

Czy weryfikacja podpisu elektronicznego musi być kwalifikowaną usługą zaufania?

Nasi Klienci, korzystający z usług weryfikacjapodpisu.pl często pytają o kwalifikowalność bądź niekwalifikowalność usług zaufania w tym weryfikacji podpisu elektronicznego, zatem spieszymy z wyjaśnieniem różnic pomiędzy tymi dwoma pojęciami i ich zastosowaniem. Firma Madkom widnieje w polskim rejestrze dostawców usług zaufania i za pośrednictwem weryfikacjapodpisu.pl świadczy niekwalifikowaną usługę walidacji podpisu elektronicznego. Czy sam fakt niekwalifikowalności usługi zaufania oznacza, że jest ona nieskuteczna? W przypadku walidacji podpisu elektronicznego absolutnie nie. Nie istnieją żadne przepisy prawa, które wymagają korzystania z usług wyłącznie kwalifikowanego dostawcy. Dlatego też Elektroniczne Poświadczenie Weryfikacji (EPW), czyli dokument poświadczający pozytywny lub negatywny wynik weryfikacji z weryfikacjapodpisu.pl może stanowić dowód w sprawach spornych np. w sądzie.

Wybór usługi kwalifikowanej bądź niekwalifikowanej zależy od ważności sprawy oraz rodzaju usługi zaufania, z której korzystamy. W przepisach prawa najczęściej przed usługą składania podpisu elektronicznego stawia się wymóg kwalifikowalności, który dotyczy konkretnych typów spraw – na przykład Kodeks Postępowania Administracyjnego wskazuje, że m.in. postanowienia, zaświadczenia czy decyzje mogą być wydawane w postaci elektronicznej pod warunkiem opatrzenia ich kwalifikowanym podpisem elektronicznym. Zaś by potwierdzić prawidłowość złożonego podpisu (również kwalifikowanego) nie jesteśmy zobligowani do skorzystania z kwalifikowanej usługi walidacji. Składanie podpisu elektronicznego jest jednorazową czynnością, którą po wykonaniu nie można ulepszyć, dlatego w niektórych przypadkach nakłada się obowiązek kwalifikowalności, by zwiększyć pewność i zaufanie do podpisu. Natomiast weryfikacji możemy dokonywać bez ograniczeń korzystając z usług różnych dostawców.

Dobrym zwyczajem jest korzystanie z kilku narzędzi do walidacji podpisu elektronicznego w przypadku pojawienia się wątpliwości podczas analizy wyniku weryfikacji. Jednak pozytywna weryfikacja w jednym z narzędzi daje dużą pewność poprawności wyniku, a na pewno nie daje przesłanek do wykluczenia prawdziwości podpisu, a co za tym idzie np. odrzucenia oferty czy wykluczenia wykonawcy w postępowaniu.

Zasady podziału dostawców usług zaufania na kwalifikowanych oraz niekwalifikowanych określa rozporządzenie 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 uchylające dyrektywę 1999/93/WE (eIDAS). Dostawcą usług zaufania jest osoba fizyczna lub prawna, która świadczy przynajmniej jedną usługę zaufania. Zaś kwalifikowana usługa zaufania to główny element umożliwiający realizację transgraniczności transakcji elektronicznych. W przypadku podpisu i pieczęci elektronicznej oraz elektronicznego znacznika czasu, kwalifikowalność tych usług oznacza, że wydane w jednym z państw Unii Europejskiej są uznawane we wszystkich pozostałych krajach członkowskich, ponieważ spełniły uniwersalne warunki określone w rozporządzeniu eIDAS oraz są rozpoznawalne dzięki unijnej liście zaufania (TSL), z której korzysta również weryfikacjapodpisu.pl.

By podpis elektroniczny mógł zostać nazwany kwalifikowanym musi spełniać wytyczne dla zaawansowanego podpisu elektronicznego zawarte w artykule 26 rozporządzenia eIDAS oraz być złożony za pomocą kwalifikowanego urządzenia, którego wymagania są opisane w załączniku II do rozporządzenia i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego mający swoje kryteria zapisane w załączniku I do rozporządzenia. Kwalifikowane usługi zaufania wydawane są przez kwalifikowanych dostawców zweryfikowanych przez organ nadzorujący w danym kraju członkowskim. W Polsce według zapisów ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej organem nadzorującym działania całej Krajowej Infrastruktury Zaufania jest minister właściwy do spraw informatyzacji. Krajowa Infrastruktura Zaufania składa się z rejestru dostawców usług zaufania, listy zaufanej oraz Narodowego Centrum Certyfikacji (NCCERT).

Rejestr dostawców usług zaufania jest jawny i znajdują się w nim dostawcy oraz świadczone przez nich usługi zaufania. Rejestr dzieli się na usługi kwalifikowane oraz niekwalifikowane. By zostać wpisanym na listę kwalifikowanych dostawców należy przejść audyt w celu zweryfikowania oceny zgodności z rozporządzeniem eIDAS. Audyt realizowany jest przez jednostki oceny zgodności, które dostępne są <https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation>. Usługa kosztuje w okolicach 15-25 tysięcy euro i kończy się otrzymaniem raportu z oceny zgodności.

Organ nadzoru stosuje działania nadzorcze ex ante oraz ex post w stosunku do kwalifikowanych dostawców usług zaufania. Zaś w przypadku niekwalifikowanych dostawców są to reaktywne działania nadzorcze ex post, zazwyczaj realizowane na zgłoszenie. Kwestię wyróżniającą dostawców kwalifikowanych jest obowiązek ubezpieczenia OC, którego minimalna suma gwarancyjna w odniesieniu do jednego zdarzenia wynosi 250 000 euro zgodnie z Rozporządzeniem ministra rozwoju i finansów z dnia 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania. Dodatkowo, w przypadku kwalifikowanego dostawcy usług zaufania istnieje zasada domniemywania zamiaru lub zaniedbania. Oznacza to, że po stronie kwalifikowanego dostawcy leży ciężar udowodnienia, że dana szkoda nie powstała z powodu zamierzonego działania bądź zaniedbania. Odwrotnie jest z niekwalifikowanym dostawcą usług zaufania, to strona zgłaszająca musi udowodnić zamiar lub zaniedbanie.

Zaleceniem zapewniającym wysoką jakość funkcjonowania kwalifikowanych dostawców usług zaufania jest współpraca pomiędzy organem nadzorującym, a organem ochrony danych osobowych w postaci wymiany informacji o ewentualnych naruszeniach wynikających z przeprowadzonego audytu w zakresie ochrony danych osobowych. Istotnym jest, by wszystkie kraje członkowskie stosowały porównywalne procedury dotyczące nadzoru nad dostawcami usług zaufania w postaci np. przeprowadzanych audytów. Rozporządzenie eIDAS zaleca wymianę informacji i dzielenie się dobrymi praktykami pomiędzy organami nadzorującymi.