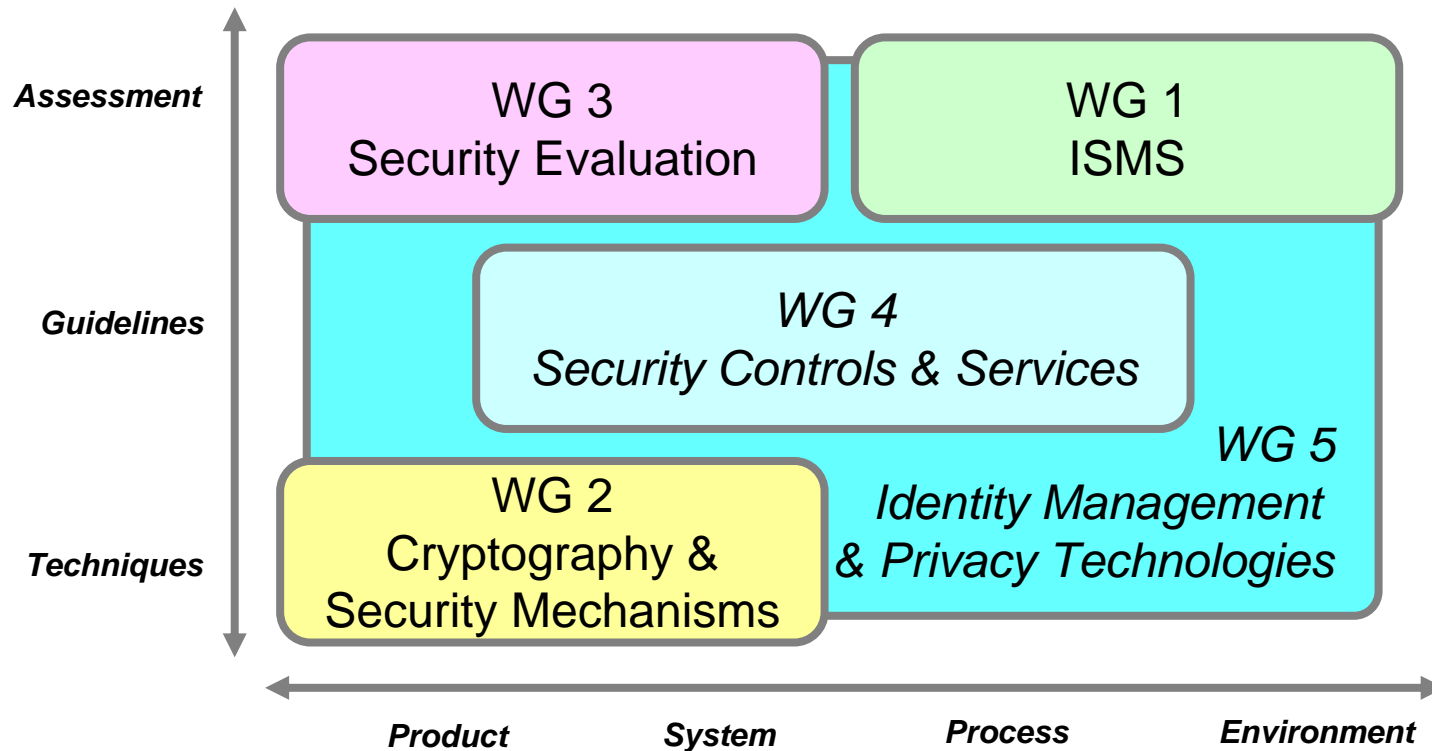
ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- WG 5 Overview  
*Kai Rannenberg*
- Identity Management Framework  
*Christophe Sténuit*
- Authentication Context for Biometrics  
*Asahiko Yamada*
- Privacy Framework/Architecture  
*Stefan Weiss*
- WG 5 Roadmap and Outlook  
*Kai Rannenberg*



# WGs within ISO/IEC JTC 1/SC 27 – IT Security Techniques

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies





## WG 5 Identity Management & Privacy Technologies Scope

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - Identity management
  - Biometrics and
  - Privacy.



