David-Olivier Jaquet-Chiffelle
Head of VIP, Virtual Identity and Privacy research center
www.vip.ch

Contribution paper: Priorities for future research (applications + legal)

Authentication and/or identification through the virtual world

by David-Olivier Jaquet-Chiffelle
Professor at the University of Applied Sciences, Bienne, Switzerland

Several applications in the e-world should protect the anonymity of the participants, at least as long as they are not doing something illegal… However, in some cases we need strong authentication of the users (for example, someone may be asked to prove that he/she is not under 18, or that he/she is the owner of some electronic money). This is usually the case for e-commerce and m-commerce services. Sometimes a secure identification of the participants is even required; typical examples may be found in e-banking, digital signatures, e-voting, e-government applications.

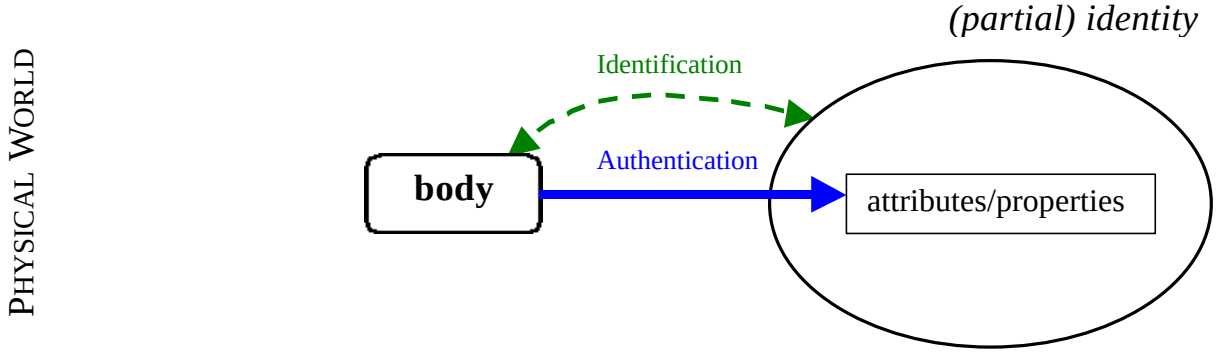
How to protect anonymity and privacy when required and how to securely authenticate and/or identify the entities involved in a protocol when necessary are to my mind among the main challenges for cryptology in the next few years. Actually these challenges are not restricted to cryptology alone; biology, biotechnology, laws for example are involved too.

Basically we have two worlds: the physical one and the virtual one.

In the physical world, the identity of a person is the collection of all his/her personal attributes/properties : name, first name, profession, date of birth, age, sex, social security number, signature, etc. Some attributes are very discriminant, others not. For example, the social security number is much more identifying than the date of birth; and the date of birth is more identifying than the age or the sex. A partial identity is a subset of an identity. Some partial identities allow the identification of their owner, others don't. The identification of a person is the creation of a link between his/her identity (or a partial identity) and this person (his/her body).

To be authenticated in the physical world, an individual has to prove that he/she owns some attributes/properties or some (partial) identity. This is a physical authentication : physical evidence, visual recognition, presentation of official papers, etc.

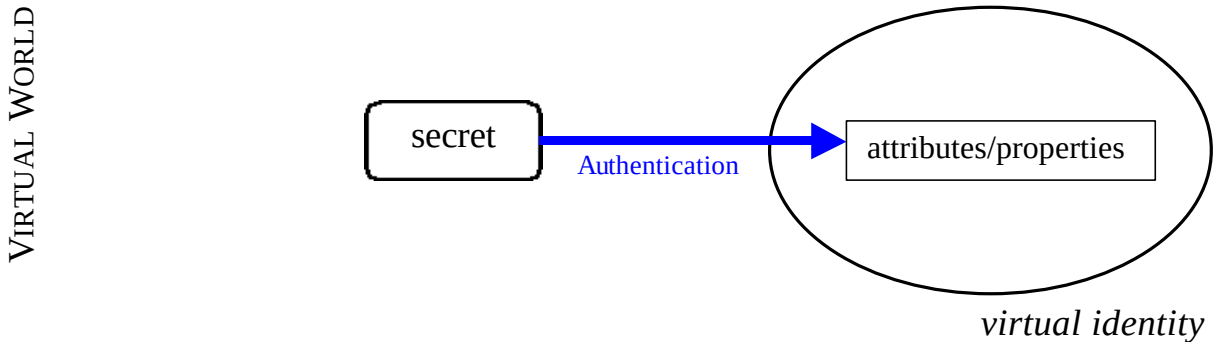
Identification implies authentication, but we can have authentication without identification.



