



Olsztyn 03.09.2019 r.

Organizacja Pracodawców
Branży Fiskalnej
ul. Pstrowskiego 14C lok. G
10-602 Olsztyn

Szanowny Pan
Tadeusz Kościński
Podsekretarz Stanu
Ministerstwo Finansów

Szanowny Pan
Tomasz Robaczyński
Podsekretarz Stanu
Ministerstwo Finansów

Dotyczy pisma nr: PT7.8100.1.8.2019

Szanowni Panowie,

W związku z prowadzonymi konsultacjami publicznymi rozporządzenia Ministra Finansów w sprawie kas rejestrujących mających postać oprogramowania z dnia 6 sierpnia 2019 r. przesyłamy nasze uwagi, skupiając się głównie na aspektach związanych z możliwością rozszczelnienia systemu poboru podatku VAT oraz możliwym pozbawieniem uczciwych podatników poczucia bezpieczeństwa.

Aktualnie stosowane rozwiązanie sprzętowych kas rejestrujących, rozwijane przez Ministerstwo Finansów od ponad 25 lat jest stabilne i bezpieczne dla budżetu Polski. Zapewnia szczelność systemu ściągania podatku VAT oraz jest bezpieczne dla uczciwych podatników chcących rzetelnie rozliczać się z naliczonych podatków podczas prowadzenia działalności gospodarczej.

Tak zbudowany system, oparty o prawidłowo działające urządzenia, homologowane w Głównym Urzędzie Miar, wraz ze skuteczną siecią serwisową dostępną na terenie całego kraju, daje poczucie bezpieczeństwa głównie mikro, małym i średnim przedsiębiorstwom. Podmioty te stać na zapewnienie sobie bezpieczeństwa serwisowego, a wypracowana przez lata forma opieki odpowiada ich potrzebom.

Obecne rozwiązanie dopracowane przez ostatnie 25 lat zapewnia **prawdziwość i niezmiennność danych zapisanych w pamięci fiskalnej**, zarówno dla podatnika jak i kontrolującego go organu podatkowego. Do niedawna obszarem, który można nazwać niedostatecznie szczelnym, była możliwość całkowitego niezarejestrowania transakcji na kasie fiskalnej.

str. 1



Celem umożliwienia przeprowadzania bardziej skutecznych kontroli potencjalnie nieuczciwych podatników, zostały wprowadzone w życie od 1 maja 2019 r. sprzętowe kasy rejestrujące on-line. Łączą one cechy poprzednich rozwiązań, czyli niezmiennosć i trwałość przechowywanych danych w pamięci fiskalnej z wysyłaniem zapisanych danych do Centralnego Repozytorium Kas. To rozwiązanie bardzo ułatwi przeprowadzanie celowanych kontroli i zwiększy nadzór nad rejestracją sprzedaży.

Powyższe rozwiązanie stosowane od maja 2019 r. jest **jednym z najbardziej bezpiecznych na świecie, zarówno dla systemu poboru podatku VAT, jak i bezpieczeństwa podatników.**

Wprowadzenie do systemu ewidencji podatku VAT nowego rozwiązania, opartego o kasy rejestrujące mające postać oprogramowania, tzw. „kas wirtualnych” doprowadzi do sytuacji, że cała wcześniejsza praca Ministerstwa Finansów uszczelniająca wpływy z podatku VAT w obszarze handlu i usług zostanie zniweczona, a rozwiązanie w projektowanym kształcie przyniesie efekt odwrotny od oczekiwanego.

W ocenie specjalistów, rozwiązanie zaproponowane w projekcie rozporządzenia doprowadzi do stanu, że zarejestrowane na kasie wirtualnej dane będą mogły być modyfikowane i usuwane, zanim zostaną wysłane do CRK. Rozwiązanie to nie zabezpiecza przed ewentualnym brakiem rejestracji sprzedaży przez nieuczciwego przedsiębiorcę oraz daje olbrzymie możliwości modyfikacji danych i zmniejszania lub całkowitego niepłacenia podatku VAT. Może również posłużyć jako doskonałe narzędzie oszustw na większą skalę, gdyż za tego typu działaniami mogą stać zorganizowane mafie VAT-owskie. Obecnie stosowane kasy sprzętowe uniemożliwiają powyżej opisane nadużycia.

Konsultowana propozycja może być analogiczna w skutkach do zmian wprowadzonych w automatach do gier losowych tzw. jednorękiach bandytach. Rozwiązanie mechaniczne zastąpiono oprogramowaniem, które umożliwiło zdalną manipulację. Spowodowało to oszustwa na niespotykaną wcześniej skalę oraz olbrzymie straty dla budżetu państwa, tzw. afera hazardowa.



Istnieje realne zagrożenie, że wprowadzane „kasy wirtualne” w kształcie proponowanym przez projekt rozporządzenia staną się **„kasami pozornymi” lub tylko pozorującymi rejestrowanie sprzedaży**, a wpływy z tytułu podatku VAT będą **„wpływami wirtualnymi”**. Organy odpowiedzialne za zaprojektowanie i wdrożenie rozwiązania będą ocenione dopiero po fakcie **zmniejszenia wpływów budżetowych** oraz pogorszeniu warunków konkurencyjności dla uczciwych przedsiębiorców.

Szczegółową ocenę zagrożeń przeprowadzamy na kolejnych stronach konsultacji projektu rozporządzenia.

W imieniu Zarządu OPBF
Prezes Zarządu

Marcin Monkiewicz

Załączniki:

1. Uwagi i zagrożenia zebrane przez specjalistów OPBF do zapisów projektu rozporządzenia.
2. Tabela dodatkowych uwag z odniesieniem do zapisów projektu rozporządzenia.
3. Cyberbezpieczeństwo rozwiązań softwarowych a administracja rządowa.
4. Raport „Security analysis of Croatia’s receipt registration and verification system”.
5. Tłumaczenie raportu z Załącznika nr 4 na język polski „Analiza bezpieczeństwa systemu rejestracji i weryfikacji paragonów w Chorwacji”.



Załącznik nr 1 do pisma OPBF z dnia 03.09.2019 r.

Uwagi i zagrożenia zebrane przez specjalistów OPBF do zapisów projektu rozporządzenia

1. Zagrożenie zmniejszenia dochodów budżetu państwa z tytułu podatku VAT.

Zaproponowana w projekcie rozporządzenia „kasa wirtualna” w wielu przypadkach może być „kasą **nierzeczywistą**” lub „kasą **pozorną**” (synonimy słowa „wirtualna”). Wskazujemy wybrane zagrożenia, które umożliwiają nieuczciwym podmiotom gospodarczym nie rejestrowanie sprzedaży bądź zaniżanie uzyskanego obrotu.

Poniżej przedstawiamy przykład zrzutu ekranu aplikacji, która umożliwia wyłączenie fiskalizacji sprzedaży. Tego typu aplikacja, będąca w przyszłości wirtualną kasą rejestrującą może posiadać **jawne lub ukryte możliwości** niepełnego ewidencjonowania sprzedaży do Centralnego Repozytorium Kas.

Rys. Przykład niehomologowanej aplikacji do prowadzenia ewidencji sprzedaży dostępnej w sklepie Google Play dla systemu operacyjnego Android.

Dopuszczając do obrotu oprogramowanie, które nie będzie homologowane przez Główny Urząd Miar, Ministerstwo Finansów akceptuje możliwość przygotowania kas wirtualnych przez nieuczciwych producentów oprogramowania, które mogą posiadać ukryte funkcje.



