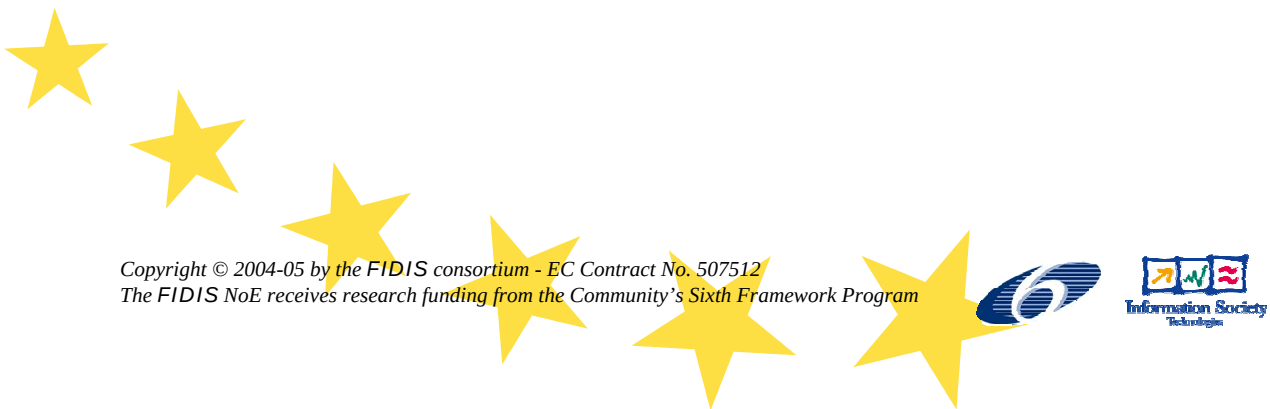
FIDIS

Future of Identity in the Information Society

Title:	D5.2: ID Fraud Workshop
Author:	WP5
Editors:	Ronald Leenes (Tilburg University, Netherlands)
Reviewers:	Denis Royer (JWG, Germany)
Identifier:	D5.2
Type:	[Workshop Report]
Version:	0.4
Date:	Thursday, 13 April 2006
Status:	[final]
Class:	[Public]
File:	fidis-wp5-D5.2-workshop-report-final.doc

Summary

This document contains a report of the FIDIS WP5 ID fraud Workshop, held on 18 May 2005 in Tilburg, the Netherlands.



The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	20.05.2005	• Initial version (Merel Prinsen)
0.2	15.07.2005	• Final version (Ronald Leenes)
0.3	04.04.2006	• Review version
0.4	08.04.2006	• Reviewed version (Denis Royer)

Foreword

This deliverable is a summary of the WP5 workshop on ID related crimes. It is to be read in conjuction with deliverable D5.2.b which contains a consolidated version of the papers that were produced for this workshop.

	Contributor(s)
Whole report	• Ronald Leenes (Tilburg University, Netherlands) • Merel Prinsen (Tilburg University, Netherlands)

Table of Contents

1 Workshop report

Workpackage 5 is concerned with ID Theft, privacy and security. The current workshop focused on ID Fraud and related crimes. ID Fraud is a broad term for what is often referred to as identity theft: The act of stealing someone's identity information in order to impersonate the victim. Identity allows each citizen to perform different roles (e.g. employee, customer, or voter) in society. The disclosure, misuse and abuse of identity may cause considerable inconvenience such as financial loss, damage to reputation, etc. Indeed, identity fraud is often committed to facilitate other crimes; hence a wide number of other crimes may be involved such as credit card fraud, impostering, computer fraud, mail theft, mail fraud, financial fraud and immigration document fraud.

At present, the (legal) nature of ID related crimes is unclear. The preceding paragraph, for instance mentions ID fraud and ID theft as crimes that are often used as synonyms, whereas from a legal perspective theft and fraud are different concepts. Also, the very concept of theft, in some jurisdictions at least, does not fit very well with the essence of ID theft that is copying information. Theft is a crime where the possessor loses possession as a result of the theft. This is not the case with ID theft. In order to gain a better understanding of what ID related crimes, to provide an umbrella to the whole range of phenomena of interest, amount to, a multidisciplinary study is required. The tools and techniques employed by ID criminals must be studied. But also the legal classification of the various practices, as well as the social consequences, need to be addressed.

