STANOWISKO

Polskiej Izby Informatyki i Telekomunikacji [PIIT]

wobec projektu Rozporządzenia Ministra Cyfryzacji

w sprawie profilu zaufanego i podpisu zaufanego

z dnia 12 lipca 2018

Polska Izba Informatyki i Telekomunikacji (dalej: PIIT, Izba) nieustannie wspiera wszelkie inicjatywy służące rozwojowi bezpiecznych narzędzi do komunikacji, w tym różnorodnych mechanizmów uwierzytelniania oraz podpisów elektronicznych służących wymianie dokumentów we wszelkich relacjach: obywatel, administracja, przedsiębiorca.

W powyższym kontekście z uwagą obserwujemy rozwój Profilu Zaufanego, dlatego też poniżej przedstawiamy kilka uwag do rozporządzenia Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego.

Wydanie przez Ministra Cyfryzacji przedmiotowego aktu wykonawczego wynika ze zmian wprowadzonych ustawą z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw. Jedną z tych zmian jest dodanie w ustawie o informatyzacji nowego art. 20d , który zobowiązuje Ministra ds. informatyzacji do wydania rozporządzenia, regulującego wydawanie, przedłużanie ważności, wykorzystywanie i unieważnianie profilu zaufanego oraz składanie podpisu zaufanego. Rozporządzenie to jest więc jedną z istotnych podstaw regulujących mechanizmy i czynniki uwierzytelniania, które mogą być wykorzystywane dla Profilu Zaufanego.

W związku z tym warto zwrócić uwagę na następujące zapisy § 8 ust. 5-7, tym bardziej, że wskazano tu nieprawidłowe odwołania pomiędzy poszczególnymi przepisami, co w praktyce może prowadzić do komplikacji w stosowaniu różnych mechanizmów autoryzacji.

- **Uwagi do § 8 ust. 5**

W § 8 ust. 5 proponujemy wprowadzić następujące zmiany:

„5. Uwierzytelnienie przy użyciu profilu zaufanego może następować również :

1) z wykorzystaniem czynników uwierzytelniania, spełniających warunki określone w ust. ~~3~~ 4, wykorzystywanych w ramach środka identyfikacji elektronicznej, o którym mowa w art. 20c ust. 8 ustawy, stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego;

2) wyłącznie przy wykorzystaniu czynnika uwierzytelniania, o którym mowa w ust. ~~3~~ 4 pkt 1, jeżeli przepisy prawa regulujące usługę online dopuszczają możliwość uwierzytelnienia użytkownika tej usługi w sposób zapewniający niski poziom bezpieczeństwa, o którym mowa w art. 8 ust. 2 rozporządzenia 910/2014".

Uzasadnienie:

Ust. 5 powinien być regulacją uzupełniającą do zasady z ust. 4, czyli podstawą jest uwierzytelnianie dwuczynnikowe, natomiast dopuszczalne w niektórych przypadkach i uzupełniające jest rozwiązanie wskazane w ust. 5. Dlatego też proponujemy podkreślić to poprzez dodanie w zdaniu wprowadzającym słowa „również". Ponadto odwołania w pkt. 1) i 2) powinny odnosić się do ust. 4 w § 8, gdzie wskazano rodzaje czynników uwierzytelnienia, a nie do ust. 3 § 8, w którym jest mowa o sposobach potwierdzania profilu i zawartości informacji z tym związanych.

- **Uwagi do § 8 ust. 6**

W § 8 ust. 6 proponujemy wprowadzić następujące zmiany:

„6. W przypadku usług online, wymagających uwierzytelnienia użytkownika profilem zaufanym, autoryzacje wymagane w tych usługach dokonywane są przy użyciu drugiego czynnika uwierzytelnienia, o którym mowa w ust. ~~3~~ 4 pkt 2, z uwzględnieniem czynników uwierzytelniania, o których mowa w ust. 4 pkt 1, ~~spełniających warunki określone w ust. 3 pkt 2.~~ ~~„~~

Uzasadnienie:

Odesłanie w ramach § 8powinno odnosić się do tzw. drugiego czynnika, a więc do ust. 4 ust. 2, a nie ust. 3 pkt. 2, w którym jest mowa o sposobach potwierdzania profilu i zawartości informacji z tym związanych. Ponadto proponujemy wykreślenie ostatniej części zdania tj. *„spełniających warunki określone w ust. 3 pkt 2”.* To odesłanie wydaje się również nieprawidłowe, gdyż odnosi się tylko do PZ potwierdzonego przy wykorzystaniu kwalifikowanego podpisu elektronicznego, a chyba nie o to chodziło w tym zapisie. Jeśli dobrze rozumiemy intencję tego zapisu, to główną kwestią jest zapewnienie drugiego czynnika w usługach online.