In the virtual world, all identities are virtual. An individual can have multiple virtual identities. A virtual identity is also a collection of attributes/properties.

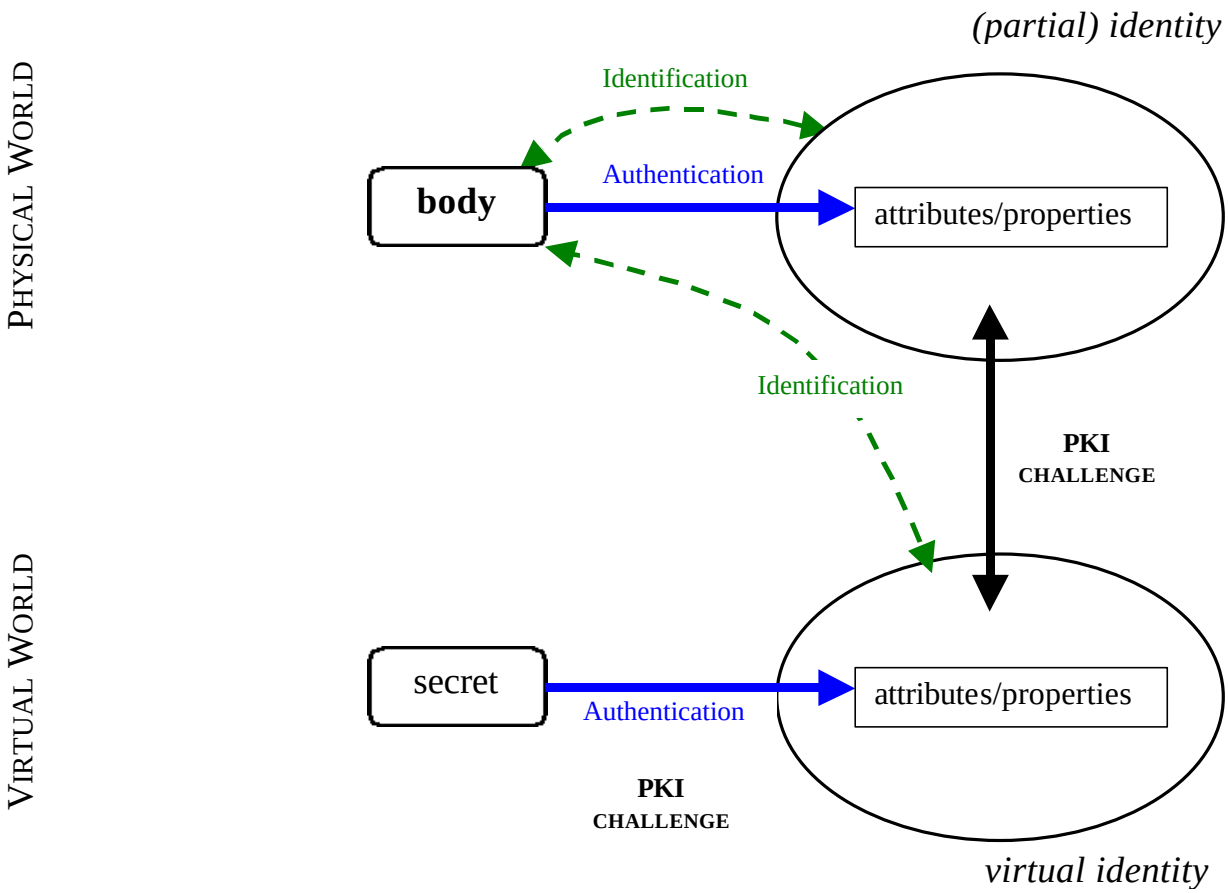
David-Olivier Jaquet-Chiffelle
Head of VIP, Virtual Identity and Privacy research center
www.vip.ch

An authentication in the virtual world consists in proving that someone is the owner of some attributes/properties of a virtual identity. This is a logical (cryptographic) authentication which is usually based on the knowledge of a specific secret related to that virtual identity. The strength of the authentication depends on the security of the cryptographic mechanism (password, challenge-response, zero-knowledge, etc).



To be authenticated in the virtual world just means to prove that we know the secret related to some virtual identity.

The authenticated link between the secret and the virtual identity can be achieved in a PKI. A PKI creates also an authenticated link between a virtual identity and a (partial) identity; it fills a gap between the physical and the virtual worlds.

