Society 4.0, czyli e-wybory

28 marca 2023

Society 4.0 przedstawia kolejny element programowy tym razem przyjemny temat głosowania przez internet.

To podstawowy element demokracji bezpośredniej, a patrząc na to co się dzieje w Izraelu czy Francji, temat staje się coraz ważniejszy. Jeśli nie nauczymy się zarządzać samymi sobą, to nie powinniśmy się nazywać społeczeństwem czy narodem. Nauka musi postępować nawet jeśli czasami będziemy żałować swoich decyzji. Jeżeli szybko nie nauczymy się rządzić samymi sobą, to demokracja, szybciej niż nam się wydaje, może się zmienić w plutokrację. Czy zaproponowany system jest trudny? Z pewnością nie jest prosty, ale jest realizowalny. Nikt za nas go nie wdroży, bo niby dlaczego miałby to zrobić?

Na początku zdefiniujmy, jakie warunku musiałyby spełnić takie wybory oraz jak głosowanie powinno wyglądać z punktu widzenia wyborcy. W kolejnym kroku spróbuję zaprojektować tak rozwiązanie, aby te warunki były spełnione. Zachęcam do wspólnej analizy i przekazywania własnych pomysłów.

Warunki, jakie musi spełnić głosowanie

Aby system do głosowania w wyborach można było uznać za poprawny, powinien on dawać gwarancję, iż wybory są:

– niepodważalne – każdy samodzielnie może sprawdzić wyniki,

– tajne – nikt poza głosującym nie może wiedzieć jaki głos oddał głosujący,

– powszechne – każdy, kto chce oddać głos i ma do tego prawo ma taką możliwość.

Od razu trzeba zauważyć, że aby wybory były niepodważalne, nie mogą być całkowicie tajne, gdyż system musi znać głos. W momencie oddawania głosu nie ma jednak konieczności ujawniania tego głosu – nic nie stoi na przeszkodzie, aby taki głos zaszyfrować i odszyfrować wszystkie głosy dopiero po zweryfikowaniu, iż nie doszło do nadużyć, np. nie logowano procesu oddawania głosów w bazie danych czy też innych nadużyć.

Większość obecnych systemów głosownia (np. estoński) nie zapewniają tajności, ale to ogromna bolączka tych systemów, bo nigdy nie wiadomo, w jaki sposób będą wykorzystywali te informacje następcy, którzy będą mieli wgląd w bazę danych w późniejszym czasie, co jest ważne zwłaszcza tam, gdzie od wyniku głosowania może np. zależeć utrzymanie pracy czy nawet w sytuacjach wywierania presji przez rodzinę.

Powszechność oznacza, iż każdy, niezależnie od tego czy jest upośledzony ruchowo, poza miejscem zamieszkania, jeżeli ma prawo oddać głos, to może to zrobić.

Ważne jest, aby nie dochodziło do nadużyć w postaci zmuszenia/oszukania osoby do oddania głosu niezgodnie ze swoją intencją, ale to należy zrobić poza system poprzez weryfikację próbki losowej już po głosowaniu, tym większej im większy był możliwy poziom naruszeń. Doskonale nadaje się do tego MUS oraz metodologia badania sprawozdania finansowego.

Kary za takie przestępstwa powinny być oczywiście bardzo surowe.

Jak takie głosowanie powinno wyglądać dla głosującego?

Głos powinien być możliwy do oddania dwoma sposobami:

– przez aplikację mobilną,

– przez przeglądarkę.

W obu przypadkach po zalogowaniu się do aplikacji mobilnej bądź aplikacji webowej i wybraniu głosowania system powinien wyświetlić formularz dla danych wyborów i następnie po jego zapisaniu poprosić o podanie własnego hasła (jaki jest sens tego hasła, wytłumaczę po następnym śródtytule).

Następnie system poprosi o podpisanie jednego z plików głosu (dokładniej w pkt 3.) swoim podpisem kwalifikowanym/profilem zaufanym/e-dowodem bądź podpisem, który obecnie jeszcze nie funkcjonuje globalnie, a mianowicie kluczem tymczasowym wygenerowanym na podstawie powyższych sposobów autoryzacji (szczegóły o kluczu tymczasowym w pkt 3). Aplikacja wyświetlałaby również tzw. HASH pliku z głosem z prośbą o jego zapisanie.

Następnie głos należy wysłać do systemu centralnego, a po przetworzeniu głosu przez system aplikacja otrzymywałaby UPO (czyli Urzędowe Potwierdzenie Odbioru). Po zakończeniu wyborów i przetworzeniu bazy danych, każdy mógłby sprawdzić, czy jego głos jest w bazie i wystarczyłoby wyszukać w tym celu głos z własnym HASH-em. Po zakończeniu całego procesu wyborów część bazy danych, niezawierającej informacji personalnych, byłaby publikowana – każdy będzie mógł poddać szczegółowej analizie dane głosowanie.

Jak to powinno wyglądać technicznie?

