Dzień dobry
W nawiązaniu do rozmowy telefonicznej przesyłam informacje o proponowanym systemie spełniającym wymogi "uwierzytelniania dynamicznego" zdefiniowanego w rozporządzeniu UE1502/2015, który zaproponowałem MC i Januszowi Cieszyńskiemu do wdrożenia lub integracji z mObywatel", ponieważ Ustawa z dnia 26 maja 2023r o aplikacji mObywatel (Dz.U. 2023 poz 1234 stanowi w art. 14 ust 4 "Uwierzytelnienie z wykorzystaniem profilu mObywatel jest dokonywane przy użyciu co najmniej dwóch czynników uwierzytelniania należących do co najmniej dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE."
natomiast Rozporządzenie Wykonawcze Komisji UE1502/2015 w załącznik pkt. 2.3.1. dla poziomu średni i wysoki stanowi: "Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego."
Natomiast "uwierzytelnianie dynamiczne" zostało zdefiniowane w załącznik UE1502/2015 pkt 1 Stosowane definicje, ustanowiło w ppkt. "3) „uwierzytelnianie dynamiczne" oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;"
zatem, proces elektroniczny z użyciem kryptografii zmieniający się z każdym uwierzytelnieniem oznacza po prostu kryptografię z kluczami jednorazowymi natomiast "podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą" ustanwiają, że to strona zaufana kontroluje "swoje dane identyfikacyjne" które zgodnie z Rozporządzeniem UE910/2014 art. 7 ust. d) wydane zostają "w momencie wydania środka identyfikacji elektronicznej w ramach tego systemu;" zatem, żadne SMS - y czy inne wysyłane stronie "zaufanej" celem uwierzytelniania nie spełniają wymogu "uwierzytelniania dynamicznego". Zatem, aplikacja mObywatel zgodnie z wykazem https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-srodka-identyfikacji/rejestr-dostawcow-srodka-identyfikacji-elektronicznej-przylaczonych-do-wezla-krajowego.html
ujawnia dane identyfikacyjne i wymagane jest "uwierzytelninie dynamiczne" a 2FA zapisane w ustawie o mObywatel art. 14 pkt 4 nie spełniające wymogów "uwierzytelninia dynamicznego" jest sprzeczne z Rozporządzeniem i zaleceniami UE1502/2015 - bezspornie, natomiast NASK jak w załącznik Pismo ABW do NASK nie wypowiedziało się w tym zakresie pomimo, że ja zostałem "okradziony" ponieważ usługa wystawiona przez BANK i Telecomy nie spełniała wymagań "uwierzytelninia dynamicznego" i w myśl Roporządzenia Dz.U. 2020 poz 1173 odpowiedzialnośc za "fradu" wynikający z niewłaściwego poziomu bezpieczeństwa usługi uwierzytelniania powinien ponieść wystawca usługi, natomiast USTAWA z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2020 poz 1173) stanowi w art. 21a. pkt. 4. "Uwierzytelnienie użytkownika systemu teleinformatycznego w celu

realizacji usługi online wymaga użycia środka identyfikacji elektronicznej na poziomie bezpieczeństwa określonym przez podmiot świadczący tę usługę." w związku z takim zapisem, podmiot wystawiający usługę może nie spełniać żadnych wymogów w zakresie poziomów bezpieczeństwa wskazanych w UE910/2014 ale również w UE2555/2022, zatem aby wyciągnąć konsekwencje wobec podmiotu wystawiającego usługę lub "Państwo" prosze o sporządzenie opinii o którą zwróciło się do NASK ABW w roku 2023 a pismo w tej sprawie w załączeniu.
Generalnie, interesuje mnie czy NASK jest zainteresowane "współpracą" nad dostosowaniem świadczonych usług oraz szkoleń dla e-gov, które zainicjował MC w celu dostosowania poziomów bezpieczeństwa usług w tym usługi/aplikacji mObywatel do spełnienia wymogów "uwierzytelniania dynamicznego" - ponieważ ja jako jedyny na świecie właściciel i twórca systemu "DynAuth" zaoferowałem Ministrowi cyfryzacji ... jednakże po zmianie władzy nie ma kontynuacji ...
Zatem, jeśli wynika to z braku zainteresowania NASK takimi QuantumResist systemami kryptograficznymi to proszę o opinię stosowanie do pisma ABW.
Nadmieniam, że ENISA zaleca dalsze działania na rzecz kryptografii PostQuantum jak w załączniku ...

Pozdrawiam

i