The goal of the workshop was to assemble a group of experts in order to address ID related crimes from the various perspectives:

- Technical,
- Socio-economical, and
- Legal.

The workshop was held back to back with the WP8 workshop on preventing ID fraud. Important input for the workshop came from the three papers that are being written as part of D5.2:

- A technical paper, co-ordinated by Svetla Nikova (COSIC, Belgium)
- A legal paper, co-ordinated by Hans Graux (ICRI, Belgium) (succeeded by Ronald Leenes, TILT, after Hans departure from academia)
- A socio-economic paper, co-ordinated by Ioannis Maghiros (JRC, Spain)

The papers will be integrated into a single document that will be available on the FIDIS website early September.

Both workshops consisted of a number of presentations as well as discussion on key points surrounding ID related crimes.

The workshop was opened by Bert-Jaap Koops, WP5 Workpackage leader, who welcomed the participants and outlined the goal of the workshop.

Short summaries of the various presentations are presented below. The presentations are available on the FIDIS website.

1.1 Summary of the Presentations

1.1.1 Martin Meints (ICPP, Germany)- Sociologic Driven View

Martin Meints first discussed social systems to show what a person is, depends on the social context in which the concept is used. In interactional systems with loose, inexplicit, rules (such as neighbourhood meetings), the conception of what constitutes a person differs from that in an organisational system such as a company, or a social subsystem, such as the economy at large.

He then discussed the need to distinguish between identity collision and identity change. These are the results of (un)intentional errors in communication between parties. *Identity collisions* always result when an identity (actually a partial identity) is assigned to the wrong person. One form of identity collision stems from role collision: For instance if you buy a car from a friend who happens to be a car dealer also. Can he be both - a friend and a car dealer at the same time? Or is he not a friend at the moment he sells the car to you?

With *identity change*, one of those involved in a communication deliberately causes the misinterpretation of their role or identity by others who are involved in the communication (intent). Within the category of identity change, four more groups can be distinguished:

a) Identity takeover

b) Identity exchange

c) Identity delegation

d) Identity creation

With *identity takeover,* a third, so far uninvolved person (the identity taker), takes over the role of one partner (Target 1) within an established communication relationship with fixed assigned roles and authenticated communication partners and then uses another partner's (Target 2) contributions or performance.

Identity exchange requires an existing (for example 1:n-) communication, e.g. of an organisation with its customers. Within this communication relationship, two bearers of the same role, such as clients, exchange their identities towards the bearer of another role (e.g. the organisation).

With *identity delegation*, the identity of one of the communication partners is deliberately transferred to a party not involved up to the moment of identity change, or the transfer is deliberately agreed within an existing communication relationship. This delegation cannot (or only later) be detected by the other communication partners. There is discussion about identity delegation: What is meant by this term? Attribution, licensed selling, inheritance or sharing? Delegation here means that the agreement has legal consequences. An example that shows some of the intricacies of this type of ID change is an undercover police officer buying drugs. He is an anonymous client. Is this an identity error? He is not correcting the expectations. Is there in this case a passive identification implicated?

With *identity creation*, on the other hand, a new identity and role, which cannot be assigned to any real person, is generated and authenticated within a new communication relationship.

The typology is not without problems. For instance: In what category should we place a man who uses his wife's credit card? Is it an identity takeover or an identity exchange, or even identity delegation?

The main categories are the identity takeover and the identity creation. The difference between these two categories depends on the context. The change is about the identity while the use is about authorisation. Central to the concept of ID 'fraud' appears to be 'malicious intent'. A problem is that usually the intent of the perpetrator is unknown at the moment the identity of the victim is acquired. Hence, Meints proposes a two step approach that distinguishes between:

- identity change
- using the acquired identity

1.1.2 Klaus Kursawe (COSIC, Belgium)– Technical Aspects

Klaus Kursawe (COSIC) discussed one of the techniques to prevent IDentity fraud: Trusted Computing (TC). Trusted Computing is a novel concept to secure the computing infrastructure, which may help create more secure authentication methods. TC relies on a standard for an small, cheap, and more or less tamper resistant security module (Trusted Platform Module, TPM). This module can protect keys, execute some cryptographic functions, and – most importantly – can attest some information about the platform to outside parties.