Przykładowo:

- kasowanie wybranych paragonów z bazy danych, zanim zostaną wysłane do CRK,
- zmniejszanie wartości wysyłanych paragonów do CRK,
- usuwanie całej bazy danych, jako „awaria” kasy, przed wysłaniem do CRK,
- drukowanie sklonowanych paragonów fiskalnych w przypadku usług powtarzających się (np. 1 porcja lodów, usługa medyczna, kufel piwa itd.),
- drukowanie sfałszowanych paragonów, które będą łudzaco przypominały paragony prawdziwe, bez wysyłania ich do CRK.

Wszystkie wymienione wyżej nadużycia są niemożliwe do zrealizowania w kasach sprzętowych homologowanych w Głównym Urzędzie Miar.

Niezależnie od przygotowanej przez producentów oprogramowania funkcjonalności kas wirtualnych, dla nieuczciwych przedsiębiorców otwierają się następujące pola do nadużyć:

- możliwość samodzielnego ufiskalnienia kasy wirtualnej na nie swój NIP
(w obecnie stosowanych kasach sprzętowych fiskalizacji oraz weryfikacji dokonuje uprawniony serwisant, a kopia wykonanej operacji pozostaje w serwisie),
- możliwość kasowania lub modyfikowania danych przez inne aplikacje przed wysłaniem do repozytorium lub przez wykonanie przywracania systemu operacyjnego np. do momentu rozpoczęcia pracy w danym dniu
(kasa sprzętowa on-line ma wszystkie dane zabezpieczone w pamięci fiskalnej oraz pamięci chronionej),
- możliwość równoległego używania z kasą wirtualną oprogramowania sprzedażowego drukującego paragony łudzaco podobne do fiskalnych,
(w kasach sprzętowych wykluczono używanie równoległego oprogramowania poprzez przeprowadzenie homologacji urządzenia w Głównym Urzędzie Miar),
- możliwość wykonania kopii całego systemu operacyjnego wraz z pobranym i ważnym kodem współdzielonym, celem wykonania wielu kopii danej kasy wirtualnej np. na czas imprezy masowej.

Przykład 1: Nieuczciwy przedsiębiorca prowadzi działalność sezonową nad morzem sprzedając lody głównie podczas imprez masowych. Celem uniknięcia płacenia podatków przed rozpoczęciem imprezy masowej instaluje na telefonie aplikację kasy wirtualnej, ufiskalnia ją na swój NIP oraz pobiera kod współdzielony, po czym wyłącza Internet w telefonie. Następnie wykonuje pełną kopię systemu operacyjnego wraz z kasą wirtualną i wgrywa (tą kopię) na kolejne 20 telefonów. Wszystkie tak przygotowane kasy wirtualne pracować będą prawidłowo przez okres co najmniej 72 godzin licząc od pobrania kodu współdzielonego wystawiając



„legalne” paragony. Personel obsługujący kasy nie ma możliwości zorientowania się, że od wystawianych paragonów nie będzie odprowadzony podatek, gdyż paragony te są „prawdziwe”. Przed upływem 72 godzin przedsiębiorca przywróci połączenie Internet na jednym telefonie, a pozostałe 20 telefonów przywróci do ustawień fabrycznych - kasa wirtualna wraz z wszystkimi danymi znikną. W efekcie wyłącznie dane o obrotach i należnym podatku VAT z jednego telefonu trafią do CRK, a dane z pozostałych 20 szt. kas wirtualnych oraz dane o należnym podatku VAT nigdy nie trafią do CRK, a podatek nie trafi do budżetu państwa.

Przykład 2: Nieuczciwy przedsiębiorca prowadzi mobilną działalność gastronomiczną – Food Truck. Posiada jedną kasę wirtualną, na której rejestruje sprzedaż w dni robocze, a w weekendy (podczas intensywniejszej pracy) używa naprzemiennie 2 szt. kas, przy czym drugą kasę ufiskalnia samodzielnie na losowo wybrany z CEiDG nr NIP. W efekcie takiego działania nieuczciwy przedsiębiorca odprowadza podatki do budżetu tylko częściowo, a obroty zarejestrowane na drugiej kasie obciążają innego podatnika. W efekcie drugi, niczego nieświadomy podatnik, będzie wzywany do Urzędu Skarbowego celem złożenia wyjaśnień. Niestety prawdopodobieństwo ściągnięcia należności podatkowych od pierwszego, nieuczciwego przedsiębiorcy, będzie mocno utrudnione, gdyż kontrolerom skarbowym ciężko będzie znaleźć nieuczciwego przedsiębiorcę, jako że na paragonach wszelkie dane będą nieprawdziwe.

Wszystkie powyższe (i wiele innych) „możliwości” **będą uszczuplały wpływy podatku VAT do budżetu**, będą również umożliwiały oszustom prowadzenie nieuczciwej konkurencji w stosunku do podmiotów prowadzących uczciwą działalność.

2. Zagrożenia z punktu widzenia bezpieczeństwa podatnika.

- ze względu na brak homologacji Głównego Urzędu Miar podatnik nie będzie miał pewności czy używana przez niego kasa wirtualna prawidłowo nalicza podatek VAT oraz przesyła wszystkie dane do CRK,
- podatnik nie będzie posiadał swojej „pewnej i niezmienniej” kopii danych o obrotach i należnym podatku VAT, co w przypadku konfliktu z organami podatkowymi może doprowadzić nawet do bankructwa przedsiębiorcy. *Kasy sprzętowe posiadają bezpieczną pamięć fiskalną.*
- podatnik używając otwartego systemu operacyjnego nie jest w stanie zabezpieczyć w sposób pewny danych o sprzedaży przed ich wykasowaniem, uszkodzeniem lub przed atakami hakerskimi,
- w przypadku wystąpienia problemów z łącznością Internetową kasa wirtualna przestanie pracować ze względu na brak ważnego klucza współdzielonego po maksymalnie 72 godzinach,
- ze względu na brak stałego nadzoru nad kasą wirtualną przez autoryzowane i przeszkolone służby serwisowe podatnik nie będzie miał możliwości prawidłowej weryfikacji używanej



przez niego kasy wirtualnej, czy działa prawidłowo oraz czy nie została zaatakowana przez wirusy lub hakerów,

- pełna odpowiedzialność za używanie błędnie działającej kasy wirtualnej spada na podatnika, a w przypadku pojawienia się problemów jedyną stroną odpowiedzialną może być producent oprogramowania i tylko do niego na drodze cywilnej podatnik będzie mógł zwrócić się o rekompensatę poniesionych strat,
- personel podatnika powinien mieć pewność, że używa prawdziwego oprogramowania kasy wirtualnej; w przypadku uruchomienia **oprogramowania udającego kasę wirtualną** niczego nieświadomy **personel narażony będzie na odpowiedzialność** zgodnie z punktem B Załącznika nr 3 do rozporządzenia: „Na osobę, która dokona sprzedaży z pominięciem kasy rejestrującej albo nie wyda paragonu fiskalnego może zostać nałożona kara grzywny za przestępstwo skarbowe albo wykroczenie skarbowe (zgodnie z art. 62 § 4 i § 5 ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy (Dz. U. z 2018 r. poz. 1958, z późn. zm.).”

