

Identity on SIM card or Hèrmes-Comm™ ID

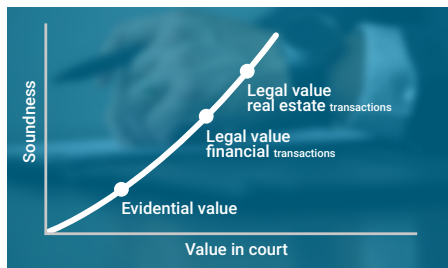
PEOPLE'S IDENTITY CERTAINTY

There are several ways to recognize a person's identity:

- Login with USERNAME + PASSWORD
- Token via SMS or Email
- Remote digital signature
- Biometric recognition (iris, fingerprints, face data, ...)
- Asymmetrical keys
- Keys certified by a *Certification Authority* (**Digital Signature**)
- Digital signature authenticated with the Public Official d. signature



Different conditions in the scenario in which they are used make the choice of one or other methods more likely, such as: type of application, criticalities in place, sophistication level of the attacks (that grows continuously and becomes more and more dangerous with time).

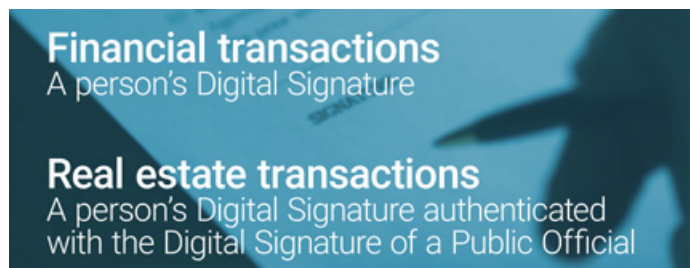


LEGAL AND TECHNICAL VALIDITY

All these methods are right and functional **from a technical standpoint**; on the other hand, they show relevant differences in their **level of security**; last two aside, *International Regulations* recognize **only evidential value** to the others. Only *Digital Signatures* have a recognized legal value because their technical level of security is considered to be safe from counterfeiting. The last level, *Digital Signature authenticated with Digital Signature of a Public Official*, is required to confer full legal value to *real estate transactions*.

FULL LEGAL VALUE

Giving the *full legal value* to a way of identification means that the identity is certain unless there is a legal complaint, thus similar to the one authenticated by a *Notary Public* for *financial transactions*. For *real estate transactions*, full legal value is only given with *Digital Signature authenticated with the Digital Signature of the Public Official*.



REGULATIONS

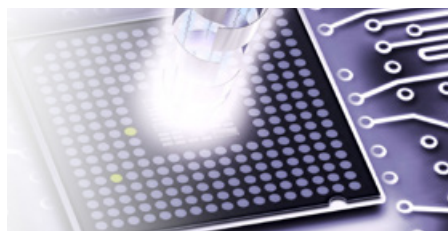
- UE - EIDAS European Electronic Identification and trust services
- UE910/2014 European directive (identification)
- UE 2366/2015 or PSD2 European directive (payments)
- USA - SEAL Digital signature and electronic authentication law
- USA - E-SIGN ACT Electronics signatures in global and national commerce act
- USA - UETA Uniform Electronic Transactions act

SMARTCARD

The internationally recognized and safe method for financial transactions is:

- A. Based on *Digital Signature*
- B. Held on a *safe electronic device* (Smartcard with cryptographic processor)
- C. Granted by a legally approved *Certification Authority* (CA).

Smartcards can't be conveniently used on mobile devices.

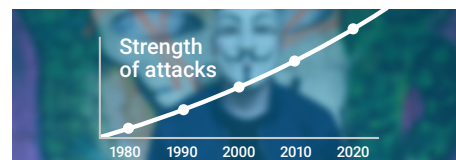


PROCEDURE FOR REQUESTING THE SMARTCARD

1. A person applies for a signature device (*Smartcard*)
2. The *Certification Authority* (CA) recognized by the State states the certain identity.
3. The CA issues the *Digital Signature* on the *Smartcard* (*safe signature device*: anti-tampering cryptographic chip) from a HSM (*Hardware Security Module*).

