# Virtual? Identity

*Bernhard Anrig, Emmanuel Benoist, and*
*David-Olivier Jaquet-Chiffelle*[*]

**Abstract**[1]

This paper deals with two concepts that are linked together: identity and identification.

The aim is to present a unifying model for identities in the Information Society. This model is driven by practical applications: identification, authentication and authorization schemes. It provides unifying tools that allow a better description and understanding of the elements involved in these schemes.

We apply this model to some typical identification, authentication and authorization schemes in order to illustrate our approach.

## 1 Introduction

Many concepts evolve around the one of identity: identification, anonymity, pseudonymity, (un)observability, (un)tracability; the identity itself has many faces.

The aim of this paper is to present a unifying model for identities in the Information Society. This model is driven by typical applications: identification, authentication and authorization schemes.

As a model it is not supposed to be definitive or universal; however, it fits very well with the current diversity of these schemes and we hope it to be broad enough to evolve and adapt itself when new schemes appear.

Our goal is not to cover all aspects of identity, this would be too ambitious. But we will present a set of unifying concepts and then use them to better understand and solve practical scenarios.

We will provide new definitions for these unifying concepts and we will illustrate these definitions with typical examples. For example, in our approach, pseudonyms are reduced to a special case of identity.

---

[*] V.I.P – Virtual Identity and Privacy research center
Berne University of Applied Sciences, CP 1180, 2501 Bienne
http://www.vip.ch contact@vip.ch

[1] The results presented in this paper have been elaborated mainly within the scope of the European project FIDIS (Future of Identity in the Information Society) which is a NoE (Network of Excellence) supported by the European Union under the 6th Framework Programme for Research and Technological Development, reference number 507512. Web-site http://www.fidis.net/ (28.04.05)

In this model, we attempt to define “identity” in the Information Society. Here, the identity clearly does not refer to the entire person anymore, but only to part of it. We should remember that, etymologically speaking, “person” comes from “personae” which means “mask”. In a way, we will refer to the mask instead of the whole person itself. This approach will lead to a new core concept: the virtual persons.

In doing so, we do not cover existential questions like the ones related to the soul for example. We consciously restrict our view to the Information Society. The existence of a soul, feelings etc. for people, animals or even programs is beyond the scope of this article.

The same set of concepts is used to modelize the identity of a human being or the identity of a legal entity.

# 2 Virtual Persons

## 2.1 Definitions

In many countries, the law distinguishes two types of personalities: the physical persons and the legal persons. First we characterize both and then we present a unifying concept: the so-called “subject”.

**Definition 1 (Physical person)** *A physical person is the physical mask of a human being.*

Note that we explicitly do not restrict our definition to living human beings as even dead people may have some rights, as for example the right to a decent funeral.

**Definition 2 (Legal person)** *A legal person is any personality which is recognized by the law of a country; it has rights and duties. It is often recorded in registers and has a legal status.*

A legal person can be for example a company, an organization or a community.

The next definition gathers together physical and legal persons, as well as everything that can —in some given context— be mistaken with such persons: for example *the wind* closing a door, or *the program* ejecting a member of a forum for using forbidden words, or *the dog* opening the door and breaking the plates.

**Definition 3 (Subject)** *A subject is any set of physical or legal entities having —in a given context— some analogy with a physical person.*

Here subject is not opposed to object. Indeed, physical objects can satisfy our definition of a subject. In our definition, subjects typically play a role, they look like the grammatical «subject»

in a sentence as it has been pointed out by Sarah Thatcher[2] during the WP2 workshop of FIDIS in Fontainebleau in December 2004. Our subjects *are*, they *have*, they *do* (or *behave*) or they *know something* just like physical persons.