The TPM contains a hierarchy of keys, platform keys as well as application keys, which guarantee that the platform and the applications running on top of the platform are not compromised. This system can be used for ID management and to prevent ID fraud/theft as it allows for Trusted Third Party (TTP) backed pseudonyms and credentials. It also allows for zero-knowledge based proofs based on the *Direct Anonymous Attestation* protocol. This means that the TPM can prove that it is a real TPM without revealing its identity.

Klaus discussed a number of shortcomings of the current implementations such as key migration, key revocation and the (lack of) secure operating systems.

1.1.3 Ronald Leenes (Tilburg University, Netherlands) – Legal Issues

Ronald Leenes presented the legal paper. He first discussed that there are many definitions for the concepts of ID theft and ID fraud and pointed out that the terms are often used interchangeably. As 'best' example of a definition, he proposed to the following one derived from Grijpink[1]:

> *"ID fraud is that someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person."*

This definition gave rise to discussion. For instance, ID fraud (according to this definition) requires malicious intent. Is this really required, or is intent with (un)intended malicious consequences a better description? Is a lack of consent required? Is it possible to speak about misuse without being criminal? There is a difference between non-criminal use and criminal

[1] Jan Grijpink, 'Identiteitsfraude als uitdaging voor de rechtstaat' [Identity Fraud as a Challenge to the Rule of Law], Privacy & Informatie August 2003, p. 148ff. [translation of the definition: Bert-Jaap Koops (Tilburg University, Netherlands)]

use. And, the term illegal is broader than criminal; do we want to include non-criminal illegal actions, such as tort?

The discussion showed a need for a clear set of concepts. A first discussion on suitable concepts took place on the 19th of May during the WP8 integration workshop (cp. minutes of the WP8 workshop). Leenes proposed to use an 'umbrella'-concept for the time being: Identity related crimes. The usefulness of this umbrella concept is illustrated by means of the life-cycle of ID crimes as derived from the IPTS report on ID-fraud, which lists:

- Fishing for data,
- Misappropriation,
- Misuse and finally
- Criminal action.

Leenes next discussed a preliminary analysis of US, EU and EU member states' legislation on ID related crimes. This analysis shows differences between the detailed US approach, which contains ID fraud provisions, and the EU approach where ID related crimes are often classified as instances of existing crimes, such as theft or fraud. It also shows differences with respect to criminal provisions and their conditions in the various member states that need to be studied in more detail. An example is the (Dutch and Belgian) limitation of theft to tangible goods, which inhibits the concept of ID theft if this relates to 'taking' someone's credit card data. The UK definition of theft seems to include the option of stealing non-tangible goods.

1.1.4 Socio-economic view

1.1.4.1 Sabine Delaitre (IPTS/JRC, Spain)

Sabine Delaitre also tried to define identity theft and identity fraud. The former is taken as the appropriation, without consent, of personal data; the latter as the use of the appropriated data. Delaitre showed that ID related crimes are on the rise in both the US, as well as in Europe. She also showed the existing types of ID crimes, as well as some newer ones which relate to the pervasiveness effect of networks. She pointed out that individuals use ID fraud to gain from businesses and governments, but that businesses also try to defraud other companies in order to obtain PII, e.g. by means of phishing.

The remainder of her presentation addresses the social consequences of ID related crimes. Important social aspects are, for instance, the reversal of the burden of proof for ID crime victims, the serious amount of time and effort it takes these victims to remedy their ID theft, the emotional impact and damage to the victim's reputation. From an economical perspective, the direct costs (e.g. damages), as well as the indirect costs (e.g. for fraud detection and prevention) are significant.

1.1.4.2 Albin Zuccato (KU, Sweden)

Albin Zuccato talked about the appearance of identity fraud in Sweden, giving the example of a phone contract concluded by someone else than the person actually using the mobile phone. The latter being someone not eligible for entering into a contract with the Telecom operator. His question included: What is precisely the difference between identity fraud and 'normal' fraud? According to Zuccato, fraud occurs when someone takes a benefit from the fraudulent action. He likes to use both identity fraud and identity theft when talking about identity

related crime. Fraud is the use of identity, while theft is the acquisition (not necessarily communication involved). However, there is a close relationship between both concepts. He also refers to the IPTS life cycle, discussed previously by Ronald Leenes.