# WG 5 Identity Management & Privacy Technologies Programme of Work

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

## Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760)
- A privacy framework (ISO/IEC 29100)
- A privacy reference architecture (ISO/IEC 29101)

## ▪ Protection Concepts

- Biometric template protection (ISO/IEC 24745)

## ▪ Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761)
- Authentication Assurance (ISO/IEC 29115)

# Agenda

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- WG 5 Overview  
*Kai Rannenberg*
- Identity Management Framework  
*Christophe Sténuit*
- Authentication Context for Biometrics  
*Asahiko Yamada*
- Privacy Framework/Architecture  
*Stefan Weiss*
- WG 5 Roadmap and Outlook  
*Kai Rannenberg*



# WG 5 Identity Management & Privacy Technologies

## IdM History

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- **October 2004**
  - **STUDY PERIOD on Identity Management established in respond to JTC 1's request**
- **May 2005**
  - **New Work Item Proposal (NP) on “A framework for identity management”**
- **May 2006**
  - **First Working Draft on “A framework for identity management”**
- **May 2007**
  - **Third Working Draft on “A framework for identity management”**



# WG 5 Identity Management and Privacy Technologies Topics

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

## ■ Identity Management Framework

- Identity (Efficiency vs. Misuse), Identification, References, Identifiers
- Identity Management: Lifecycle, Provisioning of Identities, Attributes
- IdM requirements, Control Objectives
- IdM implementation, Authentic Sources of Identity Information
- IdM and information access management: policy, privileges, authorization, authentication, IdMS federation

## ■ Collaborative works

- SC27: WG 1 on management aspects, WG 3 on evaluation aspects
- ISO TC 68/SC 2 Financial Services Security
- ITU-T SG 17 (Security, languages and Telco software)
- ITU-T Joint Coordination Activity on Network Aspects of Identification Systems (including RFID) (JCA-NID)
- FIDIS (Future of Identity in the Information Society)
- The Open Group (IdM Forum and Jericho Forum)



## Agenda

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- WG 5 Overview  
*Kai Rannenberg*
- Identity Management Framework  
*Christophe Sténuit*
- Authentication Context for Biometrics  
*Asahiko Yamada*
- Privacy Framework/Architecture  
*Stefan Weiss*
- WG 5 Roadmap and Outlook  
*Kai Rannenberg*

# 24761 ACBio (Authentication Context for Biometrics)

First WD issued in August 2005

Current draft, 3<sup>rd</sup> CD, issued in July 2007

Scope: 24761 defines the structure and the data elements of ACBio instance, which is used for checking the validity of the result of a biometric verification process executed at a remote site.