Three basic classes of authentication technologies are commonly considered

1. something you **know**
2. something you **have**
3. something you **are**

We want to introduce a fourth one:

4. something you **do**

## Something you

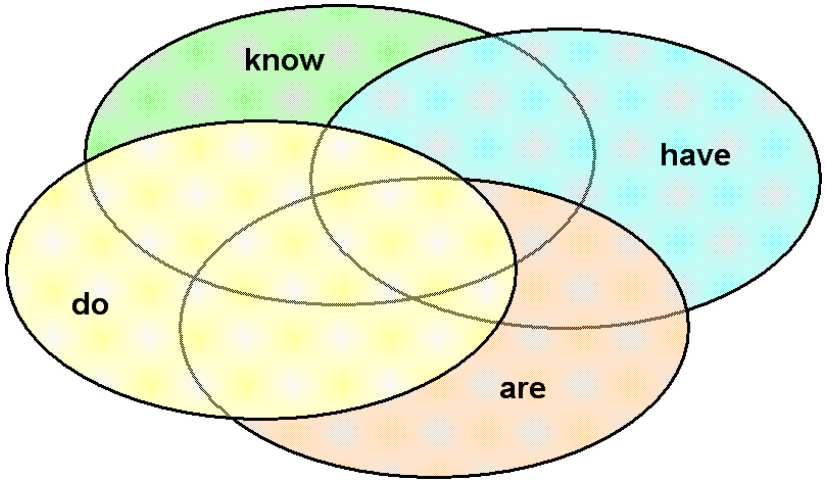


Figure 1: Classes of authentication technologies

We propose the following Cartesian representation to classify these four classes[3].

| Table 1 | *Attribute* | *Ability* |
|---|---|---|

[2] Sarah Thatcher, London School of Economics – Department of Information Systems, http://isig.lse.ac.uk/people/isig/sth.html

[3] Thierry Nabeth, INSEAD, reviewed this paper and suggested to use a Cartesian representation. http://www.insead.fr/~nabeth/

| *Role* | **Are** | **Do** |
|---|---|---|
| *Acquisition* | **Have** | **Know** |

In this table, the four classes of authentication technologies are characterized using four categories: attribute, ability, role and acquisition.

We present also the dual table, where labels and contents (i.e. categories and classes of authentication technologies) are exchanged.

| | | ***External*** | |
|---|---|---|---|
| | Table 2 | *Have* | *Do* |
| ***Internal*** | *Are* | **Attributes** | **Role** |
| | *Know* | **Acquisition** | **Ability** |

This puts into evidence two types of classes:

- internal classes (are, know)
- external classes (have, do)

The relations between these classes, their categories and their type are summarized in the following diagram:

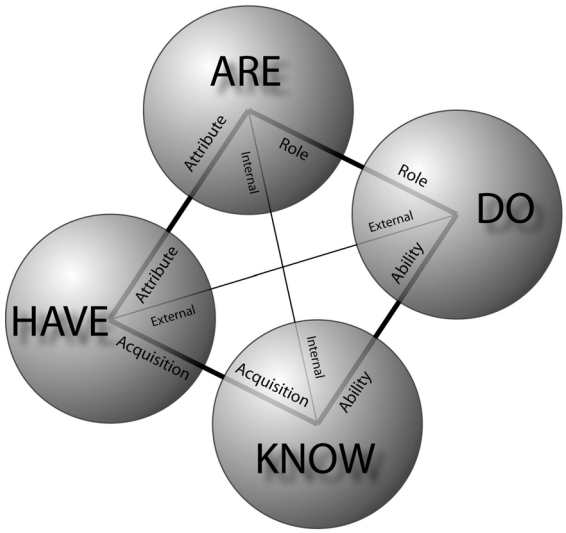


Figure 2 : Relations between authentication technologies

We will define the concept of *virtual person* while keeping in mind these authentication technologies. Indeed our definitions are "application oriented".

We observe that from a practical point of view, in most situations, a subject is accessed through a mask it is wearing. One subject can have many masks: one at work, another at home, with friends or with its banker. One mask can also be worn by many subjects: two people sharing the same computer have the same IP address. In some situations, the mask is transparent and the link between the mask and the subject is almost trivial. On the other hand, in other situations, it is difficult (or even impossible) to link a mask and the subject behind it.

However, from a practical point of view, it is enough to work with those masks, instead of the subjects, to achieve most of the tasks related to identification and/or authentication.

