

ARTYKUŁ

TECHNOLOGIE BIOMETRYCZNE --> USTAWA O OCHRONIE DANYCH OSOBOWYCH

Wraz z dynamicznym rozwojem nowoczesnych technologii, zaczęły pojawiać się pewne wątpliwości, niejasności oraz pytania dotyczące użytkowania biometrycznych systemów Kontroli Dostępu i/lub Rejestracji Czasu Pracy na ODCISK PALCA (BIOFINGER-KD/RCP).

W związku z powyższym należałoby zastanowić się:

- Dlaczego technologie biometryczne budzą tyle kontrowersji wśród Polaków?
- Skąd biorą się uprzedzenia w stosunku do technologii biometrycznych?

Poniższy artykuł stawia sobie za cel przybliżenie Państwu podstawowych informacji dotyczących biometrycznych czytników linii papilarnych, a przede wszystkim dokładne wyjaśnienie najważniejszych aspektów związanych z ochroną danych osobowych.

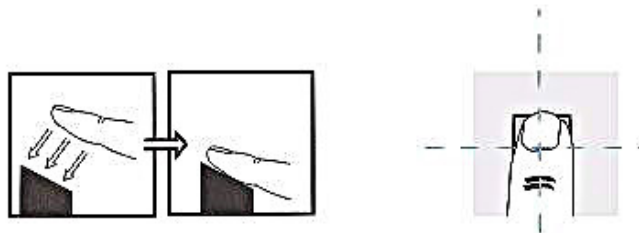
1. PODSTAWOWE INFORMACJE

Użytkownikami biometrycznych systemów Kontroli Dostępu i/lub Rejestracji Czasu Pracy na ODCISK PALCA zostają osoby, których cyfrowy obraz linii papilarnych, inaczej mówiąc, odciski wybranych palców, zostaną poprawnie zarejestrowane w pamięci biometrycznych czytników linii papilarnych. Procesem zarządzania i obsługą systemu biometrycznego oraz czytników linii papilarnych (rejestrowanie/usuwanie użytkowników, konfigurowanie czytników, itp.) zajmować może się tylko osoba do tego uprawniona, np. administrator systemu lub wykwalifikowany serwisant.

W pamięci biometrycznych czytników linii papilarnych oferowanych przez firmę PTC SECURITY SYSTEMS można zarejestrować 1500 lub 3000 cyfrowych obrazów linii papilarnych użytkowników. Dla bezpieczeństwa użytkowników, należy rejestrować co najmniej dwa palce, np. palec wskazujący z lewej oraz prawej ręki lub kciuk z lewej oraz prawej ręki, itp. W praktyce użytkownicy biometrycznych systemów Kontroli Dostępu i/lub Rejestracji Czasu Pracy na ODCISK PALCA posługują się tylko jednym zarejestrowanym palcem.

2. PROCES REJESTROWANIA UŻYTKOWNIKÓW

W procesie rejestracji cyfrowych obrazów linii papilarnych, w zależności od producenta oraz rodzaju czytnika biometrycznego, każdy użytkownik kolejno przykłada dwa lub trzy razy rejestrowany palec do wbudowanego skanera optycznego, np. dwa razy wskazujący palec z lewej ręki.



Rys. 1. Widok poprawnie przykładanego palca do skanera optycznego.



W momencie przyłożenia palca, skanery optyczne odczytują niepowtarzalne wzorce biometryczne, będące zakończeniami lub rozgałęzieniami linii papilarnych. W zależności od producenta skanerów optycznych oraz zastosowanego algorytmu kodowania danych, systemy biometryczne biorą pod uwagę odpowiednią ilość (np. 30, 40 lub 50) punktów charakterystycznych, które odgrywają podstawową rolę w autoryzacji oraz identyfikacji użytkowników.



Rys. 2. Fragment obrazu linii papilarnych w procesie cyfrowej obróbki z uwzględnionymi punktami charakterystycznymi.

W procesie autoryzacji oraz identyfikacji użytkowników odczytywane i porównywane są jedynie te punkty charakterystyczne, które powstały w wyniku matematycznej obróbki rozgałęzień oraz zakończeń w cyfrowym obrazie linii papilarnych. Każdy czytnik biometryczny posiada możliwość dokładnej konfiguracji stopnia bezpieczeństwa, który przekłada się na ilość porównywanych punktów charakterystycznych. Współczynnik bezpieczeństwa wpływa na jakość, szybkość oraz skuteczność działania systemów biometrycznych.