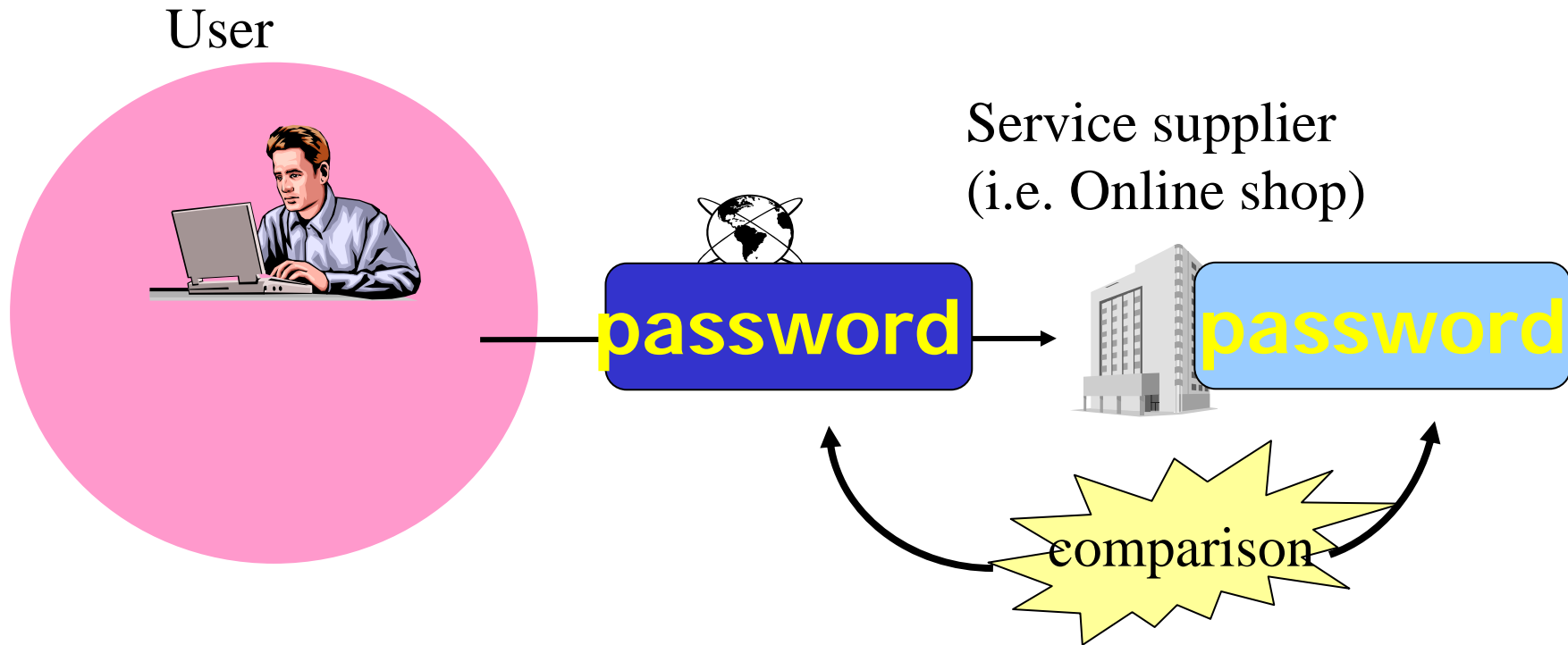
(The following slides explains what ACBio is)

Liaison relation:

SC 17 (IC card command sequence to realize ACBio)

SC 37 (inclusion of ACBio in CBEFF, BioAPI extension to handle ACBio)