This is the main motivation to create and develop the concept of *virtual person.*

**Definition 4 (Virtual Person)** *A virtual person is a mask defined by its attribute(s), and/or its role(s), and/or its ability(-ies), and/or its acquisition(s). The entity behind the mask, if it exists, is a subject.*

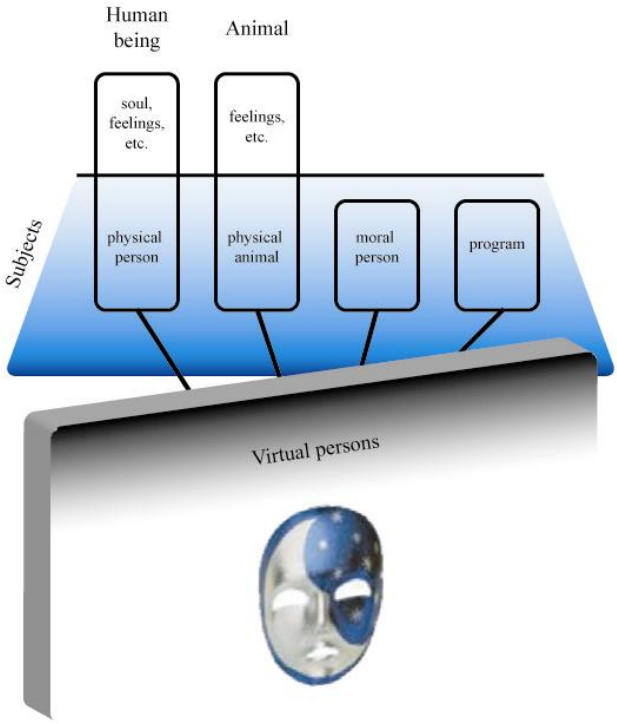


Figure 3: Virtual Persons

Fig.3 illustrates the fact that we often access a mask without any knowledge of the entity behind it. Do I talk to a single person or to a group? Is it a program or a person? Who/what did indeed close the door?

Note that the duality of tables 1 and 2 shows that we can also define a virtual person by what it knows, and/or what it has, and/or what it is and/or what it does.

## 2.2 Examples of Virtual Persons

In this section we present several examples of virtual persons. Note that a virtual person can be defined by one or more criteria.

Virtual persons can be defined by *roles*:

- **"Are"** (role & attribute) the President of the United States, the Pope, the Driver of the bus number 8, the first owner of a given car or the buyer in a given transaction.
- **"Do"** (role & ability) the person who opened the door, what has caused the door to close, the one who ejected you from the IRC forum, the person who killed JFK or the first man to walk on the moon.

In the last example, the virtual person did have some existence even before it was linked to an existing human, since it was already possible in the 50s to talk about him without knowing who he would be.

- **"Are & Do"** The instigator of a crime is defined both by it ***is*** and it ***does*** (or have done). So is the actress playing the role of catwoman.

Virtual persons can be defined by *acquisitions*: in particular, we can define a virtual person by its knowledge or what it has.

- **"Know"** (acquisition & ability) The one who knows my credit card's PIN code, the one who knows the private key corresponding to a given public key, the one who knows who killed JFK.
- **"Have"** (acquisition & attribute) The holder of my cell phone, the shareholder of 51% of the shares of a given company, the one who holds some token, the holder of your credit card...

Any *attribute* can also be used: the owner of a fingerprint, the person in front of whom I stand, the tallest person in the world.

The same is true for any *ability*: the one who can break the system, etc.

# 3 Identity and Identification

## 3.1 Identity

In the following we refer to a community of reference. Such a community *C* is either a set of subjects or a set of virtual persons.

**Definition 5 (Identifier)** *An identifier* I *is a set of information.* I *is an identifier w.r.t. a community* C *if and only if there exists a unique element in* C *that is compatible with* I.

For example:

- *Dad* is an identifier in my family,
- *Fingerprints* are supposed to be identifiers w.r.t. the world population,
- *BIE1* is an identifier w.r.t. the people working at the Berne University of applied Sciences and
- A *pseudonym* can be an identifier w.r.t. the virtual persons active in a chatroom; it may not be relevant outside of it (where other people use the same pseudonym).

**Definition 6 (Identity)** *An identifier* I *with respect to a community* C *is an identity of* P *with respect to the community* C *and according to an observer if and only if this observer can link* I *to the element* P *of* C.

Note that according to these definitions, an identifier is independent of any observer whereas an identity always depends on the observer.

For instance, a valid 4-tuple containing name, first name, date of birth and address is an identity of some physical person living in Switzerland for almost any observer in Switzerland. On the other hand, BIE1 is an identity with respect to the employees of the BFH only according to the observers knowing the abbreviation scheme. A so-called Cookie on the Internet is an identity of the virtual person «the one using this browser on this machine» with respect to the users of a web site, according to the administrator of this web site. For most other observers this might be just an identifier.

