Ze świata USOS. Część 2 – Każdy student nosi w kieszeni… komputer, czyli o Elektronicznej Legitymacji Studenckiej

Mówi się, że każdy nosi w plecaku buławę. Akurat w odniesieniu do studenta prawdziwe jest powiedzenie, że każdy nosi w kieszeni komputer i wcale to nie oznacza, że studiuje informatykę. Może określenie „komputer" jest nieco na wyrost, choć to całkiem sprawny „komputerek", z własnym procesorem, pamięcią, magistralą i systemem operacyjnym. Mowa o **ELS**, czyli *Elektronicznej Legitymacji Studenckiej*. Takie legitymacje są wydawane na polskich uczelniach od kilku lat (dokładniej od 2006 roku). ELS to plastikowa karta, która od strony graficznej na wszystkich uczelniach wygląda tak samo, gdyż wygląd ten jest określony przez rozporządzenie Ministra Nauki i Szkolnictwa Wyższego. W plastiku są osadzone układy elektroniczne, które mogą się różnić. Rozporządzenie wymaga, aby ELS była wyposażona w **układ stykowy**, a nawet precyzuje, jakie informacje mają tam być zapisane i w jakim formacie.

Układ stykowy widać gołym okiem, w podobny są wyposażone te lepsze karty płatnicze. Większość ELS ma dodatkowo (opcjonalny) **układ bezstykowy**.

Pamięć układu stykowego zwykle ma pojemność do 90 kilobajtów. Pamięć układu bezstykowego zwykle ma pojemność 1 kilobajta.

Ten układ obejmuje chip oraz antenkę do komunikacji. Jedno i drugie jest zatopione w plastiku i wypatrzyć je może tylko sprawne oko. Taki układ jest elementem np. Warszawskiej Karty Miejskiej.

Proces przygotowania ELS jest dość złożony i wymaga specjalnych urządzeń i oprogramowania. Ważną rolę pełni w nim USOS. Gdy do USOS trafią dane nowego studenta oraz zdjęcie w odpowiednim formacie (widoczne lewe ucho), pracownik dziekanatu zleca wydruk ELS. USOS sprawdza poprawność zlecenia – na raz może być aktywne tylko jedno, student nie może mieć ważnej legitymacji, musi być aktualnie zapisany na studia, a osoba zlecająca wydruk musi mieć odpowiednie uprawnienia. Zlecenia napływają równocześnie z różnych dziekanatów (na UW jest ich ponad 50), ale trafiają do centralnej bazy USOS, skąd odczytuje je pracownik **Centrum Personalizacji**. Centrum jest zwykle jedno, a podstawowym jego wyposażeniem jest komputer i drukarka. Drukarka to nie byle jaka, bo przecież ma drukować na plastiku i zapisywać dane w układzie stykowym ELS. Różne są technologie druku na plastiku, akurat na UW stosuje się **technologię termosublimacyjno-retransferową**.

Termosublimacja oznacza zmianę stanu skupienia ciała stałego bezpośrednio w stan gazowy pod wpływem bardzo wysokiej temperatury.

Termosublimacja polega na tym, że barwnik ze specjalnej kolorowej taśmy zamontowanej wewnątrz drukarki jest odrywany i przenoszony na legitymację. Taśma ma trzy kolorowe barwne prostokąty, służące do wydruku zdjęcia, oraz dwa czarne, do wydruku tekstu po obu stronach legitymacji. Retransferowość oznacza, że barwniki nie są przenoszone bezpośrednio na legitymację, tylko najpierw na przezroczystą taśmę, a dopiero z niej na plastik. Dzięki temu jakość nadruku jest lepsza, a legitymacja nie jest narażona na uszkodzenia spowodowane bardzo wysoką temperaturą potrzebną do termosublimacji. W USOSowni (ten portal informacyjny UW reklamowaliśmy w poprzednim numerze) można znaleźć artykuł o ELS ze zdjęciami ilustrującymi przebieg wydruku oraz uczestniczące w tym urządzenia (`http://usosownia.uw.edu.pl/node/292`).