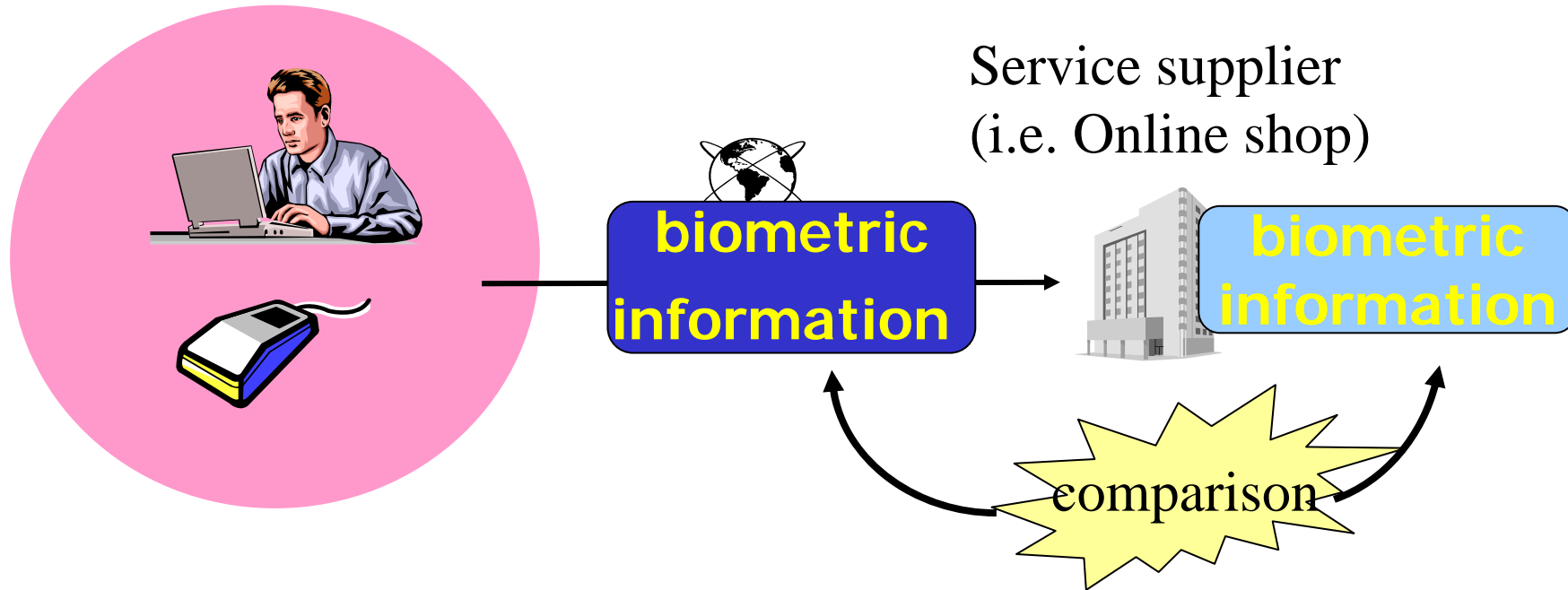
# User authentication using password



**Passwords are registered and stored in the system of the service supplier.**

# If you extend the system with biometrics

User



