CEN

WORKSHOP

AGREEMENT

CWA 15263

April 2005

ICS 35.040

English version

Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No.:CWA 15263:2005 D/E/F

0 Introduction

This document is the completed work of the CEN-ISSS-WS-DPP C2 (Technology Impact Assessment) team.

1 Scope & Objective

For the purposes of this report, the term "technologies" will be defined as those technologies that are designed with a primary purpose of enhancing the privacy of the user. Such technologies are referred to as PET (Privacy Enhancing Technologies) and IMS Identity Management Systems. These technologies can be implemented in hardware and/or software.

This report will analyse the impact of data protection technologies. It will provide recommendations for longer term co-ordinated advice to regulators, and make recommendations to ensure that standards take account of the state of the art in this area. The results will be published as a CEN Workshop Agreement.

2 References

2.1 General

OECD report: http://www.olis.oecd.org/olis/2001doc.nsf/LinkTo/dsti-iccp-reg(2001)1-final Outcome of EC workshop:
http ://europa.eu.int/comm/internal_market/privacy/docslawreport /pet/200304-pet-outcome_en.pdf

UMIS-paper:
http://www.co.umist.ac.uk/research/tech_reports/trs_2002_001_lam.pdf

Extracts from the UK contribution to SC37 WG6 Jan 2004, Includes data contributed by the European Biometrics Forum.

Definitions of various privacy related technologies from page 16 of the Commission Report on the Implementation of the DP Directive: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm

David Trower: From minutes of first CEN/ISSS DPP WS conf call.

Information and data UK DPA: http://www.informationcommissioner.gov.uk/

Information and data from RAPID docs: http://www.ra-pid.com

Information and data from PRIME docs: http://www.prime-project.eu.org/

G.W.van Blarkom, J.J.Borking, J.G.E.Olk, Handbook of Privacy and Privacy-Enhancing technologies, The caser of Intelligent Software Agent, ISBN 90 74087 33 7, The Hague 2003

J.J. Borking, C. D. Raab, Laws, Pets and Other Technologies for Privacy Protection in Journal of Informatics, Law and Technology (JILT) January 2001;

J.J.Borking, Darf Es Ein Bitchen Weniger Sein? in Datenschutz Und Datensicherheit (DUD) #2001/10- October 2001;

J.J.Borking, Privacy Incorporated Software Agent, in H.Federrath, Designing Privacy enhancing Technologies, Berlin 2001, p. 130- 140

J.C.Canon, Privacy, What Developers and IT rofessionals Should Know, Boston, 2004

Dutch Ministry of Interior and Kingdom Relations (Directorate Innovation and Information Policy (DIOS), Whitebook on Privacy-Enhancing Technologies, The Hague 2004, p. 25-40

Documents adopted by the Article 29 Working Party are available at: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

J.P. Leerentveld RA RE, G. W. van Blarkom RE, WBP Raamwerk Privacy Audit. Samenwerkingsverband Audit Aanpak, The Hague 2000.

H. van Rossum, H. Gardeniers, J.Borking, A. Cavoukian, J.Brans, N. Muttupulle, N. Magistrale, Privacy-Enhancing Technologies: The Path to Anonymity, Achtergrondstudies en verkenningen no 5a en 5b, The Hague August 1995 ISBN 90 346 320 24;

R.Hes, J.Borking, Revised Edition, Achtergrondstudies en Verkenningen no 11, The Hague 1998 ISBN 90 74087 12 4.

2.2 References on Anonymity, Unlinkability, Unobservability, and Pseudonymity

Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, LNCS 453, Springer, Berlin 1990, 246-264.

David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; The IPTS Report 67 (September 2002) 8-16.

Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, Michael Waidner: Privacy-Enhancing Identity Management; Information Security Technical Report (ISTR) Volume 9, Issue 1 (2004), Elsevier, UK, 35-44, http://dx.doi.org/10.1016/S1363-4127(04)00014-7.

Mireille Hildebrandt (Vrije Universiteit Brussel): presentation at the FIDIS workshop 2nd December, 2003; slides: http://www.calt.insead.edu/fidis/workshop/workshop-wp2-december2003/presentation/VUB/VUB_fidis_wp2_workshop_dec2003.ppt.