## 3.2 Identification

**Definition 7 (Identification)** *Identification is a process done by an observer; identification means the process of linking a virtual person to another virtual person or to a subject.*

In the identification process, the observer must answer two questions

- Do I trust the *existence* of a link ?
- Do I trust the *non existence* of a link ?

There are three[4] cases (Fig.4):

[4] Note that answering yes to both questions is a nonsense.

- *yes / no* I am convinced that both entities are linked
- *no / no* I don't know
- *no / yes* I am convinced that both entities are not linked

The thresholds used in this process to make a decision depend on the application.

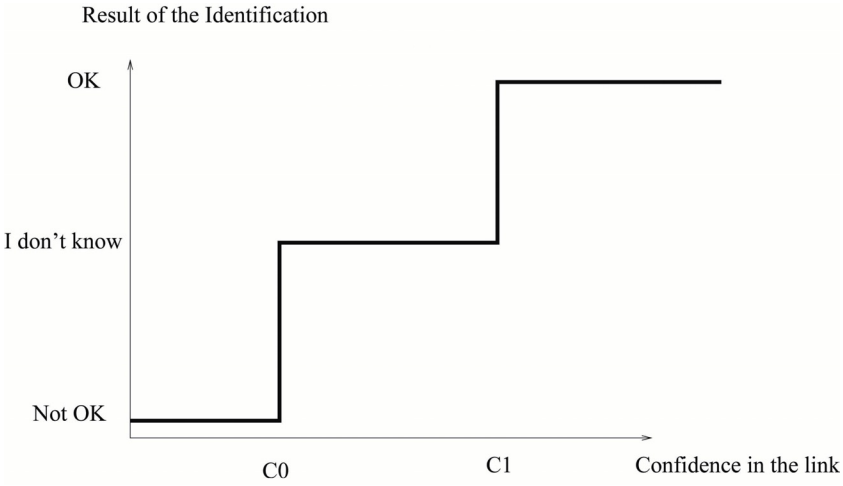


Figure 4: The three cases

For the identification of a client by the doorkeeper of a bar, C1 is quite low. On the other hand the confidence in the identity of the person launching a nuclear rocket has to be much higher.

The identification as introduced above leads to two generic cases:

- validation of a claimed link (verification of an identity)
- search for existing links (search for matches)

### 3.2.1 Verification of an Identity

We present two typical examples for such a process; of course many more can be thought of.

**Login on a System** Consider the classical problem of the identification of a user by a server. The user wants to have access to a computer system and tries to identify itself with its username (FRODO) and its password. Let's consider this situation from the point of view of the server (here the actual observer) which has to grant the access (or deny it), cf. Fig. 5.