SECURITY LEVEL

Is the security level guaranteed by the *Hèrmes-Comm™ Secure Element* necessary? Without a doubt, it already is in some applications (eg: military or with high criticalities). And in time, with cyber attacks getting better and better, it will be essential even in regular situations.





VALUE OF THE ID ON A SIM CARD

The personal identity on a SIM Card is a *technical certification of identity* that has *evidential value* but not the full *legal value*. The link between owner and SIM card is indeed:

- Certified by SIM card carrier (the shop) that does not have the power of a *Public Official*
- Registered using hardware circuits and software applications
- Not registered directly by a HSM (*Hardware Security Module*).

Counterfeiting identities with this method is technically possible.

Services based on a code sent via a text message or with installed Apps are vulnerable because they are tied to the telephone number and not to the “physical possession” of something, not even the SIM Card. A telephone number can indeed be easily transferred to a new SIM. The transition from physical SIM to eSIM (embedded into the smartphone hardware and non-removable) worsens the problem because the eSIM must be programmed OTA, an unsafe procedure; moreover, unlike a *Secure Element*, it can't be moved to other devices.

BENEFITS OF THE HÈRMES-COMM™ ID

The Hèrmes-Comm™ Technology obtains the same level of security and certainty of fully approved methods, and thus making *the identification of a person on a mobile device certain and compliant*. Apps that can make transitions (such as payments, internet banking, orders, purchase of tickets, access to reserved areas or opening of gates and cars) can communicate with Hèrmes-Comm™ to guarantee the legal and technical certainty of a person's identity. The *Secure Element* can also be used on other devices along with smartphones: PCs, Tablets and computers.



DISTINGUISHING FEATURES

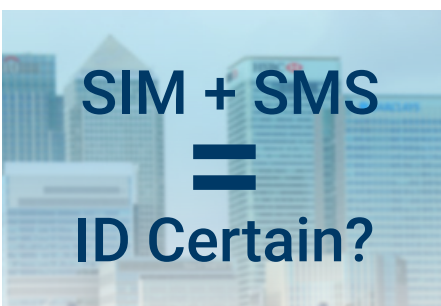
The Hèrmes-Comm™ Technology offers additional benefits to the aforementioned:

1. It uses the *digital signature standard* already in use and widespread.
2. It is independent from the *operating system*: the *Secure Element* works on any kind of *Smartphone* and *Tablet*.
3. It doesn't require any *driver software*.

SPECIAL APPLICATIONS

We can imagine a lot of applications that are not possible with regular SIMs, such as:

- Digital camera memory card that lets *digitally sign* shots (eg: in *forensics*).
- Ability to provide legal value (*digital signature and time stamp*) to videos shot on videocameras in cars, such as dash cams.



PSD2

PSD2 (*Payment Service Directive 2*), in use since Sept 9 2019, requires the use of a 2-step *authentication* for transactions. It is commonly accepted that one of them is a *text message received on the Smartphone or on the App*. This procedure is at risk because the telephone number can be transferred easily to another SIM Card. We tested this by requesting our *phone carrier* to have a number transferred from a *corporate SIM card* to a *private one*: **once the transfer was complete without any issue, we could access** our company's bank accounts and make transactions.

WHAT IS HÈRMES-COMM™

Hèrmes-Comm™ is a communication method between hardware and software

- Patented in 64 countries around the World
- Certified at the top level of Inventive Step by EPO (*European Patent Office*) and WIPO (*World Intellectual Property Organization*)
- Granted in USA by USPTO (*United States Patent and Trademark Office*)
- Nominated “Cool Vendor 2017” by Gartner Inc.
- Certified for the use with *Thin-Clients* by PRAIM



Hèrmes-Comm™ is the *Intellectual Property* of: HERMES COMM SRLs (*Innovative Startup*), via Broletto, 39 - 20121 Milan (Italy); 11622 El Camino Real, Suite 100 - San Diego, CA 92130 - USA. ©HERMES COMM SRLs 2019 - www.hermes-comm.com