Privacy card
BIOMETRIC SOLUTIONS S.R.L.

PRIVACY CARD - BIOMETRIC SOLUTIONS S.R.L.
REGISTERED IN THE SPECIAL SECTION FOR INNOVATIVE START-UPS
Registered Office: Viale Palmanova, 73/R - 33100 - Udine *(Italy); Adm. Office:* Via Francia, 4 - 37058 - Sanguinetto - Verona *(Italy); Operations Office*: Via Fortunato Zeni, 8 c/o BIC – 38068 Rovereto - Trento *(Italy);*
R.E.A.: UD – 298801 / VR – 432745 / TN- 231281 – *VAT No.:* 02929880306
SHARE CAPITAL: ***€960,000.00 fully paid-up***
www.privacycardsrl.com - info@privacycardsrl.com

The solution for personal access to ministries, courts, hospitals, public entities...

A large number of companies and entities need to verify their employees' entry and exit. The employee is required to "punch the timecard" for each entry and exit.

Usually these activities are carried out by providing each employee with a personal badge (card) that is utilised in dedicated readers, which register entries and exits.

It is well known and emphasised by various media services that there is a problem: the badge can be used by anybody and it is common practice for an employee's "timecard" to be punched by a friend. Thus, the employee is registered at work when in actual fact he/she is absent.

This problem could be easily resolved by memorising some biometric data in the control system (fingerprints being the most obvious), but this would go against the privacy concept.

In this case, the **PrivacyCard** would resolve this problem by ensuring that the badge is effectively used by its owner. Our card is able to memorise the biometric data inside the same badge, which is duly encrypted. Therefore, the said biometric data is not memorised in an archive and consequently the employee's personal data will remain in the latter's complete possession.

Let us give a factual example of the PrivacyCard functionality, let's compare the existing systems.

The systems already available on the market can be divided in two main categories.

FIRST CATEGORY	***SECOND CATEGORY***
Biometric readers that retain biometric data inside the same reader (with a memory capacity ranging from 300 to 2000 fingerprints) or in an external storage/archive (which is usually a connected network). In this case, the user's identification will be identified by comparing the fingerprint with the number of fingerprints stored in the external reader/storage.	System in which the fingerprints are memorised inside the card and not in the reader. But the fingerprint processing will be carried out inside the reader, i.e. in this case, the template (the fingerprint) will be transferred to the reader, which will carry out the matching/comparison, between the card template and the data obtained from the reader.

PRIVACY CARD

Our system entails the "matching on card": the memorised biometric data inside the card will not be readable externally and will never leave the card. On the other hand, it is the data acquired by the biometric reader which will enter the card and the matching/comparison will be carried out in the chip.

Moreover, the patent will also entail the enrolment on card, i.e. the fingerprint processing will be carried out by the chip available on the card and the biometric data will never be readable by external devices.

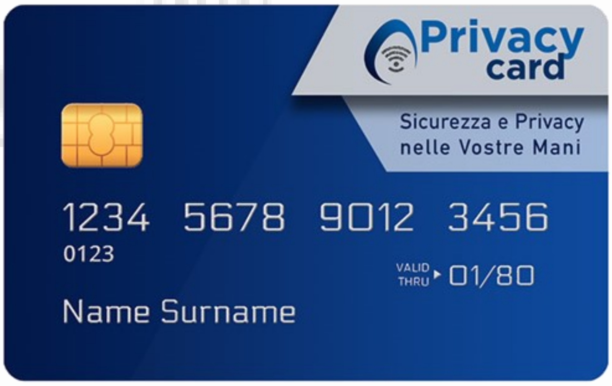
Another important aspect is the fact that there is no computer connected to the writer that will send the card fingerprint.

WHY SHOULD THE PUBLIC ADMINISTRATION USE OUR SYSTEM?

PUBLIC ENTITIES’ PROBLEMS	*WITH THE PRIVACYCARD*
Absenteeism in Italy approximately **costs 7 billion euro per annum** to the State, i.e. half a point of the GDP. The said 7 billion euro include the so-called ***“furbetti del cartellino***” (employees who avoid punching time controls) (approx. **4.9 billion euro per annum**).	The issue related to the *“furbetti del cartellino*” (employees who avoid punching time controls) would be completely resolved through our system, due to the fact that employees would be required to validate the personal fingerprint in the respective readers before punching and consequently they cannot send a colleague to replace them. Therefore, the State would be **saving approx. 4.9 billion euro per annum.**
Absenteeism results in low productivity and an increase in the hours required to carry out any type of activity.	The reduction of the *“furbetti del cartellino*” (employees who avoid punching time controls) would lead to higher productivity and a reduced number of required working hours.
Collection of sensitive data related to employees and compilation of a large number of GDPR forms.	There will not be any Privacy issue since this system is entirely in line with the Privacy Protection regulations and consequently there is no need to register the GDPR forms.
Unions are against the collection and processing of the employees’ biometric data in order to monitor attendances.	The unions will not have any reason to oppose this type of system since it is in conformity with the Privacy regulations and the data collected will remain in the employee’s possession.
Secure punching process.	**PrivacyCard** has an internal traceability system that enables the serial number memorisation of the reader used to validate the attendance.

The feature, that we have patented internationally, which makes us unique is provided by an extraordinary specific technique: the system entails the management of biometric data, which are very sensitive and valuable, since they are unique, totally offline, for the collection and verification phase, by always remaining in the possession of the owner without the possibility of being used in case of negligence. Therefore, the system ensures maximum protection of the specific data thus avoiding storage, transfer and processing issues, which would be contrary to the stringent European Privacy regulations.

The biometric card that protect your privacy!!



PrivacyCard, personal and secure, has been created to protect the citizen’s privacy.

It ensures that the user is actually the card owner, and at the same time it does not provide personal information on the user!!