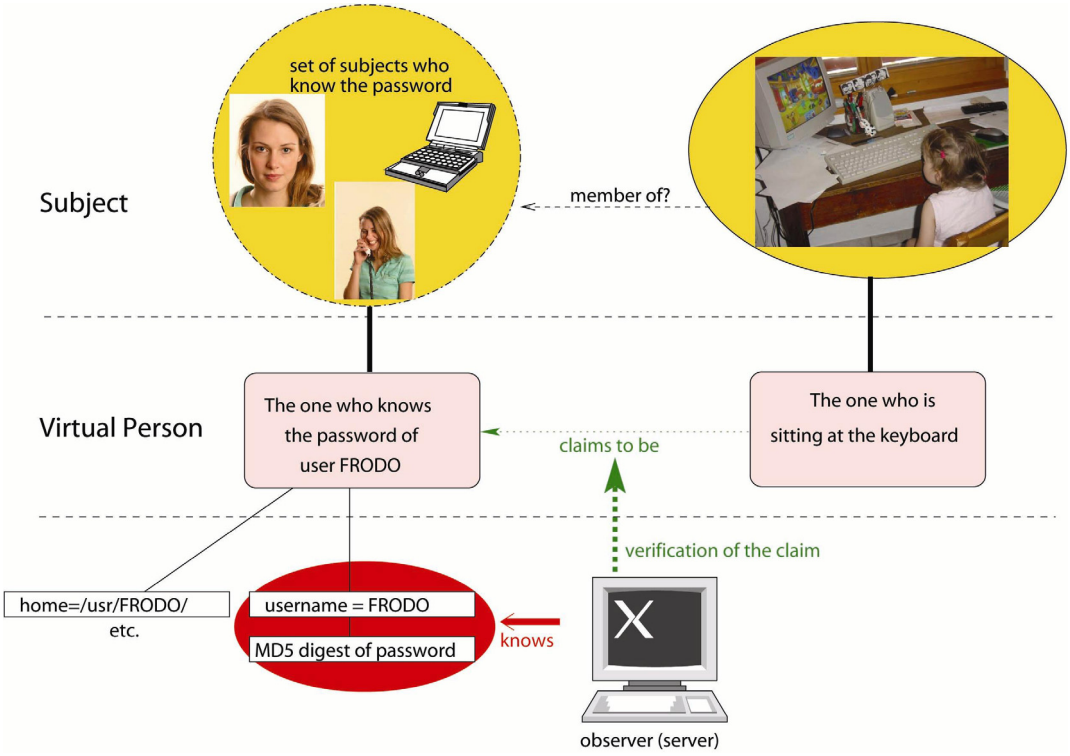


Figure 5: Login on a system

The server has to deal with two initially distinct virtual persons: the first one is the virtual person "The one who knows the password of the user FRODO", the other one is the virtual person "The one sitting at the keyboard". Moreover, the observer has access to some information tautologically identifying the first virtual person, e.g. an MD5 digest of FRODO's password. The second virtual person claims to be the first one. Here the server has to check this claim, and usually will do this by asking to provide the password. The level of confidence of the server in the existence of a link between both virtual persons is high enough if and only if the password is correct.

Note that the server can never be sure of the real existence of this link. But to give access to the resources, it is only necessary that the level of confidence in this link be high enough.

**Border Control** Consider the situation where you stand in front of a guard at a border, cf. Fig. 6. Usually the guard will ask you to show your passport in order to "check your identity". More precisely, here again, several entities interact: the guard at the border acting as the observer, the virtual person "The one described by the passport" and the virtual person "The holder of the passport".