Na awersie legitymacji jest kolorowe zdjęcie, na rewersie, w białym prostokącie, zwykle jest drukowany tzw. **kod kreskowy**. Taki kod kreskowy to nic innego tylko specjalny rodzaj czcionki, w której poszczególne znaki mają postać kresek i odstępów różnej szerokości. Kod kreskowy może być zbudowany na bazie numeru układu bezstykowego, numeru legitymacji studenckiej lub dowolnego innego unikatowego identyfikatora, jaki uczelnia przypisze studentowi. Do odczytywania kodów kreskowych służą specjalne czytniki, na uczelni z tej części ELS korzystają głównie biblioteki.

Personalizacja, czyli nadruk graficzny ELS, to tylko jedno z zadań drukarki. Równie ważne jest wpisanie odpowiedniej informacji na układ stykowy karty. Są to dane osobowe studenta, nazwa uczelni oraz data ważności legitymacji. Dane te są podpisane **podpisem elektronicznym**. Każdy pracownik uczelni, który zapisuje coś na karcie, czyli drukarz lub pracownik dziekanatu przedłużający ważność ELS (o tym będzie później), musi posiadać podpis elektroniczny, w celu cyfrowego poświadczenia zapisywanej informacji.

Jak działa taki podpis elektroniczny? W technologii **PKI** (ang. *Public Key Infrastructure* – infrastruktura klucza publicznego; inna nazwa to **kryptografia asymetryczna**) każdemu użytkownikowi przydziela się parę kluczy oraz wirtualny dokument potwierdzający fakt posiadania konkretnych kluczy przez konkretną osobę (czyli **certyfikat**), wydawany przez **urząd certyfikacji**. W Polsce jest ich tylko kilka. Urząd certyfikacji musi nie tylko dbać o wiarygodność wydawanych podpisów, ale także informować publicznie o tych podpisach, które straciły ważność. Te klucze to dwie liczby – jedna z nich, nazywana **kluczem publicznym**, jest dostępna publicznie, drugą, nazywaną **kluczem prywatnym**, trzeba chronić równie mocno jak PIN do karty płatniczej czy hasło do CAS. Oczywiście, ta para liczb musi mieć odpowiednie własności matematyczne, w szczególności uzyskanie klucza prywatnego na podstawie klucza publicznego musi być **obliczeniowo trudne**. Podpisywanie dokumentu elektronicznego polega na wykonaniu następujących czynności:

1. Tworzony jest skrót dokumentu za pomocą jednokierunkowej funkcji skrótu, czyli charakterystyczna dla niego liczba o określonej długości zależna od użytej funkcji skrótu (o takich funkcjach była mowa w poprzednim odcinku).
2. Uzyskany skrót jest szyfrowany przy wykorzystaniu klucza prywatnego osoby podpisującej. Podczas składania podpisu osoba ta wyraża zgodę na takie użycie, podając kod PIN karty, na której znajdują się klucze. Po zaszyfrowaniu skrótu dokument elektroniczny jest już podpisany.

Weryfikacja podpisanego dokumentu wygląda następująco:

1. Tworzony jest skrót dokumentu (dokładnie tak samo jak podczas podpisywania).
2. Zaszyfrowany skrót dokumentu jest deszyfrowany przy wykorzystaniu klucza publicznego osoby podpisującej.
3. Obie wyliczone wartości porównuje się. Jeśli są równe, to mamy pewność, że dokument został podpisany kluczem prywatnym pasującym do użytego klucza publicznego.

I po co ta cała zabawa z kluczami i podpisywaniem? Po to, żeby nikt nie mógł zapisanej na ELS informacji podrobić, przykładowo wpisując dłuższy termin ważności legitymacji. Taki podpis elektroniczny zapewnia: autentyczność, niezaprzeczalność i integralność dokumentu elektronicznego.

Pytanie do Czytelnika – jak wykorzystać tę samą parę kluczy w celu wysłania do kogoś tajnego listu, który tylko adresat będzie mógł odczytać?

W układzie stykowym karty jest zapisany zarówno podpisany rekord z danymi studenta, jak i certyfikat potrzebny do poświadczenia użytego podpisu cyfrowego. Odczytując dane z układu stykowego karty, można także odczytać certyfikat, czyli dowiedzieć się, kto zapisał te dane.

