Wykorzystanie podpisu cyfrowego w kartach chipowych

Sławomir Sobótka

Wstęp

Użycie dokumentów elektronicznych wymaga zastosowania nowych sposobów ich przechowywania oraz przesyłania. Jednym ze sposobów przechowywania dokumentów jest ich zapis na kartę chipową. Dokument znajdujący się na karcie może przemieszczać się wraz z jej właścicielem. Zastosowanie szyfrowania i podpisu cyfrowego zabezpiecza zapisane dokumenty przed niepowołanym dostępem, modyfikacją oraz jednoznacznie określa autora.

Karty chipowe oferują dosyć silną politykę bezpieczeństwa ponieważ zazwyczaj aby wykonać na nich większość operacji trzeba wprowadzić PIN. Dzięki temu polityka bezpieczeństwa opiera się na dwu komplementarnych elementach: coś co mam – karta, coś co wiem – PIN.

Niniejszy artykuł jest próbą zarysowania ogólnej koncepcji wykorzystania technologii kart chipowych i podpisu cyfrowego do stworzenia bezpiecznego obiegu dokumentów medycznych.

Artykuł operuje pojęciami z zakresu podpisu cyfrowego przybliżonymi w artykule „Wprowadzenie do zagadnienia Podpisu Cyfrowego” opublikowanym w poprzednim wydaniu biuletynu.

Wprowadzenie do zagadnienia kart chipowych

Karta chipowa swym wyglądem przypomina zwykłe karty płatnicze, jednak zawiera zatopiony w sobie chip – dosyć zaawansowany układ scalony. Chip jest swego rodzaju mini-komputerem, ponieważ posiada pamięć oraz procesor. Pamięć służy do przechowywania systemu operacyjnego karty, programów oraz danych użytkownika. W szczególności można w niej zapisywać dowolne dokumenty. Procesor natomiast zajmuje się wykonywaniem zapisanych na karcie programów.

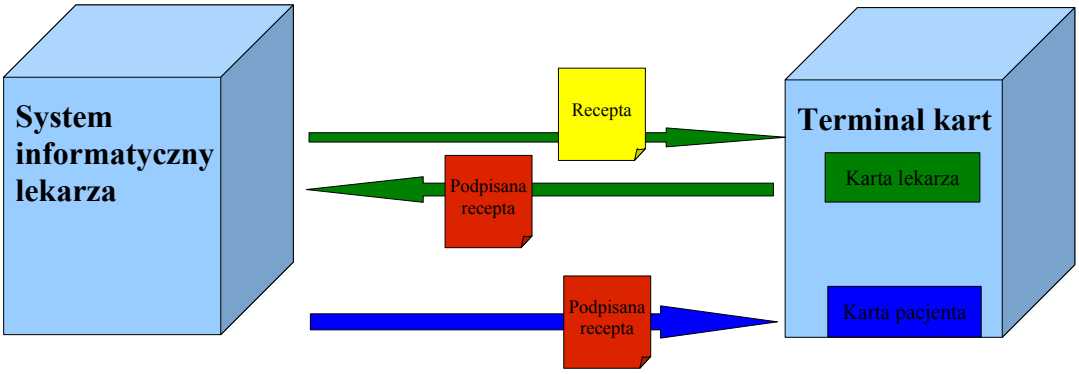
Z powyższego opisu wynika, że karta jest komputerem ogólnego przeznaczenia. Zatem pamięć może zostać wykorzystana do przechowywania certyfikatu, klucza prywatnego oraz programów do szyfrowania i podpisywania dokumentów. System operacyjny karty chroni klucz prywatny przed dostępem z zewnątrz. Procesor może wykonać program podpisujący dokumenty z wykorzystaniem składowanego w chronionej pamięci klucza prywatnego.

Oczywiście aby korzystać z kart potrzebne są terminale - urządzenia do komunikacji z kartami oraz interakcji z użytkownikiem (np.: wprowadzania PINu). Terminale zwykle pozwalają na jednoczesną obsługę kilku kart oraz można je łączyć w sieci po to aby dokonywać operacji między-kartowych. Terminale są wykorzystywane również jako urządzenia pośredniczące w komunikacji pomiędzy kartą a komputerem PC.

Przykładowy scenariusz

Rozważmy znany wszystkim scenariusz wystawienia recepty i jej realizacji z wykorzystaniem kart chipowych oferujących możliwość podpisywania i przechowywania dokumentów. Na wstępie załóżmy, że zarówno lekarz jak i pacjent posiadają własne karty chipowe.

Lekarz tworzy receptę korzystając z własnego systemu znajdującego się na jego komputerze osobistym. Następnie system wysyła do karty (oczywiście za pośrednictwem terminala) żądanie podpisania tejże recepty. W tym momencie terminal prosi o podanie PINu lekarza po to aby zabezpieczyć kartę przed wykonaniem operacji przez nieuprawnione osoby. Po pomyślnej weryfikacji PINu karta przystępuje do podpisania wysłanego do niej dokumentu. Odbywa się to w ten sposób, że procesor karty pobiera z chronionej pamięci karty klucz prywatny a następnie uruchamia program realizujący algorytm szyfrujący. Proszę zwrócić uwagę na fakt, iż klucz prywatny nie jest w żaden sposób udostępniany poza układ scalony karty. Karta poprzez terminal zwraca do systemu lekarza podpis, który to może być dołączony do recepty. Do recepty można również dołączyć certyfikat pobrany z karty lekarza.



W tym momencie recepta została podpisana cyfrowo oraz została opatrzona certyfikatem, zatem mamy pewność co do autora recepty (jednocześnie autor nie może się wyprzeć jej wygenerowania) oraz recepta jest odporna na modyfikacje. Tak przygotowaną receptę zapisujemy na kartę chipową pacjenta. Pacjent okazuje swą kartę w aptece. System aptekarza próbuje zaczytać recepty znajdujące się na karcie, jednak oczywiście pacjent musi wyrazić na to zgodę podając PIN na terminalu aptekarza. System aptekarza może zweryfikować recepty, ponieważ zostały one podpisane cyfrowo. Zatem aptekarz ma pewność, że treść recept nie została zmieniona oraz może zweryfikować ich wystawców.

Zakończenie

Przedstawiony w niniejszym artykule prosty scenariusz można łatwo uogólnić na dowolny przypadek, w którym istnieje potrzeba zabezpieczenia dokumentu cyfrowego. Karta chipowa doskonale nadaje się do tego typu zastosowań z uwagi na jej techniczną wszechstronność oraz silną politykę bezpieczeństwa opartą na podejściu: „coś co mam” i „coś co wiem”.

Pamięć karty może przechowywać klucz prywatny użytkownika oraz jego certyfikat, co jest oczywistym ułatwieniem dla człowieka. Idąc dalej, można wykorzystać kartę do tego, aby to ona sama podpisała dokument dzięki czemu nie ma potrzeby, aby klucz prywatny wydostawał się poza fizyczny obszar karty. Wreszcie sama karta może być nośnikiem podpisanego dokumentu.

Z punktu widzenia ogólnej koncepcji karta spełnia wielorakie funkcje. Może być ona dowodem tożsamości lekarza i jego „pieczęcią" gdyż pozwala na generowanie podpisów oraz jest zabezpieczona przy pomocy PINu. Karta jest również nośnikiem informacji medycznych pacjenta. Zatem możemy pokusić się o stwierdzenie, iż technologia kart chipowych jest doskonałym fundamentem infrastruktury bezpiecznego obiegu dokumentów opartego na idei podpisu cyfrowego.