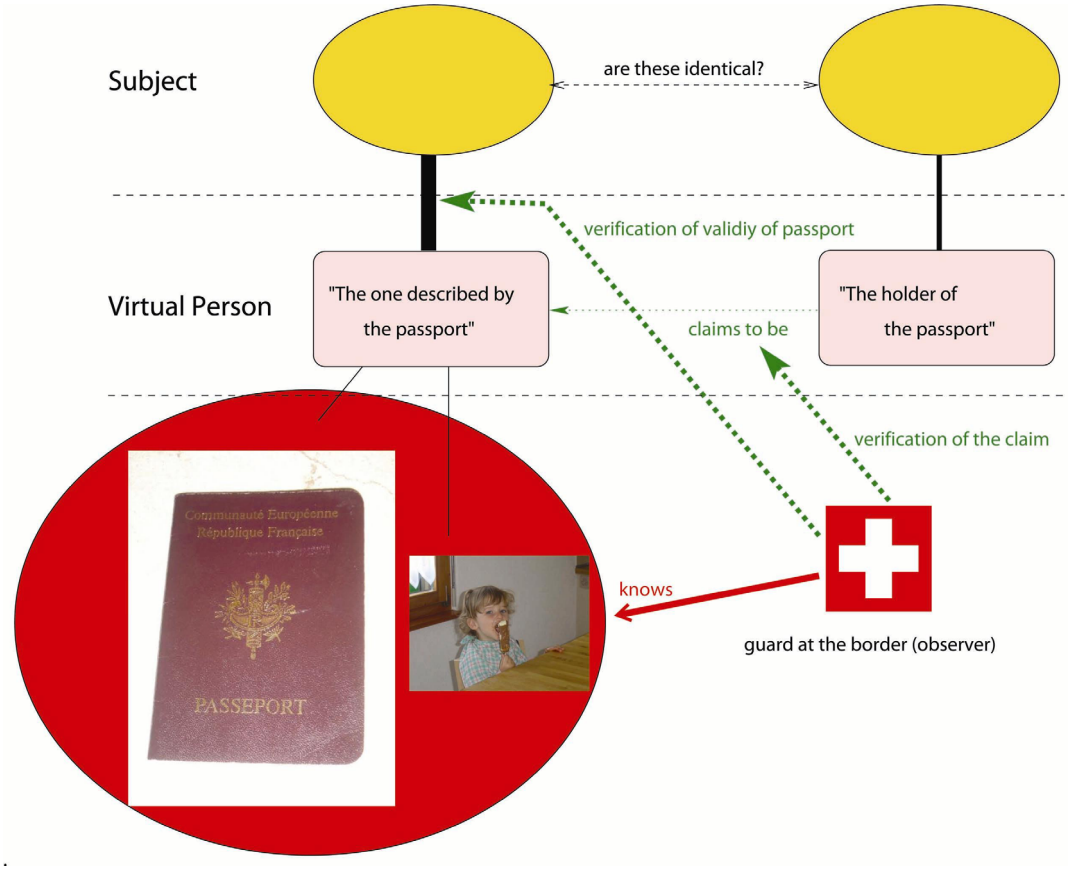


Figure 6: Border Control

Often, the guard will make two different tests:

1. First, he will try to figure out the validity of the passport; in a way he tries to check the validity of the link between this passport and a subject.
2. Then, he will check the existence of a link between both virtual persons, using the information available in the passport: a photo or some biometric data.

### 3.2.2 Search of a Link

The following examples deal with the second kind of identification: search for a possible match between one given virtual person and members of a community of virtual persons. For example, which member of the community matches «best» the given virtual person.

Typical examples: Who is the murderer? To whom do these fingerprints belong? Who is the tallest person in this room?

**Chat: Whom do I talk to?** You know that your friend Alice spends a lot of time in the evening chatting in a chatroom on the Internet. You know very well which chatroom she's usually in, and therefore on a Saturday evening, you decide to enter the same one. Several virtual persons are already in the chatroom, and you would like to know behind which pseudonym your friend Alice really is, cf. Fig .7.

The pseudonyms used in the chatroom are tautological identities of the corresponding virtual persons.

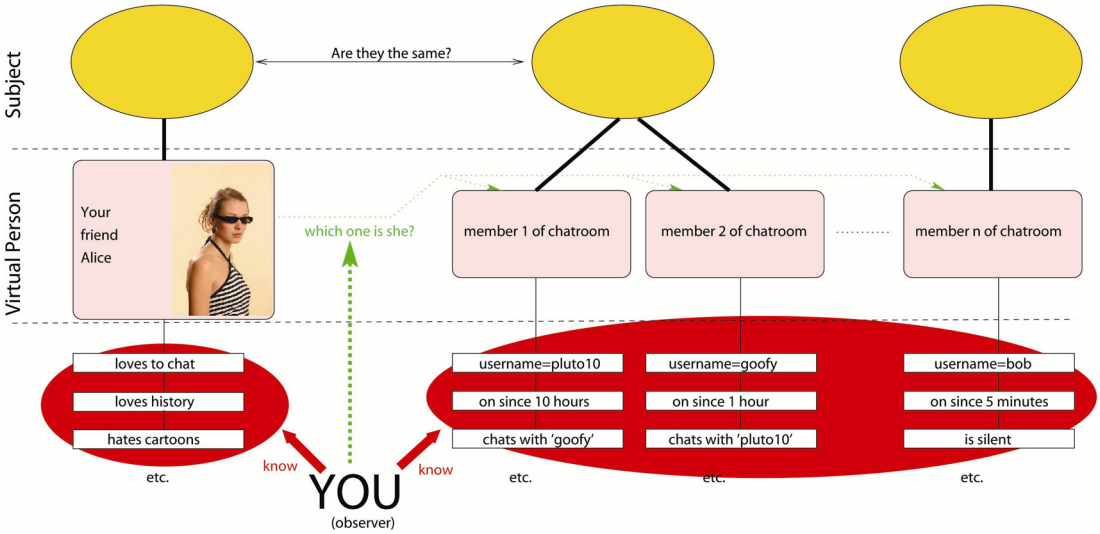


Figure 7: Whom do I talk to in this chat?