Service supplier  
(i.e. Online shop)

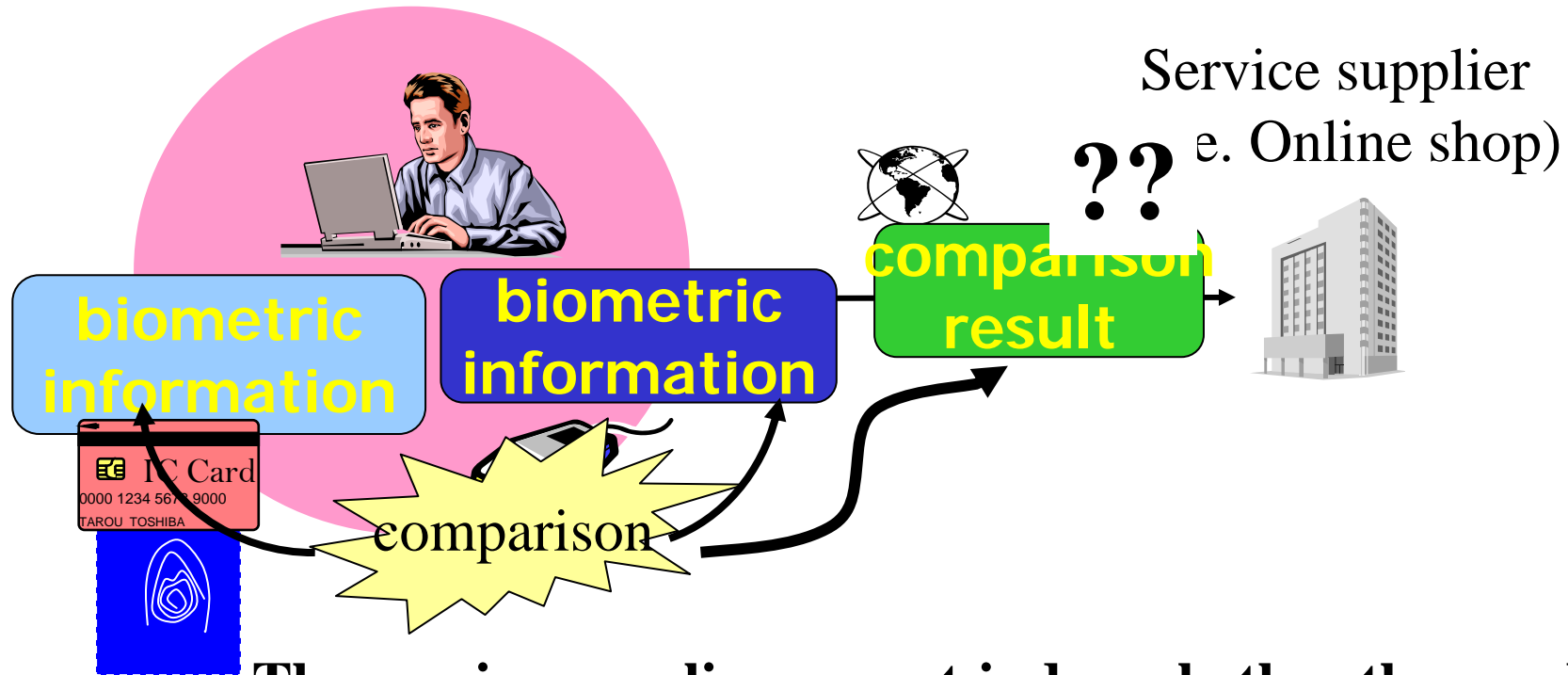
**Biometric information is stored in the system of the service supplier in advance.**

