Norma IEC i ISO umożliwia bezpieczne poświadczanie certyfikatów COVID

Antoinette Price

fot. © Dusko / Adobe Stock

W naszym coraz bardziej cyfrowym świecie musimy udowadniać swoją tożsamość, aby wykonywać wiele codziennych czynności np. uzyskać dostęp do kont bankowych i innych zasobów finansowych, robić zakupy online, fizycznie wejść do budynku, prowadzić pojazd, poddać się operacji, przekroczyć granicę, potwierdzać stan zdrowia.

W niektórych przypadkach musimy podać nazwę użytkownika i hasło, w innych – udowodnić, że jesteśmy tymi, za których się podajemy.

W ramach próby poradzenia sobie z globalną pandemią i przywrócenia normalnego życia wiele rządów wymaga dowodu szczepienia, aby móc uczestniczyć w pewnych wydarzeniach, chodzić do restauracji, i/albo negatywnego wyniku testu, aby wjechać do kraju. Dowód tożsamości ma kluczowe znaczenie dla walidacji świadectwa zdrowia lub potwierdzenia negatywnego wyniku testu.

Więcej niż mobilne prawo jazdy

W wielu krajach prawo jazdy jest powszechnie stosowanym dokumentem prawnym służącym do potwierdzania tożsamości. Wspólny Komitet Techniczny IEC i ISO (JTC 1) opracowuje Normy Międzynarodowe z zakresu technologii informacyjnych. W ramach JTC 1, podkomitet, który opracowuje Normy Międzynarodowe dla kart i urządzeń zabezpieczających do identyfikacji osobistej (SC 17), opublikował ostatnio normę ISO/IEC 18013-5 *Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application*.

„W miarę jak norma ISO/IEC 18013-5 jest przyjmowana na całym świecie jako podstawa dla mobilnych praw jazdy, widzimy również, że ta sama norma jest wykorzystywana do cyfrowych zaświadczeń o szczepieniu zgodnie ze specyfikacjami przedstawionymi przez Światową Organizację Zdrowia (WHO)", powiedział Phil Wennblom, który przewodniczy JTC 1.

Arjan Geluk prowadzi prace nad rozwojem normy i mówi więcej o jej różnorodnych zastosowaniach i potencjale.

Co oferuje norma?

ISO/IEC 18013-5 zapewnia mechanizmy udostępniania danych osobowych i gwarantuje, że osoby, które muszą zobaczyć te dane, mogą im zaufać.

Opisuje specyfikacje interfejsu do implementacji prawa jazdy w urządzeniu mobilnym, innymi słowy interfejs między mDL (mobilnym prawem jazdy – *mobile Driving Licence*) a jego czytnikiem.

Co więcej, podmioty weryfikujące inne niż organy wydające mDL, takie jak policja, służby państwowe, strony internetowe czy aplikacje, systemy dostępu do budynków, mogą zapewnić, że fotografia i dane posiadacza mDL są autentyczne, a co za tym idzie – godne zaufania.

Okoliczności, które obejmuje to m.in.:

- sytuacje, gdy obecna jest osoba, która ma sprawdzić tożsamość posiadacza mDL, np. policja podczas zatrzymania na drodze. Przewidziano również przepisy dla urządzeń połączonych i odłączonych;
- sytuacje bez nadzoru, np. automaty z wyrobami tytoniowymi lub alkoholem, przy użyciu urządzeń podłączonych lub odłączonych.

Technologie przewidziane w normie, które umożliwiają czytnikowi urządzenia mobilnego weryfikację, obejmują optyczny kod QR, komunikację zbliżeniową, Bluetooth low energy oraz Wi-Fi Aware.

Co najmniej 14 krajów, w tym Australia, kilka krajów w Azji, Europie, Ameryce Północnej i Ameryce Łacińskiej, korzysta z mobilnych praw jazdy, a kolejne kraje prowadzą testy.

Jak jeszcze można wykorzystać tę normę?

Rozwój tej normy został zainicjowany w celu udostępnienia prawa jazdy na urządzeniach mobilnych. Podczas prac komitet zdał sobie sprawę, że jest to cyfrowy dokument uwierzytelniający i szkoda byłoby opracowywać protokoły techniczne tylko w jednym celu, wiedząc, że jest wiele cyfrowych dokumentów uwierzytelniających. W związku z tym norma została opracowana tak, aby zawierała ogólne protokoły dla dokumentów mobilnych (*mobile documents* – mdocs) oraz określoną przestrzeń nazw dla mobilnego prawa jazdy.

Ponieważ normę opracowano tak, że protokoły są niezależne od typu dokumentu, komitet został poproszony o zbadanie możliwości wykorzystania tej normy poza prawem jazdy, w dowodach rejestracyjnych pojazdów i w szczególności do zaświadczeń o szczepieniach.

fot. © maramade / Adobe Stock

Podczas niedawnych testów w Rotterdamie, gdzie przeprowadzono 25 prototypowych wdrożeń normy ISO/IEC 18013-5, pokazano różnorodne możliwości tej normy. Uczestnicy przedstawili własne wdrożenia mDL oraz otrzymali przykładowy zestaw danych do dowodu rejestracyjnego i przykładowy zestaw danych dla doctype'u zdefiniowanego jako mobilny międzynarodowy certyfikat szczepień (*mobile international certificate of vaccination* – MICOV).