Przykład: Uczciwy podatnik w dobrej wierze nabywa kasę wirtualną, którą wcześniej przygotował i wprowadził do obrotu uczciwy autor oprogramowania. Autor oprogramowania przeprowadził wcześniej samodzielne, wewnętrzne testy kasy zgodnie z zapisami projektu rozporządzenia i samodzielnie wystawił kasie certyfikat. Kasa ta jednak nie poddana została żadnym zewnętrznym testom, gdyż taki obowiązek nie został nałożony na autora oprogramowania w projekcie rozporządzenia.

Mimo zrealizowania przez autora oprogramowania wewnętrznych testów, które wypadły pomyślnie nie wykazując jakichkolwiek błędów, okazało się, że kasa czasami błędnie nalicza podatki lub błędnie przesyła dane do Centralnego Repozytorium Kas.

Analizując powyższą sytuację pojawiają się następujące pytania:

- kto będzie odpowiadał przed Urzędem Skarbowym za niepoprawne dane o wartości podatku naliczonego na paragonach, które zostały wysłane do serwerów MF?
- czy za niedopłatę lub nadpłatę podatków odpowiadać będzie autor oprogramowania czy podatnik?

W przypadku proponowanego rozwiązania kasy wirtualnej podatnik nie będzie miał żadnej możliwości weryfikacji poprawności wysyłanych danych do CRK, a konsekwencja niewysłania lub wysłania błędnych danych obciążała będzie prawdopodobnie podatnika.

Obecnie używane oprogramowania księgowe umożliwiają weryfikację danych przed ich wysłaniem do administracji skarbowej. Dane te weryfikuje podatnik/księgowy i dopiero po ich sprawdzeniu przekazywane są do US. To księgowy i podatnik odpowiadają za prawidłowość wysłanych danych.

W proponowanym kształcie kasy wirtualnej podatnik nie ma pewności co do prawidłowości przesyłanych danych do CRK, którą w obecnym systemie kas sprzętowych zapewnia homologacja Głównego Urzędu Miar.



Powyżej wymieniliśmy wybrane wady rozwiązania w zaproponowanym kształcie w projekcie rozporządzenia w sprawie kas rejestrujących mających postać oprogramowania. Ilość możliwych niedoskonałości lub błędów wynikających z braku homologowania oprogramowania w Głównym Urzędzie Miar jest nieograniczona.

3. Ocena wybranych argumentów przedstawionych w dokumencie OSR (Ocena Skutków Regulacji).

Wybrane argumenty wskazane w dokumencie OSR oraz uzasadnieniu do projektu nie są trafne.

1. Dokument OSR, punkt 2:

„...Stosowanie kas w postaci oprogramowania ma zwiększyć efektywność działań administracji skarbowej w zakresie zwalczania nierejestrowanej sprzedaży detalicznej oraz unikania i uchylania się od opodatkowania w zakresie podatku VAT poprzez wprowadzone mechanizmy kontrolne w czasie rzeczywistym.”

Komentarz:

Zaproponowane w projekcie rozporządzenia rozwiązanie nie daje możliwości wprowadzenia mechanizmów kontrolnych w czasie rzeczywistym, gdyż:

- zgodnie z Załącznikiem nr 1 do projektu Rozporządzenia, w części „Wymagania techniczne dla kas dotyczące pracy kasy”, pkt 34: *„Kasa przesyła dane używając domyślnego harmonogramu przesyłania danych nie rzadziej niż co 2 godziny.”*,
- zgodnie z § 2. Projektu Rozporządzenia *„Ilekroć w rozporządzeniu jest mowa o: ...,12) kluczu współdzielonym – rozumie się przez to klucz symetryczny, udostępniany przez urząd obsługujący ministra właściwego do spraw finansów publicznych, używany jako klucz włączany dla kodów uwierzytelniania wiadomości (zgodnie z algorytmem HMAC-SHA256, norma FIPS 180-4), służącego jako element zabezpieczenia kodu QR, którego ważność określa się na 72 godziny, a czas jego wymiany 24 godziny;”*

Skoro kasa wirtualna przesyła dane nie rzadziej niż co 2 godziny (przy założeniu sprawnego, nie odłączonego przez nieuczciwego podatnika połączenia internetowego) a dalsze działanie kasy będzie możliwe bez połączenia z Internetem przez kolejne 72 godziny, to niewątpliwie **rozwiązanie takie nie daje założonych w OSR możliwości użycia mechanizmów kontrolnych w czasie rzeczywistym gdyż kasa działa w trybie off-line.**



2. Dokument OSR, punkt 3:

„...Rozwiązanie to ma zbliżone cechy rozwiązania stosowanego w Czechach, Austrii i Chorwacji.”

Komentarz:

Zaproponowane w projekcie rozporządzenia rozwiązanie „kas wirtualnych” **jest zasadniczo inne niż zastosowane w Czechach, Austrii i Chorwacji**. O ile można potwierdzić, że rozwiązanie czeskie i chorwackie oraz zaproponowane w projekcie rozporządzenia oparte jest o postać oprogramowania, to **rozbieżna jest najistotniejsza cecha** związana z możliwością przeprowadzania kontroli w czasie rzeczywistym, gdyż zaproponowane w projekcie rozporządzenia rozwiązanie **w rzeczywistości jest rozwiązaniem OFF-LINE bez zapisanych bezpiecznie danych**.

Zarówno w Czechach, jak i Chorwacji mechanizm polega na przesyłaniu wystawianych paragonów w czasie rzeczywistym do serwerów Administracji Podatkowej, zanim taki paragon zostanie wydrukowany i wręczony nabywcy (czyli jest to rozwiązanie ON-LINE). Przy tak działającym systemie można przyjąć założenie, że wysłane dane do Administracji Podatkowej nie ulegną modyfikacji ani usunięciu z „kasy wirtualnej” podatnika. Rozwiązanie pozwalające podatnikowi pracować przez kolejne 72 godziny bez podłączenia do Internetu jest rozwiązaniem wyłącznie awaryjnym, **a mimo to jest jednym z głównych problemów niezszelności systemu Chorwackiego**. Temat ten został opisany w Raporcie, który stanowi Załącznik nr 4, a jego tłumaczenie – załącznik nr 5.

Ponadto, kontaktując się w ramach konsultacji z Panem Stjepan Groš – autorem ww. Raportu, uzyskaliśmy informację, że polem do nadużyć jest 72 godzinny czas na zarejestrowanie paragonu w przypadku sytuacji awaryjnej (brak dostępu do Internetu). To właśnie **udawane sytuacje awaryjne umożliwiają unikanie rejestracji całego obrotu na kasie softwarowej**.

Ostatecznie nie można użyć stwierdzenia, że „Rozwiązanie to ma zbliżone cechy rozwiązania stosowanego w Czechach, Austrii i Chorwacji”, jeśli **główna cecha rozwiązania jest całkowicie odmienna (ON-LINE vs OFF-LINE)**.

3. Dokument OSR, punkt 1:

„...Nowe rozwiązanie pozwoli na stosowanie do prowadzenia ewidencji sprzedaży na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych kas mających postać oprogramowania, co ma zachęcić przedsiębiorców do wyjścia z szarej strefy poprzez łatwą dostępność i obniżenie całkowitych kosztów posiadania kas rejestrujących...”



Komentarz:

Stwierdzenie, mówiące, że nowe rozwiązanie ma zachęcić przedsiębiorców do wyjścia z szarej strefy jest mocno naciągane. Podmioty unikają rejestracji sprzedaży nie ze względu na brak środków lub zbyt wysokie koszty zakupu kasy sprzętowej, a z powodu niechęci płacenia podatków.