- ➔ **Issue 1. Privacy issue of users' biometric information**  
**Issue 2. Increase of TCO to protect biometric information**

# An improvement

If you store biometric information in your personal device, ....

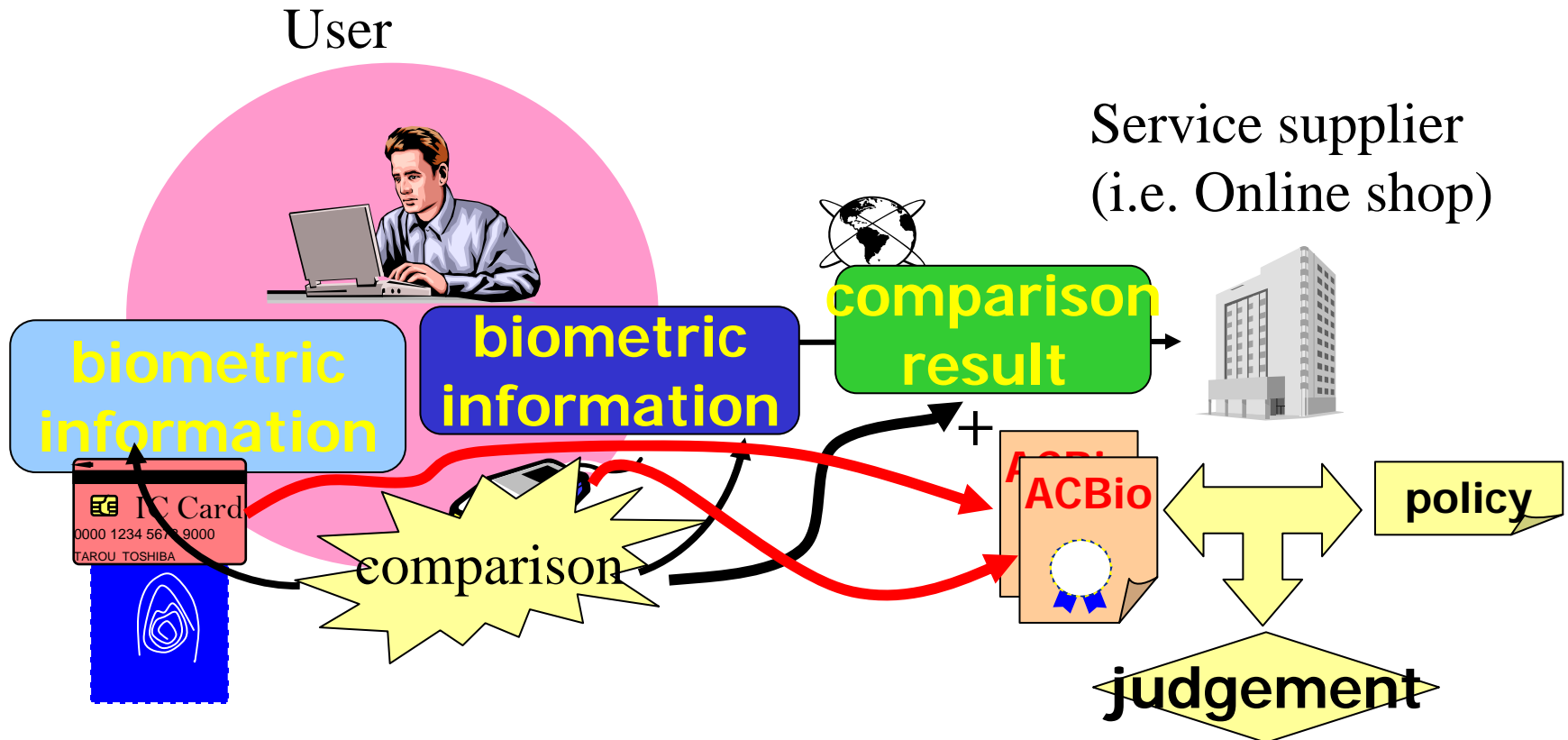
User



**The service supplier cannot judge whether the result is trustworthy!**

**If it can trust the result, the degree of trustworthiness will be dependent on the precision of the devices used and other environmental factors.**

# ACBio is a solution!



**The service supplier CAN judge the trustworthiness of the result of biometric verification with the information in ACBio instances.**

**ACBio will become the essential information for remote authentication using biometrics.**



# Agenda

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- WG 5 Overview  
*Kai Rannenberg*
- Identity Management Framework  
*Christophe Sténuit*
- Authentication Context for Biometrics  
*Asahiko Yamada*
- Privacy Framework/Architecture  
*Stefan Weiss*
- WG 5 Roadmap and Outlook  
*Kai Rannenberg*

# ISO 29100 Privacy Framework

## Purpose (as defined in Working Draft 2)

### This International Standard

- defines privacy safeguarding requirements as they relate to PII processed by any information and communication system in any jurisdiction
- is applicable on an international scale and sets a common privacy terminology, defines privacy principles when processing PII, categorizes privacy features and relates all described privacy aspects to existing security guidelines
- serves as a basis for desirable additional privacy standardization initiatives, for example a technical reference architecture, the use of specific privacy technologies, an overall privacy management, assurance of privacy compliance for outsourced data processes, privacy impact assessments and engineering specifications
- needs to be general in nature, puts organizational, technical, procedural and regulatory aspects in perspective and addresses system-specific issues on a high-level
- needs to be closely linked to existing security standards that have been widely implemented into practice
- provides guidance concerning information and communication system requirements for processing personally identifiable information to contribute to the privacy of people on an international level, regardless of the particular national or regional laws and regulations and no matter which data systems are used



# ISO 29100 Privacy Framework

## Current Outline (as defined in Working Draft 2)

- **Scope**
  - Purpose
  - Target Audience
- **Normative references, Terms and Definitions, Symbols**
- **Basic Elements of the Privacy Framework**
  - The Privacy Framework
  - The Actors
  - Personally Identifiable Information
  - Risks
  - Privacy Preferences
  - Privacy Requirements
  - Privacy Principles
- **Implementing Privacy**
- **Interdependencies**
- **Relating Privacy to IT-Security**



