STANOWISKO
Polskiej Izby Informatyki i telekomunikacji [PIIT]

w zakresie uznania przez Krajową Izbę Odwoławczą nieważności kwalifikowanego podpisu elektronicznego z uwagi na użycie skrótu SHA-1

W wyroku z dnia 10 grudnia 2018 r. Krajowa Izba Odwoławcza (dalej: „KIO" lub „Izba") uznała nieważność kwalifikowanego podpisu elektronicznego złożonego na dokumencie JEDZ (Jednolity Europejski Dokument Zamówienia) z uwagi na użycie skrótu SHA-1. W konsekwencji tego orzeczenia, jeżeli ta linia orzecznicza się utrzyma, za nieważne i podlegające odrzuceniu będą uznawane oferty podpisane przy użyciu algorytmu SHA-1. Niestety takie wyroki już w KIO zapadają. Poniżej przedstawiamy argumentację, z której wynika, że KIO pomyliła się w swej ocenie. Brak jest podstaw do uznania, że kwalifikowany podpis elektroniczny jest nieważny z uwagi na posłużenie się takim czy innym algorytmem SHA.

1. Wyrok KIO 2428/18

   W stanie faktycznym sprawy, wykonawca podpisał JEDZ z wykorzystywaniem algorytmu SHA-1. KIO uznała taki podpis za nieważny. Poniżej znajdują się fragmenty uzasadnienia.

   „Zgodnie z ww. art. 137 ust. 1 UsłZaufU, z dniem 1.7.2018 r. skończył się okres stosowania funkcji skrótu SHA-1 w zastosowaniach dotyczących zaawansowanego podpisu elektronicznego i pieczęci. Obowiązek zaprzestania stosowania SHA-1 dotyczy nie tylko certyfikatów (czyli nie dotyczy tylko dostawców certyfikatów), ale także wszelkich składanych podpisów i pieczęci pod dokumentami. Ten obowiązek dotyczy wszystkich podmiotów zarówno komercyjnych, jak i jednostek administracji publicznej, które w ramach swoich systemów udostępniają funkcjonalność tworzenia podpisu (lub pieczęci). Wymaga podkreślenia, że jeżeli certyfikat użytkownika będzie bazował na SHA-1 (i będzie ważny, bo wydany przed 1.7.2018 r.), to podpis tworzony (po 1.7.2018 r.) weryfikowany tym certyfikatem powinien zawierać skrót podpisywanej treści obliczony algorytmem SHA-2 (a nie SHA-1)".

   „Powyższe stanowisko potwierdza również komunikat Ministra Cyfryzacji z 1.3.2018 r. w sprawie wycofania algorytmu SHA-1 w zastosowaniach związanych z zaawansowanym podpisem i pieczęcią elektroniczną, zamieszczony na stronach Narodowego Centrum Certyfikacji, w którym wskazano, że: „z dniem 1.7.2018 r. kończy się przewidziany w art. 137 ustawy z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 r. poz. 1579 ze zm.) okres stosowania funkcji skrótu SHA1 w zastosowaniach dotyczących zaawansowanego podpisu elektronicznego i pieczęci. Przepis wymaga odejścia od stosowania algorytmu SHA-1 przy składaniu zaawansowanego, w tym również kwalifikowanego, podpisu elektronicznego i pieczęci elektronicznej, co jednak powoduje konieczność uprzedniego dostosowania aplikacji służących do składania lub weryfikacji podpisu elektronicznego do algorytmów rodziny SHA-2. Algorytm SHA-1 utracił rekomendację ETSI (zob. ETSl TS 119 312). Decyzją Ministra Cyfryzacji, w ramach Narodowego Centrum Certyfikacji, uruchomiony został nowy urząd certyfikacji, który umożliwia centrom świadczenie usług na nowych algorytmach. Niezbędne jest jednak

dostosowanie wszystkich systemów strony ufającej, tak aby z dniem 1.7.2018 r. było możliwe odejście od stosowania funkcji SHA-1 przy składaniu podpisu elektronicznego i pieczęci elektronicznej. Algorytm SHA-1 będzie mógł być nadal używany przy weryfikacji. Należy jednak zauważyć, że listy CRL publikowane po 1.7.2018 r. podpisywane będą z użyciem funkcji z rodziny SHA-2 (nawet jeśli dotyczą certyfikatów wydanych z użyciem funkcji SHA-1). W odniesieniu do ważnych dokumentów podpisanych na podstawie starych algorytmów dobrą praktyką jest znakowanie czasem z użyciem znaczników opartych na nowych algorytmach".