Uczciwy przedsiębiorca, który nie stosuje dzisiaj kasy fiskalnej, gdyż np. nie przekroczył obrotu na rzecz osób fizycznych w wysokości 20.000 zł rocznie, zawsze może taki przychód zaewidencjonować ręcznie w ewidencji przychodów. Ciężko zatem stwierdzić, że dostępność nowego rodzaju kas zachęci go do dodatkowego ujawnienia swoich obrotów, skoro obroty te, jako uczciwy przedsiębiorca tak czy inaczej ujawnia.

Dziwi również stwierdzenie, iż nowe rozwiązanie spowoduje „...obniżenie całkowitych kosztów posiadania kas rejestrujących...”.

Aby prawidłowo ocenić, które z rozwiązań jest tańsze dla podatnika, należy mieć możliwość porównania **całkowitego kosztu obu rozwiązań**.

W przypadku obecnie stosowanych **kas sprzętowych on-line całkowity koszt używania dla podatnika jest w pełni przewidywalny**. Uwzględniając sektor MSP, np. niewielki zakład usługowy (fryzjer, mechanik samochodowy itd.), pracujący 5 dni w tygodniu, kasa umożliwi podatnikowi pracę przez okres 7 lat i 3 miesiące (pojemność modułu fiskalnego: 1830 raportów dobowych).

Dla ww. przykładu koszty kształtować mogą się następująco:

- kasa fiskalna on-line polskiego producenta: 1249 zł netto
- fiskalizacja kasy on-line: wliczone w cenę kasy,
- Internet: 0 zł miesięcznie (w większości punktów Internet już jest zainstalowany),
- wykonanie okresowych przeglądów (co 24 miesiące), kontrolujących i weryfikujących poprawność działania urządzenia, przez autoryzowany serwis: 3 x 200 zł netto,
- gotowość serwisowa (czas interwencji maksimum 48 godz.): 0 zł,
- wykonanie końcowego odczytu pamięci fiskalnej, zapewniającego przesłanie wszystkich danych do CRK Ministerstwa Finansów: 150 zł netto.

Całkowity koszt posiadania kasy sprzętowej on-line przez okres 7 lat i 3 miesiące (87 miesięcy): 1999 zł netto, czyli 22,98 zł netto miesięcznie.

Za całkowitą kwotę niespełna 23 zł miesięcznie podatnik ma zapewnioną obsługę urządzenia przez wyszkolony i autoryzowany serwis oraz ma zagwarantowany przez Ministerstwo Finansów w treści „Rozporządzenia w sprawie kas rejestrujących” maksymalny czas na rozpoczęcie interwencji: 48 h od zgłoszenia.



W dokumencie OSR nie określono całkowitego kosztu kasy rejestrującej mającej postać oprogramowania – kasy wirtualnej. W treści projektu są wskazane niezbędne jej elementy, o których **wycenę pokusiliśmy się bazując na ofertach z rynku czeskiego, gdzie używane są kasy softwarowe z prawdziwym on-line:**

- drukarka do wydruku paragonów z kasy wirtualnej: cena od 300 zł (drukarka paragonowa bluetooth) do 1300 zł netto,
- urządzenie do zainstalowania kasy wirtualnej: telefon, tablet, komputer: cena od 300 zł do 3000 zł netto,
- koszt licencji kasy wirtualnej wraz z programem sprzedażowym (liczony jako opłata miesięczna w tzw. abonamencie): cena od 69 zł do 169 zł netto miesięcznie,
- koszty obsługi technicznej i wsparcia użytkownika: założmy, że w cenie abonamentu miesięcznego.

Całkowity koszt posiadania kasy wirtualnej (sprzęt plus opłata licencyjna) za okres 7 lat i 3 miesięcy – analogicznie do kas sprzętowych – to zakres od 6 603 zł do 19 003 zł netto, czyli od 75,90 zł do 218,43 zł netto miesięcznie.

Uwaga: zakup sprzętu z najniższego progu cenowego nie gwarantuje pracy przez ponad 7 lat i należy liczyć się z jego wcześniejszą wymianą.

Biorąc pod uwagę powyższe porównanie kasy sprzętowej i kasy wirtualnej **nieuprawnione jest stwierdzenie, że nowe rozwiązanie obniży całkowity koszt posiadania kasy rejestrującej przez podatnika.**

W ocenie OPBF koszty te mogą okazać się wyższe dla kasy wirtualnej w stosunku do obecnie znanego rozwiązania sprzętowego kasy on-line.

W powyższej ocenie nie uwzględniamy przysługującego podatnikowi odliczenia 700 zł od kasy sprzętowej, którego zasady zapisane są w „Rozporządzeniu Ministra Finansów w sprawie odliczania lub zwrotu kwot wydatkowanych za zakup kas rejestrujących oraz zwrotu tych kwot przez podatnika”.

Ponadto, nowe rozwiązanie (mimo iż może być droższe) zachęci nieuczciwych przedsiębiorców do zastosowania kas wirtualnych ze względu na łatwość manipulacji danymi, a tym samym uniemożliwi prawidłowe przeprowadzenie kontroli, zarówno od strony administracji podatkowej, personelu, jak i klientów – odbiorców usług.

Ostatecznie **zamiast oczekiwanego efektu wyjścia z szarej strefy, efekt będzie dokładnie odwrotny**, a u nieuczciwych podatników nastąpi zmniejszenie ewidencjonowania sprzedaży oraz wartości odprowadzanych przez nich podatków.



Nie widzimy żadnych przesłanek potwierdzających, że rozwiązanie oparte o oprogramowanie spowoduje zakładany w OSR wzrost ściągalsności podatków w stosunku do szczerne go rozwiązań oparte go obecnie o sprzętowe kasy on-line.

WNIOSKI

Po analizie projektu rozporządzenia specjalistom z OPBF nasuwają się następujące wnioski:

- projekt w obecnym kształcie zakłada, że użytkownikami kas wirtualnych będą wyłącznie uczciwi przedsiębiorcy,
- przy projektowaniu rozporządzenia nie uwzględnione zostały aspekty bezpieczeństwa dla uczciwych przedsiębiorców,
- w projekcie rozporządzenia nie zostały uwzględnione przepisy krajowe i unijne dotyczące cyberbezpieczeństwa aplikacji kluczowych obowiązujące organy administracji rządowej (Załącznik nr 3),
- w projekcie rozporządzenia nie zostały uwzględnione stosowne metody zabezpieczenia systemu przed praniem brudnych pieniędzy i mafiami VAT-owskimi,
- wzorując się na niezbyt szczerne m systemie chorwackim (Raport dotyczący bezpieczeństwa stanowi Załącznik nr 4 oraz jego tłumaczenie – Załącznik nr 5) i czeskim **zdecydowano o zastosowaniu jeszcze mniej skutecznego rozwiązania, oparte go o komunikację OFF-LINE**, podatnego na modyfikację lub usunięcie danych przed ich wysłaniem do Centralnego Repozytorium Kas.

Analizując sytuację w innych krajach europejskich da się zauważyć **tendencję uszczelniania rejestrowania sprzedaży przy pomocy zabezpieczeń sprzętowych**. Są to rozwiązania oparte o osobne kasy rejestrujące sprzętowe lub dedykowane urządzenia rejestrujące do kas lub komputerów. Rozwiązania te zostały lub będą zastosowane m.in. w następujących krajach: Włochy, Węgry, Niemcy, Szwecja.