- **Uwagi do § 8 ust. 7**

W § 8 ust. 7 proponujemy wprowadzić następujące zmiany:

„7. Posiadacz profilu zaufanego może dokonać zmiany:

1) adresu poczty elektronicznej lub numeru telefonu komórkowego - samodzielnie, w systemie, w którym wydawany jest profil zaufany autoryzując tę czynność w sposób, o którym mowa ust. ~~5~~ 4 pkt.2 , albo w punkcie potwierdzającym profil zaufany;

2) środka identyfikacji elektronicznej lub czynników uwierzytelniania, o których mowa w ust. 4 pkt 1 - samodzielnie w systemie podmiotu niepublicznego;

3) czynników uwierzytelniania - samodzielnie w systemie, w którym wydawany jest profil zaufany albo w systemie teleinformatycznym podmiotu niepublicznego, o ile w systemie tym udostępniono taką możliwość.”

Uzasadnienie:

W ust. 7 pkt. 1) zawarto błędne odesłanie do ust. 5, a nie do ust. 4. Sposoby są bowiem opisane w ust. 4 pkt. 2, a nie w ust. 5. W sytuacji opisanej w tym przepisie należałoby dopuścić autoryzację takiej czynności SMS-em albo innym mechanizmem.

- **Ponadto w przedstawionym projekcie rozporządzenia PIIT pragnie zwrócić uwagę i zaproponować zmianę brzmienia § 8 p. 4. 2) b) na:**

„b) inny czynnik uwierzytelniania wymagający od posiadacza profilu zaufanego wykazania się posiadaniem ustalonej uprzednio rzeczy lub urządzenia niezbędnego dla wykorzystania tego czynnika, przy czym uwierzytelnienie będzie wymagało wprowadzenia hasła do urządzenia, złożonego z ciągu przynajmniej czterech cyfr."

Uzasadnienie:

W dotychczasowym brzmieniu (bez podkreślonej części) możliwe było dokonywanie uwierzytelnienia jedynie w oparciu o wejście w posiadanie (w tym nieuprawnione) urządzenia i wykonanie czynności , która mogła być powszechnie znana albo intuicyjna. Przykładowo w usłudze Mobile Connect możliwe jest potwierdzanie woli dwoma sposobami, do wyboru przez usługodawcę:

a) wykorzystując przycisk na ekranie telefonu „Zgoda" lub „OK" lub podobny („coś co mam"),
b) wprowadzając numer PIN („coś co wiem" – hasło złożone z ciąg minimum czterech cyfr).

Praktycznie pierwszy ze sposobów ma zastosowanie przy czynnościach nie rodzących znacznych skutków prawo – biznesowych i łatwych do anulowania. Natomiast przyjmuje się, że czynności rodzące powstawanie zobowiązań powinny być potwierdzane za pomocą PIN, gdyż zabezpiecza to przed nieuprawnionym, przypadkowym lub mechanicznym użyciem. Ponieważ uwierzytelnienie w Profilu Zaufanym otwiera drogę do składania istotnych oświadczeń i deklaracji oraz dostępu do informacji prywatnych Izba sugeruję zmianę jak powyżej.

Można byłoby również rozważyć, czy we wprowadzeniu do ust. 4 w brzmieniu: *„Uwierzytelnienie z wykorzystaniem profilu zaufanego dokonywane jest w sposób zapewniający średni poziom bezpieczeństwa…"*, nie należałoby zamiast słowa *„średni"* używać słowa *„istotny"*, co wydaje się bardziej właściwe i adekwatne do pojęcia *„substantial"*, choć tu faktycznie wersja oficjalna przedmiotowego rozporządzenia w języku polskim posługuje się już określeniem *„średni"*.