

Jak zapewnić autentyczność i integralność faktury elektronicznej?

<http://ipsec.pl/faktura-elektroniczna-e-faktura/2011/jak-zapewnic-autentycznosc-integralnosc-faktury-elektron>

Zgodnie z obowiązującym od stycznia 2011 rozporządzeniem o fakturach elektronicznych autentyczność i integralność można zapewnić za pomocą innych środków niż EDI i podpis kwalifikowanych. Czyli jakich?

Środkiem technicznym wprowadzonym w celu ochrony autentyczności i integralności dokumentów elektronicznych jest podpis elektroniczny. Rozporządzenie obowiązujące do 2011 roku dopuszczało stosowanie tylko jego najsilniejszej wersji – podpisu kwalifikowanego. Jego nieprzydatność do fakturowania elektronicznego wynikała z następujących cech:

Przywiązanie do osoby fizycznej, podczas gdy w przypadku faktury wystarczająca jest ochrona z dokładnością do firmy, czyli organizacji. Nie da się uzyskać certyfikatu kwalifikowanego na firmę, więc w praktyce podpis musiała składać jedna wyznaczona osoba. Jej nieobecność wymagała w teorii posiadania zapasowych certyfikatów dla innych osób, a w praktyce była rozwiązywana przez traktowanie jej karty i certyfikatu jako "przechodniego". Jest to oczywiście sprzeczne z idea podpisu kwalifikowanego i prawem.

Konieczność ręcznej autoryzacji podpisu. Podpis kwalifikowany z założenia powinien być składany ręcznie (kod PIN), przez konkretną osobę i na konkretnym dokumencie o znanej treści. Nie da się go osadzić w systemie finansowo-księgowym tak, by podpis pod fakturami był składany w pełni automatycznie. Firmy promujące podpis kwalifikowane nagięły interpretacje ustawy w ten sposób, by możliwe było składanie podpisu kwalifikowanego np. pod porcją 5 tys. faktur po jednorazowym wpisaniu PIN. Nawet jeśli było to zgodne z prawem, to moim zdaniem było niezgodne z założeniami podpisu kwalifikowanego.

Brak możliwości stosowania klasycznego oprogramowania biurowego, typu Excel, Word czy Acrobat. Podpis kwalifikowany wymaga oprogramowania posiadającego "deklarację zgodności". Wymienione programy jej nie posiadają. Posiadają ją jedynie udostępniane przez centra certyfikacji "programy do podpisywania", które są moim zdaniem tragicznie niewygodne, oraz niektóre systemy specjalizowane do wystawiania faktur elektronicznych. W rezultacie mieliśmy sytuacje, w której do fakturowania nie możemy stosować oprogramowania, które logicznie się tutaj narzuca, a musimy stosować oprogramowanie, które się do tego nie nadaje. Prowadziło to do absurdalnych sytuacji, gdy "zgodna z prawem" faktura elektroniczna przychodziła w postaci "gołego" (niepodpisanego wewnątrz) pliku PDF, a podpis był załączony w oddzielnym pliku i weryfikowany oddzielnym programem, którego rzecz jasna nikt nie sprawdzał.

Jak widać, rozwiązanie obowiązujące w latach 2005-2011 było postawione na głowie, wbrew zdrowemu rozsądkowi i w sposób mocno nadmiarowy w stosunku do unijnej dyrektywy o fakturach elektronicznych. Nowelizacja z 2011 roku rozwiązała większość z tych problemów.

Jak to zrobić poprawnie?

Zgodnie z <http://www.mf.gov.pl/dokument.php?const=3dzial=135id=232702> nowym rozporządzeniem faktura elektroniczna musi mieć jedynie zapewnioną autentyczność i integralność. W rozporządzeniu wymienia się dwie techniki {przykładowe, które {na pewno je zapewniają ale katalog jest otwarty. To znaczy wystawca faktur może stosować wszystkie techniki, które zapewniają autentyczność i integralność faktury, ryzykując jedynie to, że jego wybór zostanie zakwestionowany podczas kontroli skarbowej.

Według niektórych dość skrajnych interpretacji autentyczność i integralność zapewni nawet wysłanie "gołego" pliku PDF emailem. Można tutaj budować dialektyczne wywody dlaczego znany adres email zapewnia autentyczność, a protokół TCP – integralność, ale moim zdaniem nie tędy droga. Zwłaszcza, że z nowym rozporządzeniem zrobienie tego zgodnie z zasadami sztuki jest łatwiejsze niż kiedykolwiek przedtem.