Jedynie w krajach o niewielkiej populacji i małej ilości punktów handlowych (np. Chorwacja, Czechy) zastosowano rozwiązania oparte o kasy wirtualne z **rzeczywistym połączeniem on-line, które charakteryzują się zapisem paragonu w repozytorium przed jego wydrukowaniem**.

W przedstawionym projekcie rozporządzenia Ministra Finansów nie skorzystano z zalet przytoczonych wyżej rozwiązań, co w konsekwencji może doprowadzić do rozszczelnienia systemu ewidencji podatku VAT.



PODSUMOWANIE

Dotychczasowe rozwiązanie sprzętowych kas fiskalnych „online” stosowane od 1 maja 2019 r. bazuje na 3 filarach bezpieczeństwa dla budżetu państwa i dla uczciwych przedsiębiorców:

- bezpieczeństwie i niezmienności zapisywanych danych w module fiskalnych i pamięci chronionej,
- poprawności działania, naliczania podatku VAT oraz braku luk poprzez homologowanie rozwiązania sprzętowo-programowego w Głównym Urzędzie Miar,
- okresowego (nie on-line) przesyłania danych do serwerów Ministerstwa Finansów, celem umożliwienia szybszego i precyzyjniejszego wyznaczania podmiotów do kontroli.

Zaproponowane w projekcie rozporządzenia kas wirtualnych opartych o oprogramowanie zniweczy wszystkie wymienione wyżej cechy bezpieczeństwa:

- dane zapisane będą w otwartych systemach operacyjnych, co nie daje żadnej gwarancji niezmienności zapisanych danych, zarówno z punktu widzenia bezpieczeństwa budżetu państwa, jak i bezpieczeństwa podatnika,
- dopuszczenie do samodzielnej certyfikacji kasy wirtualnej przez ich producentów będzie przekazaniem zbyt daleko idących kompetencji producentowi oprogramowania; podobne przekazanie możliwości samodzielnej certyfikacji Boeingowi, według ekspertów było główną przyczyną tragicznych wypadków, w których łącznie zginęło blisko 350 osób,
- przeniesienie komunikacji off-line z rozwiązania sprzętowego, w którym dane nie ulegają zniszczeniu, do rozwiązania programowego bez gwarancji bezpieczeństwa danych, daje całą paletę możliwości dla nieuczciwych osób unikania w płaceniu należnych podatków.

W związku z przedstawionymi w całym piśmie argumentami, w szczególności brakiem szczelności rozwiązania oraz prawdopodobnie wyższymi kosztami kas wirtualnych, nielogiczne wydaje się zastępowanie sprowadzonego i szczelnego systemu poboru podatków opartego o kasy sprzętowe na rzecz kas softwarowych, nie dających oczekiwanego poziomu bezpieczeństwa dla budżetu państwa i dla uczciwego podatnika.



Załącznik nr 2 do pisma OPBF z dnia 03.09.2019 r.

Tabela dodatkowych uwag z odniesieniem do zapisów projektu rozporządzenia

L.p.	Przepis	Uwagi
1	dotyczy całości projektu	W obecnym kształcie projektu Rozporządzenia każdy producent oprogramowania – kasy wirtualnej – będzie miał możliwość wyprodukowania i dystrybuowania niehomologowanego oprogramowania, którego rzeczywista funkcjonalność będzie znana tylko producentowi oraz jego klientom, bez prawa weryfikacji poprawności jego działania, zarówno po stronie Ministerstwa Finansów, jak i Głównego Urzędu Miar. Dowolny producent oprogramowania może zadeklarować, że jego oprogramowanie jest szczelne, a wszyscy mają takim zapewnieniem zawierzyć, bez prawa do ich weryfikacji. Ponadto ilość błędów (zamierzonych lub nie) popełnianych przez programistów tworzących oprogramowania kas wirtualnych, wynikających z braku homologowania w Głównym Urzędzie Miar, jest nieograniczona. W konsekwencji, wśród podatników będą mogły działać kasy wirtualne niespełniające żadnych wymogów technicznych, co w prostej linii będzie prowadziło do uszczuplenia podatku VAT.
2	dotyczy całości projektu	W obecnym kształcie projektu Rozporządzenia całkowicie pominięto służby serwisowe , które w obecnym systemie pełnią kluczową rolę: 1) kontrolują prawidłowość przypisania kasy do danego podatnika, 2) dbają o prawidłowy przebieg fiskalizacji kas (na prawidłowy NIP), 3) dokonują przeglądów technicznych kas zgodnie z wymaganiami MF, 4) na bieżąco usuwają wszelkie awarie kas, 5) stawiają się bezpłatnie na każde żądanie właściwego dla podatnika naczelnika urzędu skarbowego we wszelkich sprawach wyjaśniających dotyczących używanych przez niego kas, 6) pełnią rolę kontroli pośredniej poprzez wychwytywanie wszelkich błędów, niezgodności stawek VAT przypisanych do towarów, itd.
3	dotyczy całości projektu	W obecnym kształcie projektu Rozporządzenia nie ma zapisów gwarantujących trwałość i niezmiennosć zapisanych danych o sprzedaży realizowanej przy pomocy kasy wirtualnej. Brak fizycznego urządzenia zapisującego dane (przy „kasach sprzętowych online” funkcję tę pełni „pamięć fiskalna”) może uniemożliwić przeprowadzenie kontroli skarbowej u podatników, gdyż dane te zawsze mogą zostać usunięte, a tym samym przebieg sprzedaży stanie się niemożliwy do odtworzenia.
4	dotyczy całości projektu	W obecnym kształcie projektu Rozporządzenia (załącznik nr 1) nie ma zapisów gwarantujących możliwości kontrolowania przez nabywcę prawidłowego przebiegu transakcji. W kasach sprzętowych online taką rolę pełni wyświetlacz klienta.
5	§ 3	Zapis w projektowanym kształcie wykracza poza delegację ustawową przewidzianą dla Ministra Finansów i kłóci się z zapisami zawartymi w Art. 111b Ust. 1 Ustawy o VAT. Ustawodawca jednoznacznie wskazał, że „Ewidencja sprzedaży, o której mowa w art. 111 ust. 1, w odniesieniu do niektórych grup podatników lub rodzajów czynności może być prowadzona przy użyciu kas rejestrujących mających postać oprogramowania...”. Sformułowanie „... w odniesieniu do niektórych grup podatników...” nie może oznaczać „...wszystkich podatników VAT czynnych, jak i zwolnionych”, jak zostało zapisane w treści § 3.



