

Die Lösung für den personalisierten Zugang zu Ministerien, Gerichtshäusern, Krankenhäusern, öffentlichen Unternehmen ...



Brevetto internazionale

International patent



ISCRIZIONE NELLA SEZIONE SPECIALE DELLE START UP INNOVATIVE

In den meisten Unternehmen und Einrichtungen müssen die Ein- und Ausgänge der Mitarbeiter überprüft werden. Mit anderen Worten: Mitarbeiter müssen bei jedem Ein- und Ausgang „ihre Karte abstempeln“.

Normalerweise geschieht das, indem der Mitarbeiter mit einem persönlichen Ausweis (einer Karte) ausgestattet wird, anhand derer spezielle Lesegeräte seine Ein- und Ausgänge erfassen.

Das Problem damit ist jedoch weitgehend bekannt und war auch bereits das Thema mehrerer Berichterstattungen in den Medien: der Ausweis kann von jedem verwendet werden, und oft führt das dazu, dass ein Mitarbeiter die Karte eines Freundes „abstempelt“. Das heißt, dass ein Mitarbeiter als anwesend registriert wird, obwohl er es gar nicht ist.

Eine einfache Lösung für dieses Problem wäre, einige biometrische Daten (am offensichtlichsten: einen Fingerabdruck) im Kontrollsystem selbst abzuspeichern, was im Konflikt mit den Prinzipien des Datenschutzes steht.

PrivacyCard löst dieses Problem und garantiert gleichzeitig, dass der Ausweis tatsächlich von seinem Eigentümer verwendet wird. Unsere Karte kann die biometrischen Daten mit einer entsprechenden Verschlüsselung im Ausweis selbst speichern. Es ist somit nicht erforderlich, die biometrischen Daten in einem Archiv zu erfassen, und die personenbezogenen Daten des Mitarbeiters bleiben sein alleiniges Eigentum.

Lassen Sie uns die PrivacyCard mit bestehenden Systemen vergleichen, um ihre Funktionsweise besser zu verstehen .

Die bereits auf dem Markt befindlichen Systeme können in zwei Hauptkategorien unterteilt werden.



ERSTE KATEGORIE	ZWEITE KATEGORIE
Biometrische Lesegeräte, die biometrischen Daten im Lesegerät selbst (mit einer Speicherkapazität von 300 bis zu 2.000 Fingerabdrücken) oder in einem externen Speicher/Archiv (normalerweise einem an das Netzwerk angeschlossenen Computer) aufbewahren. In diesem Fall erfolgt die Benutzeridentifikation durch Vergleich des Fingerabdrucks mit der jeweiligen Anzahl an Fingerabdrücken, die im externen Lesegerät/Speicher gespeichert sind.	Systeme, in dem Fingerabdrücke im Abzeichen selbst, also nicht im Lesegerät, gespeichert werden. Der Vergleich der Abdrücke findet jedoch direkt im Lesegerät statt, was bedeutet, dass die Vorlage (in diesem Fall der Fingerabdruck) an das Lesegerät übertragen wird, das die Vorlage mit den vom Lesegerät erfassten Daten abgleicht.

PRIVACYCARD

Unser System funktioniert mit dem Prinzip „Matching on Card“ (Vergleich auf Papier): Die im Ausweis gespeicherten biometrischen Daten können extern nicht gelesen werden und verlassen niemals die Karte; stattdessen nimmt die Karte die vom biometrischen Lesegerät auf und der Abgleich erfolgt auf ihrem Chip.

Darüber hinaus sieht das Patent auch das „Enrollment on Card“ (Registrierung auf der Karte) vor, d. h. die Verarbeitung des Fingerabdrucks erfolgt durch den im Ausweis vorhandenen Chip und die biometrischen Daten können niemals von externen Geräten gelesen werden.