Sama aplikacja webowa i mobilna oraz podpisywanie to część platformy głównej – je omówię w innych artykułach. Skupię się na samym przekazaniu głosu oraz to jak będzie przetwarzany w systemie centralnym.

Po pierwsze głos powinien mieć dwa pliki:

a) plik z samych głosem (jak zagłosowaliśmy) oraz długi losowy

ciąg znaków – część ta powinna być zaszyfrowany globalnym kluczem publicznym przekazanym aplikacji dla danego głosowania oraz zawierać też część niezaszyfrowaną zawierającą dziedzinę głosowania (ważne np. przy wyborach samorządowych, gdzie głosuje się na innych kandydatów w innych obszarach),

b) plik zawierający zaszyfrowany plik a) hasłem znanym tylko głosującemu, który podał podczas oddawania głosu – cały plik powinien być podpisany podpisem kwalifikowanym, profilem zaufanym, e-dowodem lub tymczasowym certyfikatem (nieco więcej o tym ostatnim poniżej).

Oba pliki powinny być przekazane jednocześnie wraz z hasłem użytym do zaszyfrowania pliku.

System sprawdza:

– poprawność podpisu b),

– wyodrębnia z podpisu PESEL,

– sprawdza, czy w b) rzeczywiście jest zaszyfrowany plik a) przekazanym hasłem,

– sprawdza, czy dana osoba jest z obszaru wyborczego wskazanego w a).

Jeśli tak jest, zapisuje pliki, PESEL oraz obszar wyborczy w bazie danych, a hasło jest bezpowrotnie tracone – oczywiście cały proces nie może być logowany w żaden sposób.
System dodatkowo wylicza HASH dla pliku a) dla celu późniejszego wyszukiwania.

Po zapisie wysyłane jest UPO. Po zakończeniu głosowania komisja stwierdza poprawność przeprowadzania głosowania i przekazuje klucz prywatny, który umożliwia odszyfrowanie zapisanych plików a). Po odszyfrowaniu wszystkie głosy, które są formalnie poprawne, byłyby automatycznie zliczane. W praktyce wyniki wyborów byłyby znane po godzinie – czyli po ustaleniu przez komisję poprawności wyborów. Odszyfrowanie

kluczem prywatnym i zliczenie wyników to co najwyżej kilka minut pracy bazy danych.

Takie głosowanie jest tajne. W praktyce nie da się powiązać głosu z głosującym bez znajomości hasła ustalonego przez głosującego. Co ważne jeśli dochodziłoby do naruszeń podczas głosowania i zostałyby one stwierdzone przez komisję, to nieznane byłyby same głosy bez przekazania klucza prywatnego przez komisję, a w takim przypadku klucz nigdy nie powinien być przekazany przez komisję – należałoby go zniszczyć jeśli zostałoby potwierdzone, iż dochodziło do naruszeń.

Głosowanie byłoby niepodważalne

Zaszyfrowanie oraz wyliczenie HASH będzie można wykonać również aplikacjami trzecimi – będą to standardowe algorytmy powszechnie używane, co wykluczy możliwość oszustwa na poziomie aplikacji klienckiej.

Ilość plików a) oraz b) musi być równa, a każdy będzie mógł sprawdzić, czy jego głos znajduje się w bazie najprościej poprzez HASH lub pewniej przez analizę przekazanej bazy danych (choć to drugie raczej dla profesjonalistów).

Nie da się więc dołożyć głosów (wymagałoby to podpisu tej osoby), ich podmienić (głosujący to zweryfikują), czy też usunąć (to oczywiście też zweryfikują głosujący).

Weryfikacja poprzez losową próbkę, jak w MUS, weryfikowałaby czy nie dochodziło do naruszeń pozasystemowych.

Głosowanie byłoby powszechne

Pandemia spowodowała, że już niemal każdy ma dostęp do komórki bądź komputera. Jeśli mimo to byłyby osoby, które takiego dostępu nie mają, należałoby zapewnić możliwość oddania głosu w adekwatny sposób z urządzeń w punktach wyborczych, niemniej jednak należy naciskać, aby wykorzystywać tę alternatywę jako

ostateczność. Oczywiście wszystkie osoby musiałyby założyć co najmniej profil zaufany, ale i tak taki profil powinien już być wymagany.

Aby zapewnić powszechność, należałoby również zapewnić odpowiednią wydajność systemową. Aby to zrobić, należy wprowadzić klucz tymczasowy, który jest kluczem wygenerowanym na podstawie innych kluczy (np. profilu zaufanego) – taki klucz został już wprowadzony w jednym z polskich systemów, a mianowicie KSEF. Klucz taki jest ważny, gdyż umożliwia podpisywanie bez konieczności łączenia się z jakimikolwiek systemami zewnętrznymi co w przypadku, gdy kilkadziesiąt milionów osób będzie chciało oddać swój głos w krótkim czasie, staje się niemal koniecznością. Oczywiście taki klucz będzie należało wygenerować wcześniej, ale spora część społeczeństwa najprawdopodobniej to zrobi.

Wystarczy więc już tylko taki system wdrożyć.

Autorstwo: Sensuit
Źródło: WolneMedia.net