6	§ 5.4	Przepis nie precyzuje co ma zrobić podatnik, jeżeli producent jego kasy wirtualnej przestanie istnieć lub przestanie świadczyć usługę wsparcia. Podatnik przestanie mieć możliwość korzystania z kasy, gdyż nie będzie mógł wysyłać danych do CRK. W projekcie brak jakiegokolwiek zobowiązania producenta oprogramowania do zapewnienia wsparcia podatnikowi, jak ma to miejsce w przypadku sprzętowych kas online.
7	§ 9.2	Przy zastosowaniu otwartych systemów operacyjnych (np. Windows / Linux / Unix / MacOS / Android, ...) podatnik może zasymulować obecność drukarki dla kasy wirtualnej poprzez zainstalowanie w środowisku systemu operacyjnego sterowników wirtualnych drukarek „drukujących” do pliku. Taki mechanizm w bardzo prosty sposób może być wykorzystywany do replikowania prawidłowo wystawionych paragonów i drukowania ich, zamiast wystawiania „nowych” paragonów na ten sam towar bądź usługę.
8	§ 11.1.8	Kasa wirtualna nie ma możliwości zagwarantowania czytelnych wydruków, oraz wydruków w ogóle, gdyż kasa wirtualna nie kontroluje drukarki w sposób bezpośredni. Sam wydruk zawsze realizowany jest przy udziale zewnętrznego systemu operacyjnego (np. Windows / Linux / Unix / MacOS / Android, ...).
9	§ 11.3	Personel podatnika powinien mieć pewność, że używa prawdziwego oprogramowania kasy wirtualnej. W przypadku uruchomienia oprogramowania udającego kasę wirtualną, niczego nieświadomy personel narażony będzie na odpowiedzialność zgodnie z punktem B Załącznika nr 3 do rozporządzenia: „Na osobę, która dokona sprzedaży z pominięciem kasy rejestrującej albo nie wyda paragonu fiskalnego może zostać nałożona kara grzywny za przestępstwo skarbowe albo wykroczenie skarbowe (zgodnie z art. 62 § 4 i § 5 ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy (Dz. U. z 2018 r. poz. 1958, z późn. zm.)).”
10	§ 14.1.2	Podatnicy mają obowiązek udostępniać kasy do kontroli. Nie wskazano jednak kto te kontrole będzie przeprowadzał. Trudno sobie wyobrazić, że kontrolę aplikacji o nieznannej funkcjonalności, niehomologowanej w GUM przeprowadzić będą mogli pracownicy Urzędów Skarbowych. Jak mają oni zweryfikować, czy dane w kasie wirtualnej są prawidłowe, czy nikt ich wcześniej nie modyfikował lub czy ich nie wykasował? Powinny to kontrolować usługi serwisowe mające odpowiednią wiedzę techniczną.
11	§ 15.1	Ze względu na fakt, iż oprogramowanie kasy wirtualnej może być licencjonowane na zasadach SAS (koszt licencji miesięczny), łatwo można sobie wyobrazić nadmierną częstotliwość zgłaszania przez podatników utraty kasy wirtualnej, np. zainstalowanej na telefonie, bez ponoszenia jakichkolwiek konsekwencji. O transakcjach wykonanych na takiej „utraconej” wcześniej kasie nikt się nigdy nie dowie, ponieważ telefon jest mały i ma prawo się zgubić lub nieodwracalnie zepsuć (np. w wyniku upadku). Projekt nic nie mówi, co zrobić w przypadku zepsucia się takiego urządzenia. Nierozliczone podatki w takim przypadku nigdy nie zostaną odprowadzone do budżetu państwa. Podatnicy chcący coś ukryć, po prostu zgłoszą do Urzędu Skarbowego utratę kasy wirtualnej – telefonu, a tym samym ukryją transakcje na niej wykonane. Można nawet wyobrazić sobie sytuację, w której podatnik zgłasza do Urzędu Skarbowego utratę kasy wirtualnej, a później de facto instaluje następną kasę wirtualną dokładnie na tym samym sprzęcie – np. telefonie. Ewidentne oszustwo, na które, w obecnym kształcie projektowanych przepisów, organy kontrolne nie mogą nic poradzić.
12	§ 15.3	W przypadku kas sprzętowych, po odzyskaniu utraconej wcześniej kasy, podatnik poddaje taką kasę kontroli w autoryzowanym serwisie. Dla kas wirtualnych nie przewidziano żadnych obowiązków zweryfikowania poprawności działania, po jej odzyskaniu.



13	§ 17	Dla kas wirtualnych przewidziano możliwość ich samodzielnej fiskalizacji przez podatnika. Kasy sprzętowe fiskalizuje autoryzowany serwisant weryfikując prawidłowość podanych danych, w tym jego NIP. Jak zagwarantować, że podatnik ufiskalni kasę na swój, a nie inny NIP?
14	§ 21	Przepis określa, co podatnik ma zrobić w przypadku zakończenia pracy na kasie, ale nie określa co zrobić w przypadku sytuacji awaryjnych, takich jak skasowanie danych lub uszkodzenie sprzętu, na którym działa kasa wirtualna. Nie ma przecież możliwości zweryfikowania poprawności danych przekazanych do CRK, gdyż dane te zostały bezpowrotnie utracone przed połączeniem się z CRK.
15	Załącznik nr 1 do rozporządzenia, s. 1 ostatnie zdanie: „baza danych kasy uniemożliwia dostęp użytkownika kasy do procedur edytowania tekstu;”	Wymaganie niemożliwe do spełnienia dla wszystkich oprogramowań działających na otwartych silnikach baz danych. W bazie danych utworzonej na takim silniku, to użytkownik jest twórcą hasła administratora, którym posługuje się później program (np. kasa wirtualna), aby daną bazę danych używać. Można zatem użyć tego hasła dla innego oprogramowania, które zmodyfikuje odpowiednio wpisy w danej bazie danych (baza danych kasy wirtualnej), lub też można zaingerować bezpośrednio w zapisy w bazie danych. Można również użyć mechanizmu tzw. triggera (wyzwalacza) bazodanowego, który zmodyfikuje „w locie” dane, które mają trafić do bazy danych (np. zaniży cenę towaru, a przy tym i wartość podatku) – może się to dziać automatycznie, a aplikacja będąca kasą wirtualną w ogóle nie wykryje takiego działania.
16	Załącznik nr 1 do rozporządzenia s. 2, pkt. 2) a) - b)	W przypadku zastosowania przez producentów oprogramowania przy budowie kasy wirtualnej bibliotek dołączanych dynamicznie (tzn. dołączanych podczas pracy programu kasy) zarówno suma kontrolna, jak i wersja programu pracy kasy będą jak najbardziej poprawne, jednak biblioteki w żaden sposób nie są kontrolowane i mogą zostać podmienione (świadomie przez podatnika lub nieświadomie poprzez złośliwe oprogramowanie) na biblioteki, które umożliwią uruchomienie funkcji zabronionych.
17	Załącznik nr 1 do rozporządzenia, s. 13, pkt. 23 a), 24 a)	Wymagania niemożliwe do spełnienia. Kasa wirtualna sama z siebie nie może uniemożliwiać zmiany daty i czasu, gdyż działa pod kontrolą jakiegoś systemu operacyjnego (np. Windows / Linux / Unix / MacOS / Android, ...). W każdej chwili, zamykając oprogramowanie kasy wirtualnej podatnik ma możliwość ingerencji w datę lub czas swojego urządzenia (np. telefonu, tabletu, komputera,...).



Załącznik nr 3 do pisma OPBF z dnia 03.09.2019 r.

Cyberbezpieczeństwo rozwiązań softwarowych a administracja rządowa.

Prawidłowe zabezpieczenie systemu „kas wirtualnych”

Wszystkie akty prawne wydawane przez organy administracji rządowej, co do zasady muszą być zgodne obowiązującym prawem krajowym oraz unijnym.