„Biorąc pod rozwagę powyższe, KIO stwierdziła, że wykonawca H. nie dochował należytej staranności przy dokonywaniu czynności związanej ze złożeniem kwalifikowanego podpisu pod dokumentem JEDZ składanym zamawiającemu, albowiem uchybił bezwzględnie obowiązującym od 1.7.2018 r. przepisom i wadliwie złożył podpis przy zastosowaniu algorytmu SHA-1. Wykonawca powinien bowiem, znając treść przepisów nowelizujących UsłZaufU, dokonać uprzedniego dostosowania aplikacji służących do składania lub weryfikacji podpisu elektronicznego do algorytmów rodziny SHA-2. Przystępujący takiej czynności nie dokonał. Tym samym KIO doszła do przekonania, że podpis złożony przez wykonawcę H., nie odpowiadający aktualnie obowiązującym przepisom, jest nieważny, dlatego też konieczne było ustalenie, że czynność oceny oferty wykonawcy przez zamawiającego pod kątem prawidłowości złożonego pod oświadczeniem JEDZ podpisu była wadliwa".

2. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2016.1579).

   Jak wynika z wyroku KIO 2428/18, Izba oparła się w swym rozstrzygnięciu na przepisie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (dalej: „UZIE"). Powołano się również na komunikat Ministerstwa Cyfryzacji z dnia 1 marca 2018 r. (dalej: „Komunikat MC").

   Wymaga wskazania, że ustawa UZIE reguluje sposób stosowania 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 (Dz. Urz. UE L 257 z 28.08.2014, str. 73) – dalej: „Rozporządzenie 910/2014 lub eIDEAS". Rozporządzenie 910/2014 jako takie obowiązuje bezpośrednio, nie wymaga się jego implementacji do polskiego porządku prawnego. Zatem ustawa UZIE normuje tylko wybrane aspekty związane z usługami zaufania; pozostałe uregulowania obowiązują zgodnie z treścią Rozporządzenia eIDEAS. Prowadzi to do pierwszego wniosku, że ustawa nie może być z Rozporządzeniem 910/2014 sprzeczna.

   Izba wskazała na przepis art. 137 ustawy UZIE:

   1. Do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych można stosować funkcję skrótu SHA-1, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu.

2. Dostawcy usług zaufania, producenci oprogramowania oraz podmioty publiczne obowiązani są do odpowiedniego dostosowania oprogramowania oraz systemów teleinformatycznych do zmian i terminu określonych w ust. 1.

Wymaga podkreślenia, że z treści art. 137 wynika, że miał on inny cel niż przyjęła KIO w wyroku. W treści ust. 1 wprost wskazano, że skrót SHA-1 może być stosowany do dnia 1 lipca 2018 r., chyba że wymagania techniczne wynikające z aktów wykonawczych do Rozporządzenia 910/2014 wyłączą taką możliwość. **Zatem przepis miał na celu uspokoić rynek w Polsce, że skrót SHA-1 do dnia 1 lipca 2018 r. może być stosowany**. W przeciwnym razie mogłaby pojawić się niepewność co do możliwości stosowania tego skrótu. **Przepis nie zawiera w swej treści zakazu posługiwania się skrótem SHA-1, tym bardziej nie przewidziano jakichkolwiek sankcji np. w postaci podważenia ważności podpisu**. Co więcej, z ust. 2 wynika, że p**rzepis ten kierowany jest to specyficznej kategorii podmiotów tj: dostawców usług zaufania, producentów oprogramowania oraz podmiotów publicznych**. Te kategorie podmiotów zobowiązane zostały do odpowiedniego dostosowania oprogramowania oraz systemów teleinformatycznych. Zatem przykładowo, zamawiający publiczny podpisując dokumenty elektronicznie nie powinien się takim skrótem posługiwać. **Nie wynika z tego przepisu jednak, aby przedsiębiorca – składający ofertę w postępowaniu o udzielenie zamówienia publicznego – nie mógł się posłużyć skrótem SHA-1. Jest tak dlatego, że podpis elektroniczny złożony z zastosowaniem skrótu SHA-1 w dalszym ciągu pozostaje ważny**. Przepis art. 137 UZIE tego statusu nie podważa. Nawet zaprzestanie używania skrótu SHA-1 przez podmioty publiczne nie oznacza, że zamawiający może nie uznawać podpisów elektronicznych utworzonych przy zastosowaniu SHA-1 przez wykonawców. Brak jest takiej sankcji, i brak jest obecnie podstaw do jej wprowadzenia bądź wyinterpretowania.

