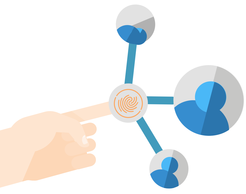
Gemalto answers to 9 myths frequently associated to biometric usages

MYTH 1.

My fingerprint can be easily duplicated

Definitely not, the card can't be fooled by a 2D replication of your fingerprint.



MYTH 2.

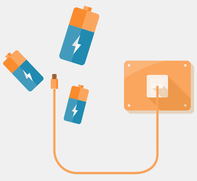
My fingerprint data will be shared with others

No, your fingerprint information is only stored on the card. It is never sent to the bank or collected by a third party.

MYTH 3.

The card needs to be charged to provide power to work

You are right, the card needs power to work. However, with Gemalto's solution, the card doesn't rely on a battery to work. The payment terminal provides all the power the card needs.



MYTH 4.

An attacker could just chop off my finger and use the card

This is an extreme and unlikely scenario as you can block your card with a single phone call. Additionally, biometric sensors and verification algorithms are evolving rapidly to avoid this kind of risk.

MYTH 5.

Attackers could extract the biometric data stored on my card

Absolutely not, all finger print data is converted and encrypted. So even if they did get the file, they wouldn't be able to be access the data.

MYTH 6.

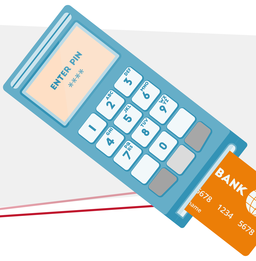
My fingerprints change because of my job, it won't work for me

No reason to worry, the card allows automated and regular updates to the fingerprint templates.

MYTH 7.

It is useless for people that have to pay for others people's goods

All new biometric cards still have the option to use the PIN code.



MYTH 8.

The new payment card will not be accepted everywhere

Yes, Biometric cards work wherever you can pay with a card today, meaning no terminals or roll out costs for merchants.

MYTH 9.

Finger print scanners don't work all the time

Biometric cards must be certified by international payment networks, ensuring greater reliability than current experiences (e.g. with smartphone).

To find out more about the biometric EMV card, visit

www.gemalto.com/financial/cards/emv-biometric-card