Zuccato said that he does not believe in law as the means to motivate businesses and individuals to invest in means to prevent the theft of IDs. Requirements analysis using risk analysis, business modelling and stakeholder domain in his view are more promising. In this assessment, various kinds of (potential) damages have to be taken into account:

1. Damage to the organizations reputation.
2. Damage from reduced customer trust (which is necessary to conduct business).
3. Damage through to the fraudulent abuse of stolen identities.
4. Damage from legal prosecutions.

Note that Zuccato distinguishes 4 damage types, where Meints distinguishes 3 types.

1.1.5 Stephen Frey and Andrew Wallwork (LSE, UK)

Stephen Frey and Andrew Wallwork briefly talked about what level of operability would limit the risks of identity fraud.

1.1.6 Stephan Engberg (OBI, Denmark)

According to Stephan Engberg, security issues are getting worse. There is a vicious circle: There is an increasing amount of data and there is more insecurity with regard to data processing technology, so people want more and more data, which leaves them with more insecurity. In his opinion, technologies using biometrics are the most problematic group.

We need to change our way of looking at security. There is too much focus on identification. In real life we have relationships, we work on social manners and we recognize familiar people and base our trust on this recognition. Engberg says that in the end you are the one to decide what others, for instance a supermarket, know about you. You can pay in cash and have an anonymous client card. Not so in the online world.

We tend to forget the human element in the system. This aspect must be taken into consideration in the chain of analysis. There is also a problem with the way we deploy services: “[…] we don’t need security products, but secure products”. We already knew all the security problems being a potential threat five years ago, but we didn’t do anything about them.

About RFID: Even local payment will not help in the end. So we have to take actions here. Even though consumers want convenience (risks are abstract).

The rest of his presentation outlined (ID relates) problems with regard to online services and developments that cause even more potential issues.

1.2 Discussion

Due to the fact that the workshop ran behind schedule, the discussion was postponed to the Workpackage 8 meeting on the following day (19th of May).

1.3 List of participants

- Bernhard Anrig, VIP
- Emmanuel Benoist, VIP
- Sabine Delaitre, IPTS
- Stephan Engberg, OBI
- Stephen Frey, LSE
- Mireille Hildebrandt, VUB
- Bert-Jaap Koops, TILT
- Klaus Kursawa, COSIC
- Ronald Leenes, TILT
- Ioannis Maghiros, IPTS
- Svetla Nikova, COSIC
- Wim Schreurs, VUB
- Michaël Vanfleteren, ICRI
- Michiel Verlinden, VUB
- Jozef Vyskoc, VaF
- Andrew Wallwork, LSE
- Albin Zuccato, KAU

2 Programme

Workshop, WP5

Tilburg, Netherlands

18th May, 2005

Agenda

DAY 1

09h30-09h45 Welcome (TILT)

09h45-10h00 Introduction workshop, D5.2 (TILT)

10h00-11h00 Presentation, Martin Meints (ICPP)

- Sociologic driven view on ID-theft and ID-fraud

11h00-11h30 *Coffee break*

11h30-12h15 Presentation Klaus Kursawe (COSIC)

- D5.2: Technical aspects

12h15-13h00 Presentation Ronald Leenes (TILT/ICRI)

- D5.2: Legal aspects
- ID Law survey

13h00-14h30 *Lunch*

14h30-15h15 Presentation Sabine Delaitre & Albin Zuccato (IPTS/KAU)

- D5.2: Socio-economic aspects

15h15-15h30 *Tea Break*

15h30-16h00 Presentation Stephen Frey/Andrew Wallwork (LSE)

16h00- 16h45 Invited speaker, Stephan Engberg (CEO – Open Business Innovation)

- Causes and ways to do identity theft

16h45- 17h30 Discussion and conclusion on D5.2 (TILT)

- planning, delivery
- scientific paper