Independent Centre for Privacy Protection & Studio Notarile Genghini: Identity Management Systems (IMS): Identification and Comparison Study; commissioned by the Joint Research Centre Seville, Spain, September 2003, http://www.datenschutzzentrum.de/projekte/idmanage/study.htm.

ISO IS 15408, 1999, http://www.commoncriteria.org/.

Birgit Pfitzmann (collected by): Information Hiding Terminology -- Results of an informal plenary meeting and additional proposals; Information Hiding, LNCS 1174, Springer, Berlin 1996, 347-350.

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes -- Untraceable Communication with Very Small Bandwidth Overhead; 7th IFIP

International Conference on Information Security (IFIP/Sec '91), Elsevier, Amsterdam 1991, 245-258.

Andreas Pfitzmann, Michael Waidner: Networks without user observability -- design options; Eurocrypt '85, LNCS 219, Springer, Berlin 1986, 245-253; revised and extended version in: Computers & Security 6/2 (1987) 158-166.

Michael K. Reiter, Aviel D. Rubin: Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security 1(1), November 1998, 66-92.

Claude E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656-715.

Stuart Stubblebine, Paul Syverson: Authentic Attributes with Fine-Grained Anonymity Protection; Financial Cryptography 2000, LNCS Series, Springer, Berlin 2000.

Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt '89, LNCS 434, Springer, Berlin 1990, 302-319.

J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf: Modeling the security of steganographic systems; 2nd Workshop on Information Hiding, LNCS 1525, Springer, Berlin 1998, 345-355.

2.3 Project references and Publications on PET (Healthcare)

Project References

- Privacy Enhancement in Data Management in e-Health (PRIDE-H)(IST-2001-32647). The IST Programme. Commission of the European Communities - Directorate-General Information Society. (2001- 2003)

- Privacy Enhancement in Data Management in E-Health for Genomic Medicine (PRIDEH GEN) (IST-2001-38719). The IST Programme. Commission of the European Communities - Directorate-General Information Society. (2002- 2004)

- Privacy Protection in e Pharma (PPeP), EU-Canada Collaboration Initiative in Health Telematics (2003)

Publications

- **De Moor GJE, Claerhout B.**
  Leading the Way for Privacy Protection in e Pharma – White Paper
  21/5/2003, Custodix-Pfizer; EU-Canada Collaboration, DG INFSO (EC).

- **De Meyer F, Claerhout B., De Moor GJE.**
  The PRIDEH project: taking up Privacy Protection Services in e-Health.
  Proceedings MIC 2002 "Health Continuum and Data Echange". IOS Press, 2002, p. 171-177.

- **Claerhout B**, **De Moor GJE**, **De Meyer F.** Secure Communication and Management of Clinical and Genomic Data: the use of Pseudonymisation as Privacy Enhancing Technique.
  Proceedings MIE 2003. IOS Press. 2003, p 170-175.

- **Claerhout B**, **De Moor GJE**
  From Grid to HealthGrid: introducing Privacy Protection.
  Proceedings of the First European HealthGrid Conference, p. 226-233.
  (Jan 16th-17th,2003). Document from Information Society Technologies, European Commission.

- **Claerhout B**, **De Moor GJE**
  Privacy Protection in e-Health
  Stud Health Technol Inform. IOS Press, 2003 (in press)

- **Claerhout B**, **De Moor GJE**, **De Meyer F.**
  Secure communication and management of clinical and genomic data; the use of pseudonymisation as privacy enhancing technique.
  Stud Health Technol Inform. 2003;95:170-5.

- **Claerhout B**, **De Moor GJE** Privacy Protection for Clinical and Genomic Data: the Use of Privacy Enhancing Techniques in Medicine.
  Int. Journal of Medical Informatics (in press).

- **Claerhout B**, **De Moor GJE**.
  Privacy Protection for HealthGrid Applications.
  Method Inf Med.(in press).

- **De Moor GJE**, **Claerhout B**.
  Privacy Enhancing Techniques in e-Health: an Overview
  Stud Health Technol Inform. 2004 (in press)

3 Definitions

Anonymity

To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes (cfr Andreas Pfitzmann PRIME)
Anonymity is the state of being not identifiable within a set of subjects, the *anonymity set*.
ISO 15408 states: "Anonymity ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the