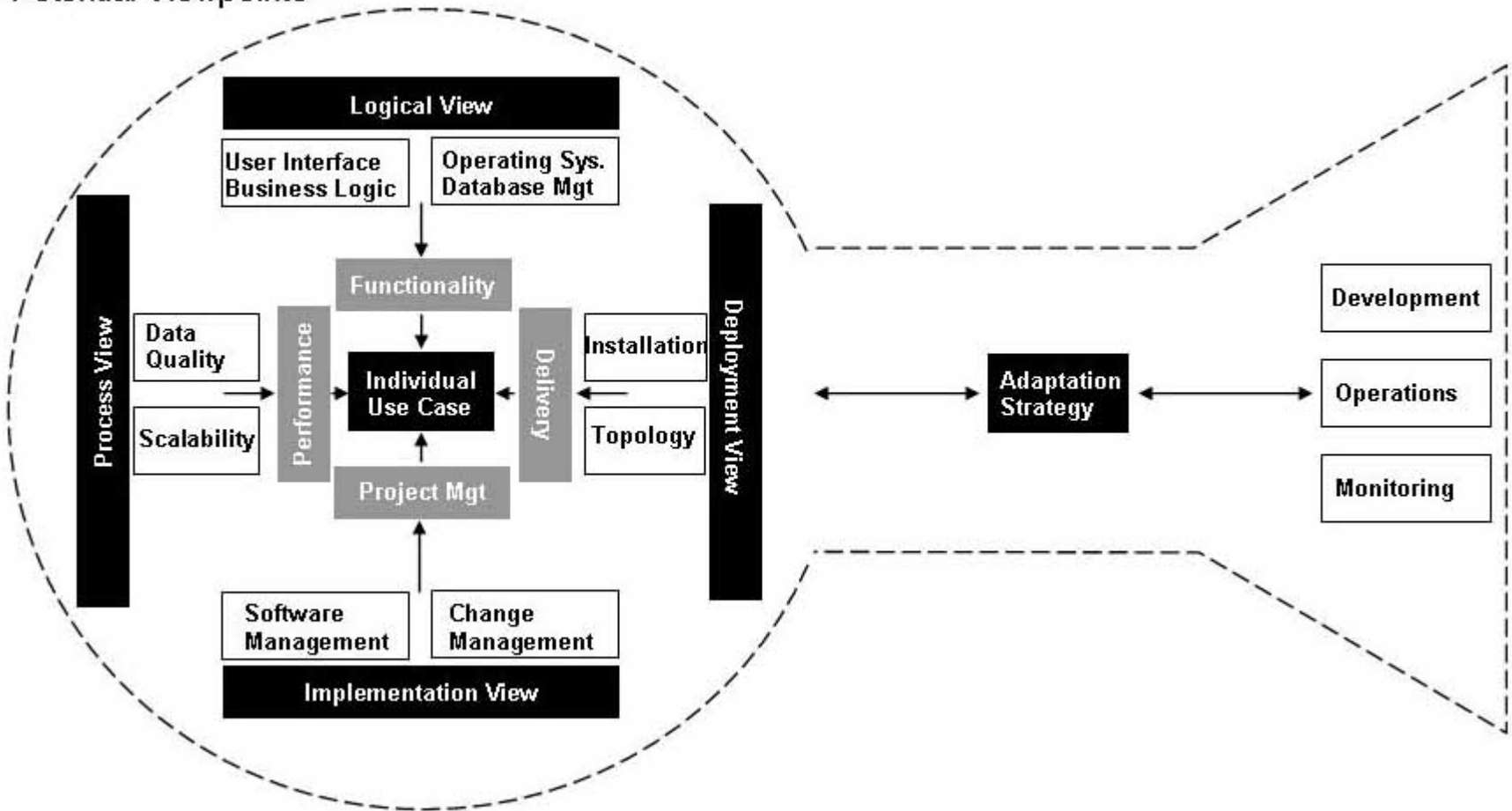
# ISO 29101 Privacy Reference Architecture Purpose (as defined in Call for Contributions)

**ISO 29101 – A privacy reference architecture – should**

- **provide guidance concerning a consistent and effective technical implementation of privacy safeguarding requirements within information and communication systems**
  - **establish a privacy-enhanced system architecture that enables system architects to build necessary privacy safeguarding measures into the system in a cohesive way across system platforms and to combine them with existing security measures, all to improve the proper handling of personally identifiable information overall**
  - **provide best practices in advancing the use of privacy-enhancing technologies**
- **A recent 'Call for Contributions' seeks further contributions in the form of case studies, architecture models, reports, product descriptions, white papers, research prototypes or others related to the viewpoints suggested in the following graphical representation.**

