Gliwice, 16 maja 2017

UWAGI DO PRZEDSTAWIONYCH PRZEZ ZUS ALTERNATYWNYCH METOD PODPISYWANIA OŚWIADCZENIA LEKARZA ORAZ DOKUMENTÓW eZLA,AZLA,FZLA,ZLA_K

Niniejsze uwagi powstały na bazie prezentacji przedstawionej 28 kwietnia 2017 roku w Centrali ZUS i informacji przekazanej przez przedstawicieli ZUS. Należy zauważyć że informacje te nie były wyczerpujące, szczególnie w odniesieniu do drugiej z przedstawionych metod alternatywnych podpisywania dokumentów.

Uwagi do metody 1 polegającej na wygenerowaniu przez ZUS (lub inne Centrum Authority któremu ZUS zleci tą czynność) par kluczy (kryptografia asymetryczna- prawdopodobnie RSA) i certyfikatu potwierdzającego związek podpisującego z konkretnym kluczem prywatnym, a następnie przekazaniu klucza prywatnego do uprawnionego lekarza.

Przede wszystkim należy zwrócić uwagę że przekazanie klucza prywatnego do 145 tysięcy uprawnionych lekarzy jest bardzo dużym wyzwaniem, gdyż klucz ten może być przekazany tylko bardzo dobrze zabezpieczonym kanałem. Jeśli nawet pomyślnie uda się rozwiązać ten problem to kolejnym wyzwaniem jest fakt że komputery lekarzy (o ile w ogóle go posiada, bardzo często nie ma ich w POZ-tach poza recepcją) są środowiskiem niecertyfikowanym, o niemożliwym do zweryfikowania poziomie bezpieczeństwa. Z dużą pewnością można przyjąć że bez większego problemu uda się pozyskać przez ulokowango w tym środowisku exploita znaczącą liczbę kluczy wraz z hasłami (lub PIN-ami) służącymi do potwierdzenia woli złożenia podpisu elektronicznego. Tak pozyskane klucze mogą posłużyć do zorganizowanego ataku typu DDoS na usługą ZUS polegającego na seryjnym przesyłaniu fikcyjnych zwolnień (ale z poprawnym składniowo PESEL-em) aż do zablokowania możliwości korzystania z systemu przez lekarzy którzy chcą przesłać autentyczne zwolnienie. Mniejszym zagrożeniem jest możliwość wygenerowanie autentycznego zwolnienia dla osoby która się o nie ubiegała. Przypadki takie mogą być wyjaśniane indywidualnie.

Tak więc największym zagrożeniem jest słabo zabezpieczone środowisko do składania podpisu elektronicznego i trudność w bezpiecznym przekazaniu klucza prywatnego do każdego z lekarzy. Niezależnie od powyższego należy zwrócić uwagę na fakt wskazany przez przedstawicieli Porozumienia Zielonogórskiego, to jest brak sprzętu komputerowego w małych POZ-tach, szczególnie w terenie pozamiejskim.

Uwagi do **metody drugiej** polegającej na wykorzystaniu smartfonów z użyciem numeru seryjnego telefonu komórkowego IMEI i numeru telefonicznego (i/lub karty SIM).

W trakcie spotkania nie wyjaśniono co oznacza użyty w prezentacji termin „podpisywanie" z użyciem aplikacji mobilnej pobranej ze strony ZUS i zainstalowaniem lokalnie na smartfonie. W szczególności brak informacji czy faktycznie ma mieć miejsce użycie klucza prywatnego stanowiącego niezbędny komponent do wyliczenia podpisu (z dokumentu lub jego funkcji skrótu), czy też chodzi o wysłanie unikalnego tokenu z konkretnego urządzenia które uwierzytelniło się dwuskładnikowo z użyciem numeru seryjnego telefonu IMEI i numeru abonenta przy użyciu bezpiecznego kanału informacji (wymóg obligatoryjny ochrony danych służących do uwierzytelnienia). Z opisu metody i samej prezentacji wynika że do formularza umieszczonego na portalu ZUS należy wpisać otrzymany SMS-em kod wysłany na

uwierzytelnione urządzenie przez ZUS, czyli metoda jest analogiczna do stosowanej przez ePUAP.

Ograniczeniem stosowania tej metody może być brak powszechnego posiadania urządzeń mobilnych przez lekarzy i pokrycie zasięgiem sieci komórkowej całego obszaru Polski gdzie znajdują się placówki POZ-ów, co zresztą sygnalizował przedstawiciel Porozumienia Zielonogórskiego. Metoda ta jest jednak znacznie bezpieczniejsza od opisanej poprzednio, choć należy zwrócić uwagę że na urządzeniach mobilnych mogą być zainstalowane różne wersje systemu operacyjnego, w przeważającej ilości jest to system Android. Ostatnie analizy wskazują że wersje poniżej 6.1 są podatne na atak , a z całą pewnością nie uda się wykluczyć z użycia przez lekarzy starszych wersji systemu. Jednak w całościowej ocenie bezpieczeństwa druga metoda (z zastrzeżeniem braku szczegółowej wiedzy na temat jej komponentów i działania) wydaje się bezpieczniejsza i nie naraża tym samym na prosty do skonstruowania atak na usługę.

Opinię sporządził:

Marek Ujejski

CISM

Ekspert STORM