## IMPORTANT!!!
## CORRECT TESTING AND APPLICATION OF RFID UHF TAGS

Anti-metal tags
If the tag is anti-metal it should be pasted (glued) on the metal surface. Pasted on metal, but do not hold it in your hand!
The tag is so designed, it only works on metal.

Regular tags
If you have a regular tag, stick it on a cardboard box, plastic and the like. It can not be glued to the metal or Liquid !!! You can not test tags in your hand !!! You have to test it as it should work REALLY.

Laundry textile tags
If you have laundry tags they must be sewn into the fabric!
If tags for clothes, you should hang them on clothes.

Tags for liquids
Special tags for bottles and water, tags used for liquids.
There are no universal tags.

You must correctly check the tags using their actual application.

The smaller the tag - the smaller its reading range.

The reading range is achieved by installing a powerful antenna.

## RFID UHF TAG

RFID technology's main properties are remote identify and track tags attached to objects and informations exchange.

Today we will talk about the security measures we can use to protect the data within an UHF RFID passive transponder. This standard is the most used kind of radio frequency in logistic and industrial applications for its ability to read multiple tags at far distance. And also we will talk about the new chip standard …

Today the  UHF RFID transponders are Class 1 Gen 2. This kind of tag was release of 12 years ago in order to create to unify tag and hardware manufacturers under one global standard for a better interoperability. The previous version named Class 1 Gen 1 contained virtually no security features because at the time security measures were auxiliary in production. In the 2004 newly emerging issues forcing EPCglobal and ISO to respond with increased security measures on UHF tags in the Gen 2 standard. The results were to provide the first layer of protection against hackers through serialized TID numbers and passwords.

## TID numbers

These numbers were introduced for identifications purposes but in these years became widely used for the authentication, due to its uniqueness for each tag and uncounterfeiting skills. Each tag leaves the factory with a unique TID number and it is not modifiable by a normal user. Generally, to authenticate a tag that is suspected to be fake, the only way to check it is reading the EPC memory bank and the TID memory bank, if they doesn't match, that tag is counterfeit.

## Passwords

On Class 1 Gen 2 tags are available two differents password functionalities: the access password and the kill password. Both passwords are stored in factory on the reserved memory block and come pre-encoded with zeros, which do not function as an access or kill code.

### Access password

The access password on UHF Gen 2 tags must be modified in order to be used. Four lock states exist on each memory bank:

Unlocked
Perma-unlocked (can never be locked)
Locked
Perma-locked (can never be unlocked)
When a memory bank is locked, only the reader that interrogates it first with the access code could read it. The access code can also prevent readers from reading the reserved memory bank if it is locked. It is important to note that a small piece of software is usually required in order for the reader to interrogate the tag.

### Kill password

This code is used for applications that require tags to change state/phase to indicate a specific event has occurred. In retail applications it is used because once an item is purchased the tag can be killed, making it permanently unreadable. Many producer in different markets, that track their products during the manufacturing and storage phase, kill them when leave the factory.