Należy wskazać na treść uzasadnienia do projektu ustawy UZIE, który potwierdza słuszność powyższego wywodu: „*Ważnym przepisem dla zapewnienia ciągłości usług zaufania w Polsce jest art. 137, wskazujący na **możliwość stosowania skrótu SHA-1** do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych. Dotychczasowe przepisy wymagały wprost stosowania tego algorytmu, co spowodowało, że oprogramowanie stosowane do składania i weryfikacji podpisów, nie było dostosowywane do innych skrótów rekomendowanych w standardzie ETSI TS 119 312 dotyczącej wymagań w zakresie stosowania algorytmów kryptograficznych w infrastrukturze podpisu elektronicznego. **Mając na uwadze, że norma ta wprost nie rekomenduje dalszego używania skrótu SHA-1 ze względu na możliwe naruszenia bezpieczeństwa, należało wprowadzić przepisy przejściowe umożliwiające stopniowe odejście od stosowania tego skrótu.** Nie można było jednak wprost zrezygnować ze wskazywania algorytmu technicznego w przepisach prawa, opierając się jedynie na normach, ponieważ zgodnie z normą ETSI EN 319 412-2 dotyczącą profili certyfikatów wydawanych osobom fizycznym, stosowanie wymagań określonych w standardzie ETSI TS 119 312 może być zastąpione krajowymi zaleceniami*”.

W uzasadnieniu wyraźnie zaznaczono, że przepis art. 137 wskazuje na „możliwość stosowania skrótu SHA-1” – możliwość jest odwrotnością jakiegokolwiek ograniczenia czy zakazu. Dalej w uzasadnieniu podkreślono, że norma ETSI TS 119 312 (ETSI - Europejski Instytut Norm Telekomunikacyjnych) „*wprost nie rekomenduje dalszego używania skrótu SHA-1 ze względu na możliwe naruszenia bezpieczeństwa [i] należało wprowadzić przepisy przejściowe umożliwiające stopniowe odejście od stosowania tego skrótu*”.

Zatem wyraźnie z powyższego wynika, że norma **ETSI co prawda „nie rekomenduje dalszego używania skrótu SHA-1" ale z jej treści, względnie z treści przepisów prawa wspólnotowego (jak również krajowego polskiego) nie wynika jakikolwiek zakaz, tym bardziej obwarowany sankcją uznania takiego podpisu za nie posiadający przymiotów kwalifikowanego podpisu elektronicznego**. Jest to zatem w najlepszym razie lex imperfecta – czyli norma, za której nie wykonanie nie grożą żadne sankcje.

Należy dodać, że w opinii specjalistów, obecnie nie jest realnie prawdopodobna ingerencja w podpisany skrótem SHA-a dokument, a tym samym nie ma zagrożenia ingerencji w treść dokumentu. Rekomendacje ETSI mają w tym zakresie charakter działania na przyszłość. Innymi słowy, wskazuje się jako pożądane stopniowe odchodzenie od SHA-1, jednakże w żaden sposób się tego nie zakazuje.

Komunikat MC również nie zawiera wprost wskazań, na podstawie których można by uznać, że oferta (czy JEDZ) podpisane podpisem kwalifikowanym z użyciem skrótu SHA-1 będą uznawane za nieważne. Wydźwięk komunikatu wskazuje bardziej na zalecenia i rekomendowane działania. Trzeba jednocześnie przyznać, że Komunikat nie jest jednoznaczny. Z pewnością jednak nie ma w nim słowa na temat sankcji za niezastosowanie się do Komunikatu i/lub art. 137 UZIE. Świadczy o tym przykładowo zwrot: „*Warto rozważyć wycofanie SHA-1 również z innych zastosowań, chociaż mogą wystąpić i takie rozwiązania informatyczne, gdzie nie jest to możliwe lub konieczne (np. HMAC)*". Innymi słowy, MC w treści komunikatu przyznaje, że wycofanie się z SHA-1 może okazać się niemożliwe.