Autentyczność i integralność faktury elektronicznej można teraz zapewniać za pomocą podpisu elektronicznego składanego z pomocą zwykłych certyfikatów komercyjnych. Certyfikaty te można uzyskać za darmo (<http://startssl.com/>) lub kupić

za kilkadziesiąt złotych w polskich (jako {certyfikat niekwalifikowany albo {komercyjny) lub zagranicznych centrach certyfikacji (tzw. {email certificate). Te certyfikaty mają następujące zalety jeśli chodzi o podpisywanie faktur elektronicznych:

- Nie są przechowywane na karcie elektronicznej, mogą być przechowywane w systemie Windows lub w magazynie certyfikatów Acrobat, nie muszą być zabezpieczone kodem PIN – podpis może być składany całkowicie automatycznie.
- Mogą być używane w każdym programie biurowym (Excel, Word, OpenOffice, Acrobat) czy pocztowym (Windows LiveMail, Thunderbird).
- Dostępny jest szereg darmowych lub tanih bibliotek pozwalających na automatyzację składania podpisu pod dokumentami (np. <http://www.itextpdf.com/> dla plików PDF).

W tej sytuacji generowanie faktury elektronicznej w małych i średnich firmach ogranicza się do stosowania klasycznych narzędzi biurowych, które w większości posiadają wbudowane funkcje podpisu elektronicznego. Jeśli mamy zainstalowany w systemie "zwykły" certyfikat (ja mam np. od <http://startssl.com/>) to programy takie jak Excel, Word czy OpenOffice będą go widzieć automatycznie i umożliwiać podpisanie nim każdego dokumentu jako części procesu zapisywania jego ostatecznej wersji. I tak funkcje podpisu są w różnych programach dostępne w następujących miejscach:

- **OpenOffice** wersje 2 i nowsze – menu {Plik rarr; Podpisy cyfrowe rarr; Dodaj **Microsoft Office starsze wersje (2002, XP)** – menu {Narzędzia rarr; Opcje rarr; Bezpieczeństwo rarr; Podpisy cyfrowe rarr; Dodaj **Microsoft Office nowsze wersje (2007, 2010)** – menu {Plik rarr; Informacje rarr; Ochrona dokumentu rarr; Dodaj podpis cyfrowy **Adobe Acrobat** – menu {Advanced rarr; Sign & Certify rarr; Certify without visible signature (to najprostszy sposób, w rzeczywistości funkcje te są http://www.securitystandard.pl/news/327774/Podpis_elektroniczne_wiele_bardziej_rozbudowane/)

W załącznikach poniżej można znaleźć wszystkie wymienione formaty plików z podpisem złożonym za pomocą certyfikatu StartSSL. Podpisane pliki można przesłać kontrahentowi już dowolnie – e-mailem. Można również umieścić pliki z fakturami w serwisie takim jak <http://www.wuala.com/referral/NNJ> albo <https://www.dropbox.com/referrals/NTE5MzEwOTE0OQ?src=global9> w katalogach dzielonych z poszczególnymi kontrahentami. Zapewni to po pierwsze łatwość wymiany faktur, po drugie – co bardzo istotne – kopie zapasowe i po trzecie łatwy i szybki dostęp dla urzędu skarbowego w trybie on-line (§7 <http://www.mf.gov.pl/dokument.php?const=3dzial=135id->

Na koniec chciałbym jeszcze zastrzec, że wymienione techniki zapewniają autentyczność i integralność dokumentów elektronicznych na poziomie, który moim zdaniem jest w pełni odpowiedni dla faktur elektronicznych. Nie mogę jednak zagwarantować, że interpretacja ta będzie podzielana przez wszystkie urzędy skarbowe w całym kraju. Co więcej, poruszam tutaj tylko kwestie autentyczności i integralności, nie zajmując się innymi wymaganiami z rozporządzenia (zgoda, udostępnianie itd).

Jeśli planujemy duże wdrożenie faktur elektronicznych to najlepiej po prostu wystąpić o interpretację indywidualną, opisując w jaki sposób faktury elektroniczne są wystawiane i podpisywane.

Wydaje mi się, że przyszłość należy tutaj do oprogramowania finansowo-księgowego, które w końcu może w łatwy i tani sposób dodać funkcje fakturowania elektronicznego, a zwłaszcza do serwisów online (w stylu i-Faktura). Wyposażenie ich w funkcje fakturowania elektronicznego zgodnie z opisanymi powyżej technikami zapewnienia autentyczności i integralności dałoby im ogromną przewagę konkurencyjną.