Nr rejestracyjny: 2023/51/I/ST6/02770; Kierownik projektu: prof. dr hab. Mirosław Kutyłowski

IDanon

Portfel tożsamości we wrogim środowisku: prywatność i zaufanie “by-design”

Weryfikacja tożsamości i/lub uprawnień uczestników obrotu cyfrowego jest jednym z kluczowych komponentów niezbędnych do bezpiecznego funkcjonowania cyberprzestrzeni. Co więcej, procedury identyfikacji powinny zapewniać ujawnienie tylko takiej ilości informacji, jaka jest niezbędna dla wykonania określonych czynności przez użytkownika. Wynika to z zasady minimalizacji danych, będącej jednym z podstawowych paradygmatów bezpieczeństwa komputerowego. Jest to również wymaganie wynikające z obowiązujących przepisów prawnych - Rozporządzenia o Ochronie Danych Osobowych (RODO) Parlamentu Europejskiego i Rady Europy.

Z zasady minimalizacji wynika konieczność stosowania narzędzi takich jak certyfikaty atrybutów czy tokeny nadające określone uprawnienia. W pierwszym przypadku, ujawniane są jedynie konkretne atrybuty użytkownika (np. pełnoletniość czy uprawnienia zawodowe), a nie dane identyfikujące osobę fizyczną. W drugim przypadku, nie są nawet ujawniane atrybuty niosące określone uprawnienia lecz bezpośrednio same uprawnienia wynikające z weryfikacji przeprowadzonej przez wystawcę tokena. Ważnym rodzajem są tokeny jednorazowe, obecnie szeroko stosowane jako skuteczny zamiennik dla zawodnych mechanizmów CAPTCHA.

Zasada minimalizacji dotyczy nie tylko końcowego adresata procesów identyfikacji i uwierzytelniania, ale także organizacji wydającej użytkownikom środki umożliwiające przejście przez te procesy. Szczególnie gdy organizacje te mają charakter scentralizowany, może dojść do powstawania w jednym miejscu danych mogących w istotny sposób zdradzać aktywność użytkowników. Skuteczny atak na taką organizację dostarcza nieocenionych informacji i stanowi poważne zagrożenie bezpieczeństwa publicznego.

Europejskie Rozporządzenie eIDAS 2 znajdujące się w końcowej fazie procesu legislacyjnego, podejmuje te kwestie wprowadzając ideę decentralizacji ekosystemu identyfikacji. W koncepcji tej zasadniczą rolę odgrywa Europejski Portfel Tożsamości - urządzenie kontrolowane przez posiadacza tożsamości, kontrolujące procesy identyfikacji i uwierzytelniania, a w szczególności gospodarujące otrzymanymi certyfikatami atrybutów. Tym samym skraca się drogę od źródła atrybutów do ich wykorzystania przez posiadacza.

Rozporządzenie zakreśla jedynie ogólną ideę pozostawiając wolne pole do różnorodnych realizacji. Niestety, realizacja stoi wobec wielu wyzwań o podstawowym charakterze. Z tego względu obecnie realizowane programy pilotażowe skoncentrowane są na zastosowaniach o dosyć zachowawczym charakterze.

Europejski Portfel Tożsamości, tak jak wiele innych rozwiązań kryptograficznych, stoi wobec szeregu krytycznych problemów wymagających pilnego rozwiązania. Przy tak dużej skali zastosowań należy wziąć pod uwagę to, że urządzenia mogą zostać zainfekowane wrogim kodem, zwłaszcza przez ich wytwórcę. Jest to szczególnie groźne w przypadku rozwiązań typu czarna skrzynka. Urządzenia mogą ulegać awariom, a wspierająca infrastruktura może być niedostępna. Na koniec, wskutek braku silnych mechanizmów kontroli dostępu, urządzenie może być wykorzystane przez osoby trzecie.

Celem projektu jest przedstawienie rozwiązań, które uodporniają ekosystem identyfikacji na te zagrożenia. Jednym z paradygmatów jest rozproszenie portfela i wspierających systemów, tak aby niewłaściwe działanie pojedynczych komponentów nie stanowiło o załamaniu się systemu. Jednocześnie zostaną zrealizowane dwa cele: ochrona danych osobowych oraz weryfikowalność procesów przez użytkownika. Mechanizmy te mają zostać zrealizowane w warstwie kryptograficznej, w dużym stopniu niezależnie od warstwy sprzętowej.

Szczególną uwagę poświęcimy zagadnieniom bezpiecznego składania podpisu cyfrowego oraz systemowi tokenów kryptograficznych. W tym ostatnim przypadku zamierzamy zrealizować jednorazowość tokenów bez opierania się o centralny system rejestracji użycia tokenów poprzez przeniesienie odpowiedzialności do bezpiecznych komponentów rozproszonych wśród użytkowników. Fundamentalnym celem jest też uwolnienie procesu wydawania tokenów - tak aby wystawcami mogli być sami użytkownicy, a nie tylko wielkie organizacje jak ma to miejsce obecnie. Oczywiście, zmiana paradygmatu działania wymaga zbudowania efektywnych protokołów kryptograficznych z dowodliwymi własnościami bezpieczeństwa, niezaprzeczalności i ochrony prywatności. Co więcej, rozwiązania te muszą być lekkie w sensie złożoności komunikacyjnej i obliczeniowej, a także przejrzyste z punktu widzenia przeciętnego użytkownika, który może nie zaakceptować zbyt dużej ilości "kryptograficznej magii".