In this situation, you are the observer of the situation and the community is the set of virtual persons currently active in this chatroom. You know well the virtual person “My friend Alice” and have some information about her. In the chatroom, there are actually *n* different virtual persons, each one having a name (pseudonym) and some other attributes which are visible to you: for example, how long he/she has been in the chatroom, as well as the partners one specific virtual person is chatting with. You can even eavesdrop on some of the conversations going on and get information thereof. Your goal, as the observer, is now to select the virtual person(s) in the chatroom which your think matches or match “My friend Alice”.

In an optimal situation, you find only one virtual person that matches Alice's profile with high probability from your point of view; but in other cases you might not be so sure. Note that in Fig. 7, there are two virtual persons, members 1 and 2 of the chatroom, which belong to the same subject. Such a situation is clearly possible.

**What's her name?** Now consider the following common situation: a woman is standing in front of you and you know very well you have met her a long time ago but you can't remember her name, cf. Fig. 8.

You quickly go through your memory and try to match one of the virtual persons you've met before with the virtual person “Person now standing in front of you”. Again, in this situation, you are the observer trying to get a link that you can trust while eliminating all the other ones.

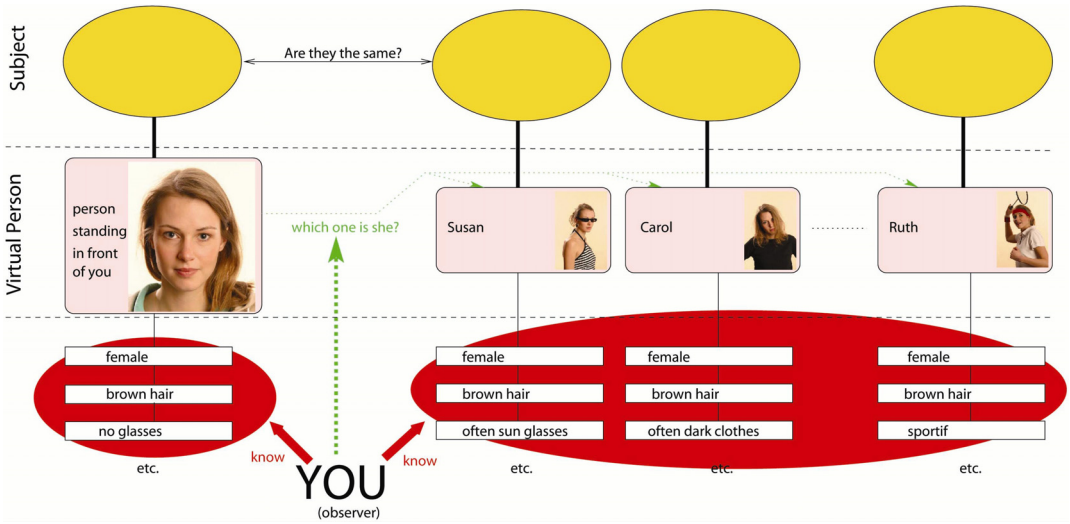


Figure 8: What’s her name?*

# 4 Conclusion

The concepts defined in this article, especially both concepts of subjects and of virtual persons, allow a better description and understanding of many identification, authentication and authorization schemes, by creating a generic model. We have seen that we can apply this model in a diversity of examples: username/password, border control, finding someone in a chatroom.

The concept of virtual persons allows a unified handling of (currently) existing and/or non-existing subjects, even if the subjects are of different types.

Pseudonyms become a special kind of identity. Authentication and authorization schemes become a special case of identification in our unifying model. Indeed, identification is not always linked to a subject anymore.

From a practical point of view, most identifications actually occur between virtual persons.

* Pictures of the woman in this paper are copyrighted. Christoph Edelhoff has granted us the right to use them.

# Bibliography

We want to quote here two recent references dealing with identity, identification and authentication.

*WHO GOES THERE ? Authentication Through the Lens of Privacy*

Stefan T. Kent and Linette I. Millett, editors

National Research Council of the National Academies
The National Academy Press, Washington DC, 2003
ISBN 0 – 309 – 08896 - 8

*TOWARDS UNDERSTANDING IDENTITY*

Caspar Bowden, Microsoft
Pete Bramhall, HP
Kim Cameron, Microsoft
Marco Casassa-Mont, HP
David Colville, Capgemini UK
David Goodman, IBM
Jeremy Hilton, Viviale
Michael Marhoefer, Siemens
Michael White, Guardeonics

www.eema.org, EEMA, 2004