Jedyny zapis z komunikatu, który można uznać za wskazówki dla podmiotów publicznych (zamawiających) w zakresie zarządzania postępowaniami o udzielenie zamówienia znajduje się na końcu i stanowi: „*W przypadku urzędów administracji publicznej, oprócz dostosowania systemów informatycznych, zalecane jest dokonanie przeglądu przepisów prawa lub dokumentacji projektów tak, aby usunąć zapisy przewidujące stosowanie SHA-1 jako funkcji skrótu".* Zatem można by ewentualnie rozważać nieważność podpisu z użyciem SHA-1 pod ofertą/JEDZ, gdyby zamawiający wprost to wykluczył w SIWZ zaznaczając, że odrzuci taką ofertę. Jednakże nawet w takiej sytuacji byłoby to co najmniej wątpliwe, gdyż Zamawiający (analogicznie jak KIO) nie ma prawa samodzielnie decydować czy podpis elektroniczny jest ważny, skoro w świetle przepisów prawa, nie można zidentyfikować wprost normy prawnej pozwalającą mu taką okoliczność stwierdzić. Kiedy mamy do czynienia z podpisem elektronicznym wynika przede wszystkim z Rozporządzenia 910/2014.

3. Rozporządzenie 910/2014 (tzw. eIDAS)

Zgodnie z treścią Rozporządzenia 910/2014 "kwalifikowany podpis elektroniczny" oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Sposób składania podpisu elektronicznego, poziom bezpieczeństwa jaki musi być zachowany wynikają z dalszych części Rozporządzenia, w tym załącznika II. Istotne są przy tym również inne przepisy rozporządzenia.

Nie przytaczając treści przepisów w tym miejscu należy poczynić generalną uwagę, że **nie wynika z nich (ani z innych przepisów prawa wspólnotowego) aby kwalifikowany podpis elektroniczny przestał nim być z uwagi na zastosowanie skrótu SHA-1**. Skoro zatem przykładowo art. 27 ust. 2 Rozporządzenia 910/2014 stanowi, iż *państwo członkowskie uznaje zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane podpisy elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust.* 5", to należy z tego wnioskować, że **tak długo jak podpis spełnia przesłanki z Rozporządzenia 910/2014 nie można mu odmówić ważności**.

Zamawiający mają prawo weryfikować ważność podpisów, ale w oparciu o przepisy art. 32 i 33 Rozporządzenia 910/2014, które dotyczą wymogów dla walidacji kwalifikowanych podpisów elektronicznych. Nie ma tu bezpośredniego związku z funkcją skrótu SHA-1 i faktem, że algorytm ten nie jest rekomendowany. Należy zwrócić uwagę, że przepisy wykonawcze wydane na podstawie Rozporządzenia 910/2014 powołują szereg dokumentów technicznych, które należy uwzględnić w procesie weryfikacji poprawności podpisu elektronicznego. Jeżeli kwalifikowana usługa walidacji potwierdza wiarygodność podpisu to powinien być uznany za prawidłowy. Usługa walidacji – świadczona przez dostawcę kwalifikowanej usługi – musi respektować wszystkie przepisy prawa i wymagania zawarte w wielu dokumentach normatywnych. Poprawność implementacji oraz sposób stosowania prawa i standardów przez dostawcę usług zaufania są kontrolowane przez niezależnych tzw. akredytowanych audytorów. Uzyskanie pozytywnego raportu zgodności wydawanego przez podmiot audytujący jest warunkiem koniecznym, aby krajowy nadzór nad usługami zaufania (w Polsce jest to Ministerstwo Cyfryzacji) uznał usługę danego dostawcy jako usługę kwalifikowaną. **Obecnie skorzystanie z kwalifikowanej usługi walidacji dla dokumentu podpisanego z użyciem SHA-1 (np. przez zamawiającego publicznego) nie może tylko z tego powodu dać wyniku negatywnego, gdyż algorytm SHA-1 nie został nigdzie wprost zabroniony. Skoro tak, to nie może być podstaw do arbitralnego uznania przez KIO (w oderwaniu od procesu walidacji opisanego w Rozporządzeniu 910/2014) czy inny podmiot publiczny nieważności kwalifikowanego podpisu, który prawidłowo przeszedł proces walidacji.**