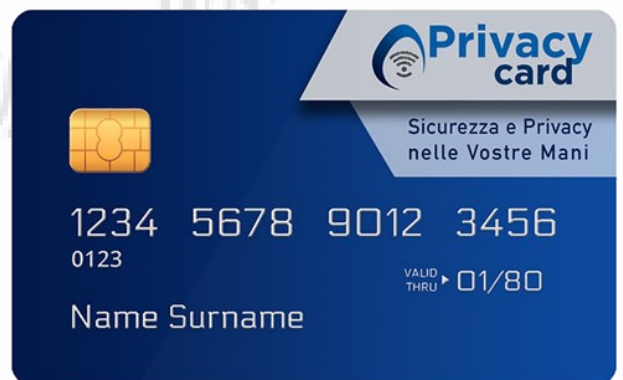
Weiter zu bedenken ist, dass das Gerät, das den Fingerabdruck an den Ausweis schickt, nicht an einen Computer angeschlossen sein sollte.

WARUM SOLLTEN ÖFFENTLICHE EINRICHTUNGEN UNSER SYSTEM VERWENDEN ?

PROBLEME IN ÖFFENTLICHEN EINRICHTUNGEN	MIT PRIVACYCARD
Fehlzeiten in Italien verursachen dem Staat jährliche Kosten von rund 7 Milliarden Euro , was etwa 0,5 Punkte des BIL entspricht. Ein großer Teil dieser 7 Milliarden Euro wird durch so genannte „ Kartenschummler “ verursacht (ca. 4,9 Milliarden Euro jährlich).	Mit unserem System könnte das Problem des „Kartenschummeln“ vollständig gelöst werden, da der Mitarbeiter seinen Fingerabdruck von den entsprechenden Lesegeräten überprüfen lassen muss und somit keinen Kollegen an seiner Stelle für ihn abstempeln lassen kann. Für den Staat würde dies Einsparungen von ca. 4,9 Milliarden Euro pro Jahr bedeuten.
Fehlzeiten führen zu einer geringen Produktivität und die Erhöhung der zur Durchführung der jeweiligen Geschäftstätigkeit erforderlichen Arbeitsstunden.	Eine Verminderung des „Kartenschummeln“ würde somit sowohl die Produktivität erhöhen als auch zu einer Verringerung der Arbeitsstunden führen.
Erfassen sensibler personenbezogener Daten der Mitarbeiter und Ausfüllen zahlreicher DSGVO-Formulare.	Da dieses System vollkommen den Datenschutzbestimmungen entspricht, bestehen keine Datenschutzbedenken und es müssen keine DSGVO-Formulare ausgefüllt werden.
Die Gewerkschaften lehnen die Erfassung biometrischer Daten von Mitarbeitern und deren Verwendung zur Anwesenheitssteuerung ab.	Dahingegen gibt es für die Gewerkschaften keinen Anlass, sich diesem System zu widersetzen, da die erfassten Daten nicht nur den Datenschutzbestimmungen entsprechen, sondern sie auch im Eigentum des Mitarbeiters verbleiben.
Sicheres Abstempeln.	PrivacyCard ist mit einem internen Rückverfolgungssystem ausgestattet, in dem die Seriennummer des Lesegeräts gespeichert wird, mit dem die Anwesenheit überprüft wurde.

Das von uns international patentierte Merkmal, das uns einzigartig macht, zeichnet sich durch eine außergewöhnliche technische Spezifikation aus: Das System ermöglicht es, biometrische Daten, die einzigartig und somit sehr wertvoll sind, vollkommen offline zu verwalten, sowohl zum Zeitpunkt der Erfassung als auch der Validierung. Die Daten verbleiben dennoch jederzeit in den Händen des jeweiligen Eigentümers und können auch bei Fahrlässigkeit nicht verloren werden. Das System garantiert daher den maximalen Schutz dieser besonderen Daten und vermeidet die Probleme mit der Erfassung, der Übermittlung und der Verarbeitung, die im Konflikt mit den strengen europäischen Datenschutzbestimmungen stehen.

**Die zu 100% sichere
die deine Daten
schützt!**



Die sichere und personalisierte **PrivacyCard** wurde zum Schutz der Privatsphäre der Bürger entwickelt.

Sie garantiert, dass sich die Karte tatsächlich im Eigentum des Benutzers befindet, stellt jedoch keine personenbezogenen Daten über ihn bereit.