Jeden z aktów, którym jest **Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa** (Dz.U. 2018, poz. 1560)

opisuje w Art. 1.:

- 1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
- 2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
- 3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Art. 3.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Art. 4 wymienia podmioty, które są objęte systemem cyberbezpieczeństwa i są to między innymi:

- 7) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62, 1000 i 1366)

Uwzględniając wyżej wskazane zapisy Ustawy o krajowym systemie cyberbezpieczeństwa zauważyć należy, że **jednym z podmiotów objętych systemem cyberbezpieczeństwa jest Minister Finansów wraz z właściwymi służbami odpowiadającymi za prawidłowe wpływy podatków do budżetu państwa.**

W projekcie rozporządzenia w sprawie kas rejestrujących mających postać oprogramowania nie zostały spełnione między innymi następujące wymagania wobec systemów informacyjnych opisane w Rozdziale 3 Ustawy o krajowym systemie cyberbezpieczeństwa:

1. wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
 - a. utrzymanie i bezpieczną eksploatację systemu informacyjnego,

str. 17



- b. **bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,**
 - c. bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
 - d. wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
 - e. objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;
2. **zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,**
 3. stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
 - a. stosowanie mechanizmów zapewniających poufność, integralność, dostępność i **autentyczność danych** przetwarzanych w systemie informacyjnym,
 - b. dbałość o aktualizację oprogramowania,
 - c. **ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,**
 - d. niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.

Wskazane wyżej punkty w jasny sposób pokazują, że najważniejsze z punktu widzenia bezpieczeństwa działania infrastruktury systemów informacyjnych jest jej właściwe zaprojektowanie, wykorzystywanie oraz modernizacja i rozwój.

Obowiązkiem dostawców komponentów systemu – w tym przypadku producentów (developerów) kas mających postać oprogramowania – jest **zapewnienie utrzymania ich bezpieczeństwa na wymaganym poziomie**, a co za tym idzie ich rozwój nie tylko w kierunku nowych funkcjonalności ale **przede wszystkim kładzenie nacisku na ich bezpieczeństwo**.

W ramach tych działań rozporządzenie ministra finansów **musi nałożyć obowiązek** monitorowania i analizowania wykrytych podatności nie tylko samej aplikacji kasowej, ale również środowiska softwarowego w jakim będzie ona pracować ze szczególnym uwzględnieniem systemów operacyjnych, silników baz danych, systemów transmisji danych, wykorzystywanych protokołów transmisyjnych, protokołów szyfrujących.

Jednym z ważniejszych obowiązków dostawców aplikacji kasy softwarowej musi być regularne publikowanie biuletynu bezpieczeństwa wskazującego wykryte luki i sposoby ich zablokowania. **Tylko przy spełnieniu wymogów ustawy o cyberbezpieczeństwie i poddaniu oprogramowania kasy softwarowej certyfikacji (homologacji) przez Główny Urząd Miar podatnik użytkujący kasę softwarową może mieć pewność, że zrobił wszystko aby w sposób bezpieczny jej używać i nie narażać się na popełnienie przestępstwa karno-skarbowego.**



Aby zapewnić zgodność projektu „Rozporządzenia ministra finansów w sprawie kas rejestrujących mających postać oprogramowania” z obowiązującą „Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa” należy poddać ją konsultacji ze specjalistami z zakresu cyberbezpieczeństwa i uwzględnić ich zalecenia.

Szczególną uwagę należy zwrócić na załącznik nr 1 projektu rozporządzenia: „Wymagania techniczne dla kas dotyczące ich zawartości”, ponieważ tutaj **zawarte winny być wszystkie parametry dotyczące bezpieczeństwa kas softwarowych.**

Security analysis of Croatia's receipt registration and verification system

Stjepan Groš

University of Zagreb, Faculty of Electrical and Computing Engineering,
Unska 3, 10000 Zagreb, Croatia
E-Mail: stjepan.gros@fer.hr

Abstract—Beginning with 2013, a law in Croatia came into the force that requires owners of restaurants, café bars, and similar types of businesses that work with cash to register every receipt with a Tax Administration servers before issuing it to a customer. For the purpose of implementing the law APIS-IT, a Croatian IT company, developed a protocol based on XML, SOAP, and public key cryptography. They also implemented the server side system. It is a well known fact that developing protocols in general, and security protocols in particular, is a very tricky endeavor in which even the security professionals make mistakes. In this paper a security analysis of the protocol for receipt registration, the components of the system, and implementations is presented. Note that this is only a partial analysis, based on publicly available information, which doesn't include testings on live systems due to being illegal by the new Criminal law in Croatia. We identified two weaknesses of the current system. But the main problem of the system is the fact that many business owners are now open to different attacks and nothing has been done to remedy that situation. This is actually a broader problem since, with ever increasing number of on line services nothing is done to increase security awareness of people.

Index Terms—security,xml,threats,finance,analysis

I. INTRODUCTION

Beginning with 2013, a law [1] in Croatia came into the force that requires owners of restaurants, café bars, and other types of businesses that work directly with cash to register every receipt with the Tax Administration (TA) servers before issuing it to a customer. This is only a first phase of system deployment and during 2013, the rest of the businesses will also follow. For the purpose of implementing the law, APIS-IT, a Croatian IT company, developed a protocol based on XML, SOAP and public key cryptography, along with a server side system. It is a well known fact that developing protocols in general, and security protocols in particular, is a very tricky endeavor in which even the security professionals make mistakes. In this paper a security analysis of the protocol for receipt registration, the components of the system, and implementations is presented.

The paper is structured into 6 sections. First, in Section II we present the motivation for the introduction of the system for receipt registration. We also give an overview of its architecture and protocols used for communication. Finally, we get an overview of controls used to protect the system from deception. Then, in Section III we give a threat model, i.e. the model in which we are going to analyze the security of the system. In Section IV we enumerate different attacks against the system that allow different threat agents to circumvent controls and gain some advantage. This analysis is done under the

assumption of the perfect implementation, i.e. no programming or configuration errors in the implementation. But, in Section V we review some problems that might arise in case there are errors and omissions in implementation or deployment. Finally, the paper finishes with the Section VI in which we give conclusions, recommendations for improvements and outline the further work to be done.

II. THE SYSTEM UNDER THE SECURITY ANALYSIS

The system under the security analysis, i.e. the *Fiscal system*, was developed to prevent fraud that was based on the manipulation with receipts done by fraudulent businesses. In essence, receipts weren't issued, or if issued they were easily erased from the cash registers since they've only been stored locally. There were a control mechanisms in place to prevent such scenario, i.e. the customers could send receipt numbers to the TA which would verify that those receipts are really reported, and also TA could do inspections of both businesses and customers. Namely, customers were required by the law to take receipts. But this control mechanisms were inefficient, i.e. customers didn't report receipts, even if they did TA had problems verifying reported receipts because of diverse ways of enumerating them and manual work involved, and inspections are inefficient and costly. Thus, the Fiscal system was introduced with the following goals:

- Having each receipt stored on TA's servers at the moment receipt is issued, in order to prevent manipulation, i.e. to assure non repudiation, integrity and authenticity.
- Unifying receipt numbering schemes in order to make receipt checking easier and possible to automate.

Note that inspections by TA are still necessary in order to enforce receipts being issued. Furthermore, because of resource constraints in terms of a number of available inspectors, the customers are also encouraged to send receipt IDs to TA. This is further incentivized with different prizes that customers can win.

Based on these requirements, the architecture was developed along with appropriate protocols.

In essence, the architecture of the fiscal system is relatively simple. It consists of two entities, a client machine which submits receipts and TA's server which accepts receipts, records them and issues signed response (Figure 1).

The messages are exchanged using SOAP over HTTPS, while the data is serialized in XML format. To ensure authenticity, integrity and non-repudiation of the messages public

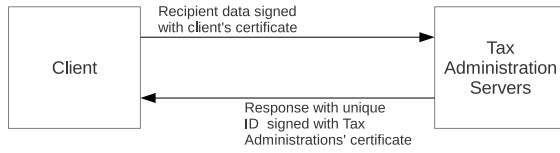


Fig. 1. The architecture of the fiscal system

key cryptography is used. Each entity in this system is issued a certificate by Financial Agency (FINA) [2] which acts as Government's Certificate Authority. The messages are signed before being sent and this signature is generated according to the XML Security specification. To ensure confidentiality (and integrity) of messages while being in transit, SSL/TLS is used. In total, six messages are defined:

- Receipt request/response pair of messages used to register receipt with TA.
- Request/response pair used to register office space.
- Simple echo request/response messages used to test TA's server availability.