Należy zaznaczyć, że przepis art. 137 UZIE nie wprowadza dodatkowego wymogu dla procesu walidacji. Po pierwsze, nie przewiduje on sankcji w postaci nieważności lub nieuznawania podpisu utworzonego z zastosowaniem funkcji skrótu SHA-1, a po drugie, wprowadzenie takiego rygoru (nieważności podpisu) w polskim prawie powodowałoby sprzeczność z Rozporządzeniem 910/2014, które nie przewiduje dla kwalifikowanych, podpisów elektronicznych wytworzonych z wykorzystaniem funkcji skrótu SHA-1 jakichkolwiek negatywnych skutków.

Wymaga szczególnego podkreślenia, że również **dyrektywa 2014/24/UE (dyrektywa klasyczna) – a więc akt prawny odnoszący się wprost do zamówień publicznych – w art. 22 ust. 6 c) ii wskazuje, że jeżeli oferta jest podpisywana z wykorzystaniem kwalifikowanego certyfikatu, który jest umieszczony na zaufanej liście, instytucje zamawiające nie mogą stosować dodatkowych wymogów mogących utrudnić oferentom korzystanie z tych podpisów**. Stwierdzanie nieważności podpisu z uwagi na algorytm SHA-1 jest właśnie takim nieuprawnionym tworzeniem dodatkowych wymogów wobec wykonawców, utrudniającym im składanie ofert w formie elektronicznej.

Warto w tym miejscu przytoczyć również przepis art. art. 78(1) Kodeksu cywilnego, który stanowi, że do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym. Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej. **Zatem tak długo jak podpis spełnia definicję kwalifikowanego podpisu elektronicznego, tak długo dokumenty w ten sposób podpisane są ważne, nawet jeżeli użyto skrótu SHA-1.** Można z tego wyciągnąć wniosek, że na podstawie przepisów powszechnie obowiązujących, w tym z art. 137 UZIE, nie można uznać takiego podpisu za nieważny, jak uczyniła KIO.

Konkludując, algorytm SHA-1 nie jest rekomendowany z punktu widzenia standardów technicznych. Z tego wynika między innymi treść art. 137 UZIE. Dla bezpieczeństwa długookresowego podpisywanych elektronicznie dokumentów ma rzeczywiście znaczenie przy użyciu jakiego algorytmu kryptograficznego podpis został utworzony. Zatem dbałość o najwyższe standardy bezpieczeństwa wskazuje, że należy zaprzestać stosowania SHA-1, zwłaszcza, że art. 137 ustawy UZIE wyraźnie tego wymaga (choć nie od wszystkich i nie przewidując za to sankcji). Nie oznacza to jednak, że zamawiający mają podstawę prawną do odrzucenia ofert składanych przez wykonawców z użyciem SHA-1 i to niezależnie od tego czy podpis był złożony przed czy po 2 lipca 2018 r. Podstawa prawna ku temu nie istnieje, gdyż taki podpis w dalszym ciągu ma charakter kwalifikowany tj. spełniający wymogi ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (ustawa Pzp) wraz z aktami wykonawczymi do niej. Należy przy tym dodać, że obecnie ryzyko naruszenia bezpieczeństwa jest jedynie iluzoryczne. Poziom bezpieczeństwa kryptograficznego jest na tyle wysoki, że przy obecnej wiedzy i możliwościach technicznych algorytm SHA-1 de facto zapewnia bezpieczeństwo prawne i faktyczne podpisowi elektronicznemu w procesie ubiegania się o zamówienie publiczne. Zaniechanie jego rekomendowania wynika z obaw o bezpieczeństwo w przyszłości. Z tego względu **algorytm SHA 1 nie został obecnie wprost zakazany przez żaden przepis wspólnotowy, tym bardziej taki który przewidywałby sankcję nieważności. Zakaz taki w każdym razie nie wynika ani z ustawy Pzp, ustawy UZIE, komunikatu MC, ani z Rozporządzenia 910/2014 czy innych aktów prawnych**. Prowadzi to do wniosku, że KIO pomyliła się wydając orzeczenie w sprawie o sygnaturze KIO 2428/18.

Na zakończenie warto dodać, że w tej sprawie powinien wypowiedzieć się Prezes Urzędu Zamówień Publicznych lub Ministerstwo Cyfryzacji.