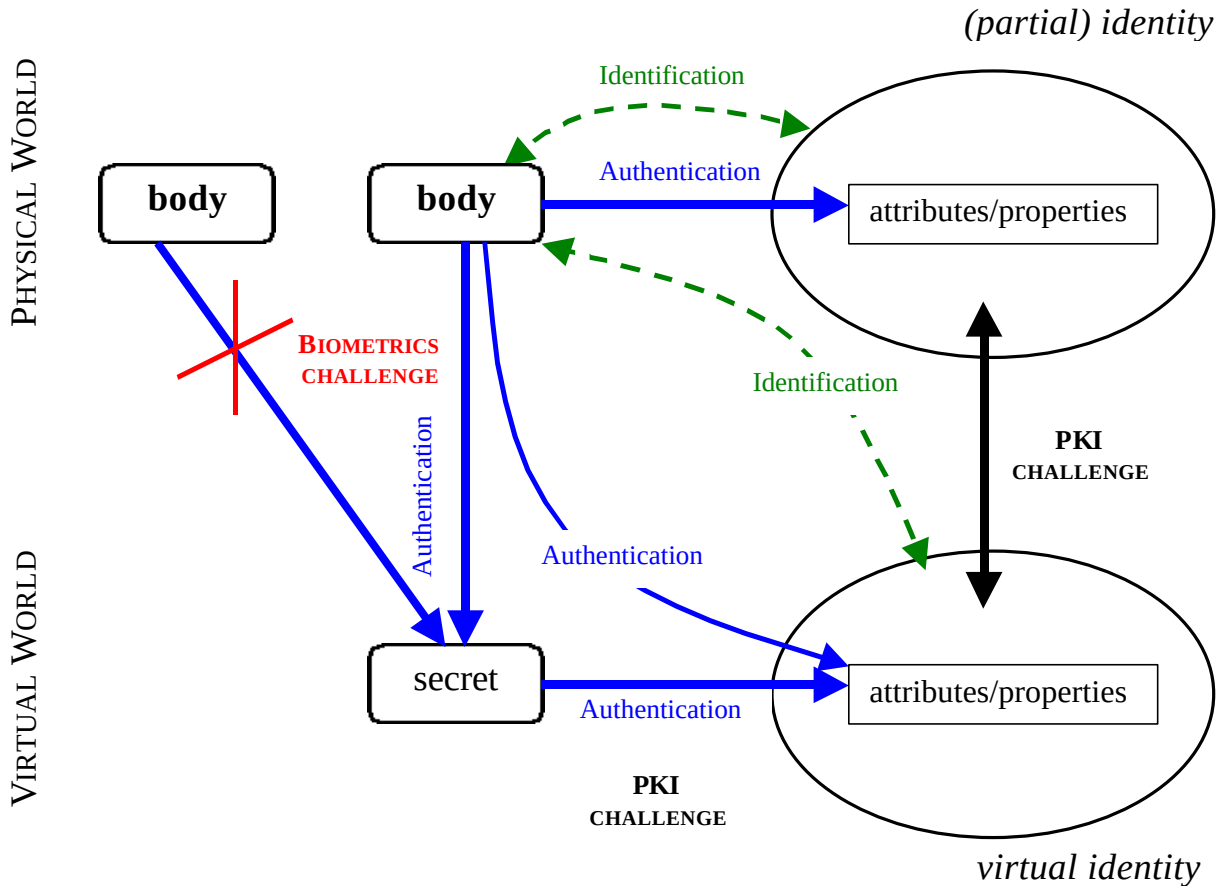


David-Olivier Jaquet-Chiffelle
Head of VIP, Virtual Identity and Privacy research center
www.vip.ch

Given a PKI, a virtual identity is identifying if and only if its corresponding (partial) identity is.

A PKI alone is not enough to make authentication and identification through the virtual world equivalent to those in the physical one. If we want the authentication through the virtual world to be able to replace the one of in the physical world, we need to fill another gap between those two worlds.

The fact that somebody knows a secret is not a strong link between the secret and himself/herself; it is at most a link between the secret and the memory of a person. Another person could know the secret too!. A strong link must be strongly related to the body of a person. It must therefore involve biometrics data.



What is challenging is to find highly discriminant biometrics data which are easy to use and hard to forge.

Therefore, to make authentication and identification through the virtual world equivalent to those in the physical one, we need to solve not only the PKI challenge but also what I call the biometrics challenge.

A third challenge consists in solving the previous ones while preserving privacy. Biometrics data are very sensitive; we cannot change them, we keep them for our whole life. Centralized databases with biometrics data, for example, are very critical from a privacy point of view.

These challenges are to my mind the key(!) challenges to make transactions in the virtual world as trustful as those in the physical one from both the technological and the legal point of view.