# ISO 29101 Privacy Reference Architecture Draft for Topics in Call for Contributions

## Privacy Reference Architecture Potential Viewpoints





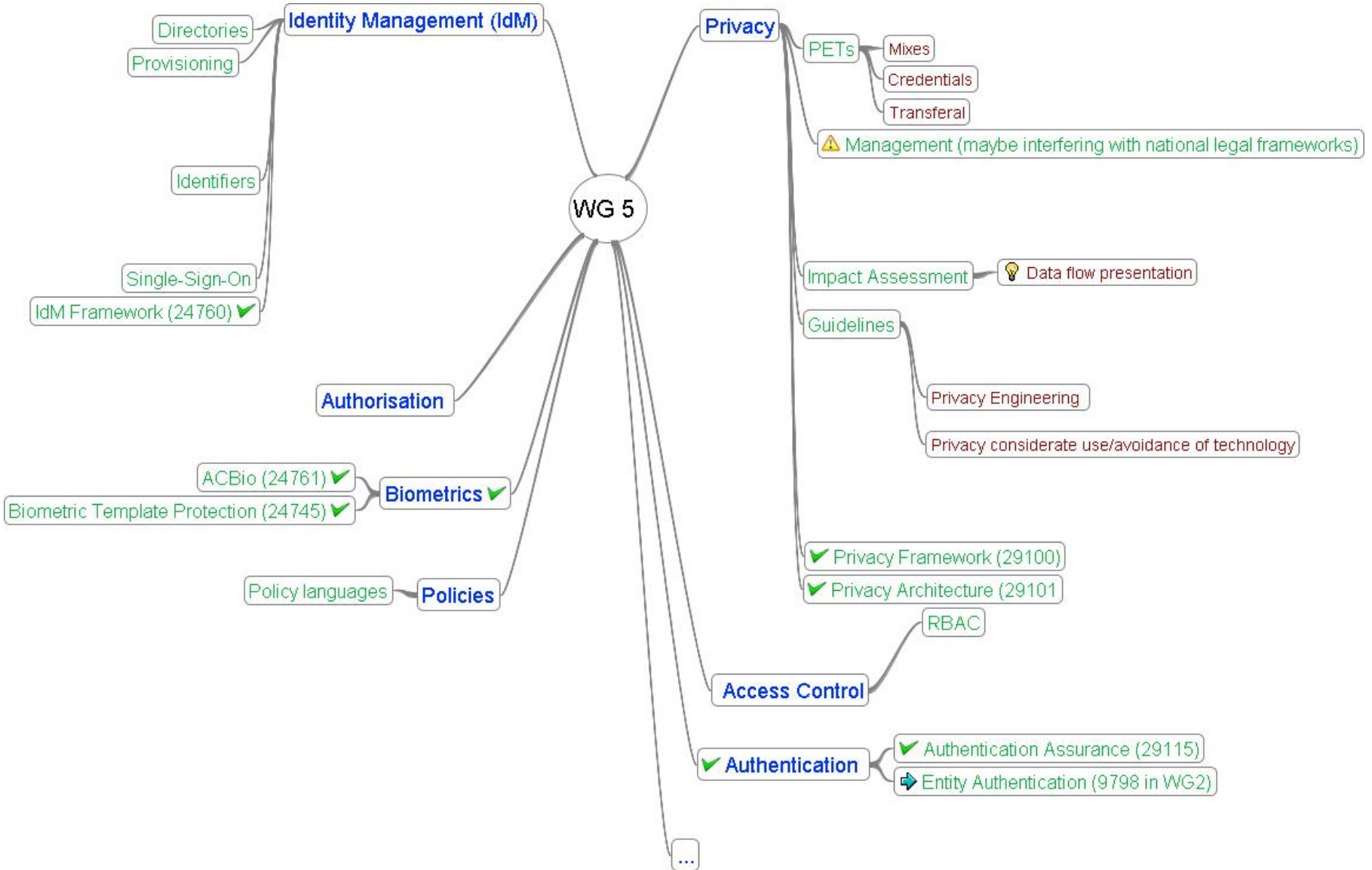
# Agenda

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- WG 5 Overview  
*Kai Rannenberg*
- Identity Management Framework  
*Christophe Sténuit*
- Authentication Context for Biometrics  
*Asahiko Yamada*
- Privacy Framework/Architecture  
*Stefan Weiss*
- WG 5 Roadmap and Outlook  
*Kai Rannenberg*

# WG 5 Identity Management & Privacy Technologies Preliminary Roadmap

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies





# WG 5

## Identity Management & Privacy Technologies

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

Thank you very much for your attention

Kai.Rannenberg@m-chair.net

cstenuit@ogeris.be

stefanweiss@deloitte.de

Yamada.Asahiko@toshiba-sol.co.jp

ISO/IEC JTC 1/SC 27 „IT Security Techniques“

[www.jtc1sc27.din.de/en](http://www.jtc1sc27.din.de/en)

SD6 Glossary of IT Security Terminology

SD7 Catalogue of SC 27 Standards & Projects