Nie wprowadzając zmian do protokołów ISO/IEC 18013-5, komitet wyznaczył doctype MICOV i zdefiniował przestrzeń nazw obejmującą elementy danych, które są wspólne dla Europejskiego Cyfrowego Certyfikatu COVID (EU Digital COVID Certificate – EU DCC) oraz cyfrowej dokumentacji certyfikatów COVID-19 w WHO: status szczepienia (DDCC:VS).

Ta norma jest dobrze znana. Jest stosowana przez branżę technologii bezpiecznej identyfikacji, a także przez dostawców nowych aplikacji i usług typu – portfel. Ponadto, Apple i Google przyjęły ją i zapewniają wsparcie na poziomie mobilnego systemu operacyjnego. Apple będzie wspierać mDL w swoim portfelu, zgodnie z ISO/IEC 18013-5, natomiast Android zdefiniował interfejs programowania aplikacji poświadczeń tożsamości, czym wdraża normę ISO/IEC 18013-5

dla mobilnego prawa jazdy i każdego innego rodzaju poświadczenia mobilnego.

Ponadto, Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych wystosował prośbę o informacje (*request for information* – RFI) odnoszące się do normy w celu poinformowania o zbliżającym się procesie legislacyjnym, który dotyczyłby norm bezpieczeństwa i wymagań dla wydawania mobilnych lub cyfrowych praw jazdy. Umożliwiłoby to agencjom federalnym akceptowanie tych dokumentów uwierzytelniających do celów urzędowych, jak określono w rozporządzeniu i ustawie REAL ID Act.

Komisja Europejska również zauważa, że rozwój Europejskiego Portfela Tożsamości Cyfrowej (European Digital Identity Wallet) powinien skorzystać z zapisów tej normy.

Komitet opracował dokument *Guidelines for developing an ISO-compliant mdoc for eHealth*, który objaśnia, w jaki sposób wykorzystać normę dla certyfikatu szczepień.

Czy ta norma obejmuje kwestię poufności danych?

Jedną z kluczowych kwestii dotyczących normy ISO/IEC 18013-5 jest poziom poufności dla posiadaczy mDL zwiększony w porównaniu z fizycznymi kartami przez umożliwienie użytkownikom:

- udostępniania tylko istotnych danych: norma umożliwia minimalizację danych (np. udostępnienie jedynie informacji, że ma się więcej niż 21 lat, zamiast podawanie pełnej daty urodzenia);
- udzielenie zgodny na udostępnienie: mechanizmy kontrolne umożliwiające posiadaczowi mDL udostępnienie tylko niektórych elementów danych wymaganych przez weryfikatora i tylko po uzyskaniu wyraźnej zgody;
- utrzymanie telefonu pod kontrolą: telefon nie jest przekazywany innym, w przeciwieństwie do fizycznych kart;
- uzyskanie informacji, czy ich dane są przechowywane: posiadacz mDL otrzymuje wyraźne powiadomienie, jeżeli weryfikator zamierza zatrzymać jego dane. Weryfikatorzy mogą uniknąć odpowiedzialności za przechowywanie danych;
- odporność na śledzenie. W projekcie uwzględniono mechanizmy zapobiegające śledzeniu.

Jeśli chodzi o wykorzystanie świadectw szczepień, to istotna różnica między EU DCC a opracowanym przez nas jest taka, że w przypadku tego pierwszego istnieje kod QR, który zawiera wszystkie Twoje dane osobowe związane ze szczepieniem. Natomiast w odpowiedniku mobilnym jest kod QR, ale zawiera on tylko informacje do ustanowienia bezpiecznego połączenia. Dzięki temu czytnik mobilny może zażądać konkretnie tego, co jest potrzebne do danego przypadku użycia, a użytkownik zatwierdza tylko udostępnienie danych niezbędnych do tej operacji. Protokół ochrony prywatności opisany w normie nie umożliwia identyfikacji użytkowników, jeśli nie można ich rozpoznać na podstawie przesyłanych danych.

Uważam, że jeśli będziemy potrzebować certyfikatów z bardzo osobistymi danymi przez dłuższy czas, przydatna będzie możliwość udostępniania tylko określonych informacji osobistych, które są wymagane.

Norma wykorzystuje metody szyfrowania i uwierzytelniania wiadomości w celu ochrony przed klonowaniem, podsłuchiwaniem oraz nieautoryzowanym dostępem. W ten sposób zachowana jest poufność, integralność i autentyczność wymiany danych pomiędzy mDL a czytnikiem.

Tłum. I. P.
IEC e-tech, Issue 06/2021