3. OCHRONA DANYCH OSOBOWYCH

Biometryczne czytniki linii papilarnych oferowane przez firmę PTC SECURITY SYSTEMS nie zapisują, ani nie przechowują w wewnętrznej pamięci rzeczywistych obrazów odcisków palców (obrazów linii papilarnych) zarejestrowanych użytkowników. W pamięci czytników biometrycznych zakodowane są jedynie odpowiednie wzorce biometryczne według matematycznych algorytmów stworzonych przez producentów skanerów optycznych. Na wzorce biometryczne składa się odpowiednia ilość punktów charakterystycznych, odpowiadająca zakończeniom i rozgałęzieniom w liniach papilarnych. W procesie autoryzacji oraz identyfikacji użytkowników porównywane są tylko punkty charakterystyczne odczytywane i rozpoznawane według odpowiedniego algorytmu matematycznego.



Nieemożliwe jest odczytanie lub kradzież danych z wewnętrznej pamięci czytników biometrycznych, zawierających informacje o ilości lub rozkładzie punktów charakterystycznych, czy też ich użycie w celu odtworzenia rzeczywistego obrazu linii papilarnych danego użytkownika. Zakodowanych danych w żaden sposób nie można wykorzystać do innych celów niezwiązanych z biometryczną autoryzacją użytkowników w systemach Kontroli Dostępu i/lub Rejestracji Czasu Pracy BIOFINGER-KD/RCP.

4. CZY OBAWIAMY SIĘ NOWOCZESNYCH TECHNOLOGII BIOMETRYCZNYCH? SŁOWO PRAWDY

Czy należy obawiać się nowoczesnych technologii biometrycznych?

Fakty i mity.

Należałoby tutaj wymienić dwa główne aspekty, które wg autora artykułu mogą powodować pewne obawy i negacje wśród użytkowników.

1. Bariera psychologiczna

Niektóre osoby obawiają się lub negują proces rejestrowania cyfrowego obrazu linii papilarnych, innymi słowy wprowadzania odcisków palców do pamięci biometrycznych czytników linii papilarnych, ponieważ wywołuje to u nich negatywne emocje i skojarzenia związane z procesem pobierania rzeczywistych obrazów odcisków palców przez organa ścigania (Policję). Proces rejestracji użytkowników nie ma nic wspólnego z przestępczością, karalnością lub kartoteką skazanych.

Nowoczesne technologie zawsze wyprzedzają ludzką mentalność, myślenie oraz różne przyzwyczajenia i dlatego należy dobrze zrozumieć działanie systemów biometrycznych jak również powoli przyzwyczajając się do udogodnień, jakie niosą ze sobą nowoczesne technologie biometryczne. Jako jeden z licznych przykładów należałoby wymienić Stany Zjednoczone Ameryki Północnej, które w szerokim zakresie w portach lotniczych wprowadziły biometryczną kontrolę osób przyjeżdżających, a w najbliższym czasie obywatele Unii Europejskiej będą również posiadali paszporty biometryczne. W niedalekiej przyszłości wszelkie płatności elektroniczne będą autoryzowane przez użytkownika tylko przy pomocy odcisku palca lub innej charakterystycznej części ludzkiego ciała.

2. Spojrzeć prawdzie w oczy

Nieuzasadnioną negacją w procesie rejestrowania cyfrowego obrazu linii papilarnych w przypadku biometrycznych systemów Rejestracji Czasu Pracy na ODCISK PALCA oferowanych przez firmę PTC SECURITY SYSTEMS jest obawa pracowników przed poznaniem prawdy przez pracodawcę, a co z tym się wiąże zaburzenie niektórych negatywnych przyzwyczajień i zachowań nieuczciwych pracowników.

Powyższe „słowo prawdy” dotyczy tylko tych pracowników, którzy oszukują swojego pracodawcę spóźniając się do pracy, wychodząc z pracy przedwcześnie lub wyświadczają, tzw. koleżeńską przysługę w formie „podbicia karty” lub złożenia fałszywego podpisu na liście obecności.

Ogólnie wiadomo, iż biometrycznych systemów Rejestracji Czasu Pracy nie można w żaden sposób oszukać, przez co niektóre osoby będą starały się wprowadzać jak najwięcej nieuzasadnionego zamieszania próbując chronić własne przyzwyczajenia i zachowania.



Mam nadzieję, iż treść powyższego artykułu w pewnym stopniu przybliżyła i uświadomiła Państwu pojęcie ochrony danych osobowych, ukazała źródło niektórych negatywnych ludzkich emocji związanych z procesem rejestrowania użytkowników oraz rozwiała nieuzasadnione obawy wobec korzystania z nowoczesnych technologii biometrycznych.

Z biegiem czasu coraz więcej osób w Polsce zmieni swoje poglądy i nastawienie wobec wszelkich urządzeń oraz systemów biometrycznych, mając przede wszystkim na względzie pełen KOMFORT i BEZPIECZEŃSTWO, jakie stwarzają między innymi kompleksowe rozwiązania oferowane przez firmę PTC SECURITY SYSTEMS.

Pozostając z wyrazami szacunku,
Jacek Lipski



PTC SECURITY SYSTEMS
mgr inż. JACEK LIPSKI
www.ptc.gda.pl
Gdańsk, 2005 rok