No tak, ale przecież konduktor w pociągu czy kontroler w tramwaju nie ma przy sobie urządzenia do odczytu danych z układu stykowego (no, przynajmniej jeszcze nie ma). Jak zatem ma sprawdzić ważność legitymacji i uprawnienia studenta do zniżki? MNiSW przewidziało ten problem i wymaga dodatkowo umieszczenia na rewersie ELS **hologramu** z datą ważności. Taki hologram to specjalny rodzaj „znaczka", trudny do podrobienia (technika wytwarzania podobna jest do produkcji banknotów). Zatem ważność legitymacji jest poświadczana na dwa sposoby: poprzez datę wpisaną cyfrowo na układzie stykowym i naklejony na ELS hologram z datą.

A to jeszcze nie koniec! Przecież na większości ELS jest także układ bezstykowy. Układ ten może zawierać 16 sektorów, służących do zapisu informacji. W pewnych miastach niektóre z tych sektorów są wykorzystywane jako nośnik karty miejskiej (tak jest np. w Warszawie, Poznaniu, Wrocławiu czy Krakowie). Dlatego właśnie blankiety ELS, nim od producenta trafią na uczelnię, najpierw wędrują do MZK, gdzie przygotowuje się sektory układu bezstykowego do pełnienia roli karty miejskiej.

Numer układu stykowego i układu bezstykowego jest unikatowy dla każdej karty na świecie. Oba te numery trafiają, oczywiście, do USOS-a wraz z informacją o wydaniu studentowi ELS i o użytym certyfikacie.

Uff, ELS gotowa, teraz może trafić do rąk studenta. Student może się nią cieszyć… przez semestr, bo po semestrze traci ważność. Na szczęście przedłużanie ważności ELS jest prostsze od jej drukowania, bo nie wymaga zmian w części graficznej. Nie potrzeba do tego drukarki, dzięki temu można to zrobić w dowolnym dziekanacie. Potrzebny jest jedynie czytnik układu stykowego i podpis cyfrowy. Pracownik dziekanatu wkłada ELS do jednego czytnika, a swoją kartę z certyfikatem do drugiego (często jest on wbudowany w klawiaturę). USOS odczytuje informacje z ELS, zmienia datę ważności, podpisuje zmieniony rekord (oczywiście pyta o PIN) i zapisuje go na legitymacji. Przy okazji upewnia się, że ma do czynienia z aktywnym studentem, a także, że nikt niepowołany nie próbował gmerać w układzie stykowym karty.

Blankiety używane jako nośniki ELS są dodatkowo zabezpieczane różnego rodzaju kluczami. Wymienimy tylko niektóre. Każda partia kart jest zabezpieczona tzw. **transportowym kluczem systemowym**. Przed wykonaniem na karcie jakiejkolwiek operacji trzeba zdjąć blokadę. Każda uczelnia posługuje się własnym **kluczem macierzystym** – ściśle tajnym kluczem zabezpieczającym karty wydawane przez uczelnię przed zapisem. Ten klucz zna tylko USOS. Każda karta jest jeszcze chroniona unikatowym **kluczem zabezpieczającym** pliki legitymacji studenckiej przed zapisem, stworzonym przez zastosowanie odpowiedniego algorytmu do klucza macierzystego uczelni i numeru seryjnego karty. Osobnymi kluczami chronione są sektory układu bezstykowego.

Dziś ELS najczęściej pełni rolę legitymacji studenckiej, karty bibliotecznej, nośnika karty miejskiej. A w przyszłości? Możliwości jest wiele – może to być karta dostępowa, karta lojalnościowa, karta do realizacji mikropłatności, nośnik kwalifikowanego podpisu cyfrowego (żeby i student mógł czasem coś cyfrowo podpisać), a potencjalnie dowolnej aplikacji napisanej w Javie.

Java to język programowania często wykorzystywany do pisania aplikacji na karty stykowe czy komórki.

Przykładowo, na UW w niektórych akademikach ELS otwiera drzwi wejściowe do budynku (oczywiście pod warunkiem, że student jest zakwaterowany w tym akademiku). Także bramka w Bibliotece Uniwersyteckiej przepuszcza studentów z ważną ELS.

Do obsługi ELS w USOS-ie powstał specjalny duży moduł. Zlecanie wydruku, sterowanie pracą drukarki, przedłużanie ważności, zapis i odczyt z układu stykowego i bezstykowego, obsługa podpisów cyfrowych – to tylko część realizowanych funkcji. Trzon oprogramowania powstał jako praca magisterska dwóch studentów Wydziału MIM. Zgadnij, Czytelniku, czyje pierwsze dwie legitymacje zostały wydrukowane na UW.

Janina MINCER-DASZKIEWICZ