Office space registration is used, presumably, for two purposes. First, for TA to know where receipts are issued, and secondly, to restrict the use of a single receipt on different locations.

But, of those, we are interested only in the first pair of messages used to register receipt with TA. So, each generated receipt has to be sent to TA prior to being issued to a customer, to obtain *unique receipt ID*. In this paper we will use abbreviation *JIR* for this unique receipt ID as it is so designated in appropriate documentation. An example of a JIR is:

```
6b7749c6-56c1-4cf5-b7f7-9f29cebc9f7f
```

Which is basically standard UUID format. Along with JIR, each receipt also has an *issuer's protection code*, we'll use abbreviation *ZKI* from now on as it is used in the Croatian documents. This code is generated by concatenating OIB, timestamp, receipt ID, office space ID, cash register ID, and total sum, then signing all that and finally taking MD5 of the signature data. Note that ZKI is generated by cash register without any data or involvement from TA's servers. An example of an ZKI is:

```
a1e6b1428f0cc755f0c82aa7a1327e35
```

The motivation for introducing this code is to protect issuer from a malicious third party [3] and also in cases when the issuer doesn't have connectivity to TA, then he can use this code instead of JIR.

There are two controls that force business owner to issue proper receipt:

- 1) A customer that checks receipt data on TA.
- 2) Direct controls by TA's inspectors.

Customers are required by law to take receipt with them. Additionally, they can also check JIRs by submitting them on TA's Web pages (or via SMS messages). In that way business owners are forced to issue receipt and they are prevented from

falsifying JIRs. Additionally, inspectors serve as control of both business owners (which are required by the law to issue receipt) and customers (which are also required by the law to take receipt). But, the reality is that there are not a lot of inspectors, their knowledge and equipment is rather poor. Customers, on the other hand, don't usually take receipt. This makes this control mechanisms rather weak.

Customers can verify receipt using either SMS message or a Web application [4] developed specially for that purpose. In both cases, the customer sends the following information:

- Either JIR or ZKI.
- Date and time when receipt was issued.
- Total amount.

If the entered data is correct, i.e. TA has data about the receipt, the Web application will only give information that receipt is correct. If the receipt can not be found in the TA's database the system will give to a customer a message to try again later. Note that due to the length of JIR and ZKI this control is weakened since retyping those codes is very hard, especially with SMS messages. Thus, errors are very likely and this further incentivizes customers *not* to verify receipts.

Note one interesting question. ZKI looks harder to read, but is shorter. JIR, on the other hand, is easier to read, but longer to type. So, it is reasonably to believe that customers will type ZKI more frequently, even though they are the same in term of the numbers and letters and the only difference is in dashes.

III. THREAT MODEL

As a first step we have to establish a threat model, i.e. a model that defines what are the threat sources and associated threats that can impact a system. Threat sources we analyze are:

- Business owners trying to circumvent paying taxes by manipulating receipts as they used to do.
- Individuals and crime organizations trying to take financial advantage of the system.
- Political groups and movements, like Anonymous, trying to subvert a system for PR purposes.

Business owners have incentive to manipulate system in order to avoid paying taxes. The ultimate goal is not to register smaller sum of money than there actually was. This can be done in two ways, (i) by not issuing receipt, or (ii) by somehow manipulating receipts themselves. Since not issuing receipt has nothing to do with the security analysis we'll ignore that scenario so we are only interested how business owner can manipulate receipts. We also ignore non-technical manipulations, like manipulations with fake receipts (quotes). We also assume that business owners have a complete control of cash register, both hardware, network connectivity, and software.

One thing to note is that business owners can be different in size, what will have impact on their network topology and controls they implement. Here, we'll assume small business owners, i.e. owners of restaurants, café bars and similar types of businesses.

It is the fact that cash register now has to be connected to the Internet (it has to be in order to be able to communicate with

Tax Administration's servers). Some of those will be directly accessible on the Internet (by having public IP address). Many will be run by Windows operating system, and thus will be threatened by usual threats, like malware. Last, but not least, probably business owners will offer their customers to access the Internet over the same LAN they use for communication with Tax Administration. This connectivity increases number of potential attackers, which we grouped into two categories, according to their motives for the attacks.

The first category consists of *individuals and crime organizations*. The difference is in the resources available to mount an attack. Obviously, individuals have fewer resources, while crime organizations have much larger resources on their disposal. So, individuals can try to attack at most few cash registers, while crime organizations can attack as much as they want.

The second group are political groups that aren't so much interested in financial gain but are satisfied with PR like events, like DoS attacks.

In the majority of the following text we'll assume *perfect implementation*, that is, will assume that programmers, both on server and client side, that implemented the protocol didn't make any programming mistakes. This is obviously very unrealistic assumption, especially from the point of business owners. At the end we'll outline possible mistakes that programmes could make and what this means in terms of attack possibilities. Still, this is a topic for a separate research.

IV. ATTACKS

A. Attacks by business owner

As we saw in Section II there are two primary controls that check invoices issued by business owners, customers and inspectors. Customers can not access cash register in order to check if invoice is handled properly or not, while TA's inspectors can to some degree.

So, here are some possibilities what business owners can do in order *not to* register valid receipt with the TA while in the same time avoiding being caught by the customers reporting invoice data to TA:

- Business owner can generate receipt only with ZKI. Then, he observes if the customer takes receipt or not. If he takes it then the Business owner registers receipt with TA, otherwise, he removes receipt from the system.

Note also that ZKI can be a random number, there is no way for customer, or TA, to check if it is valid or not. That means that if TA receives receipt with only ZKI it *can not prove* that this receipt was issued by certain business owner. This relates to the verification of receipt via Web or SMS. In that case many businesses can coordinate to issue receipts with the same ZKI, amount, date and time. Alternatively, they can reuse one's receipt.

Note that it is relatively easy to force customers to use ZKI instead of JIR. All they have to do is to print some random JIR. If the customer types JIR, the error will be reported and finally, if the customer is persistent enough he will finally try with ZKI.

- The way receipt checking with TA is implemented opens up possibility of reusing JIRs. Business owner can issue one receipt that will be registered with TA's servers. Then JIR and ZKI can be reused for other receipts with the same amount within a certain time frame.
- Since either JIR or ZKI is typed when the receipt is verified, this means that they don't have to be correlated. In other words, you can write JIR and ZKI belonging to a different receipts. But, for the time being it is questionable if this opens up some new possibilities to avoid registering invoice with TA.

Note that if issuing multiple receipts with the same JIR/ZKI then care must be taken about invoice numbers which are required to be sequential.

Now, second control, i.e. TA's inspectors, complicates things a bit, but not much. The first avoidance tactic in the previous list is the most dangerous. Namely, it rests on the fact that two, or more, persons don't collude, that is, they don't compare their invoices. TA's inspectors might do that, that is, they might collect somehow few invoices and if any two have the same JIR or ZKI, obviously the business owner has tried to circumvent the system.

The key difference between customers and TA's inspectors is that the latter can inspect data on cash register to some degree. What could happen is:

- Inspector comes with a bunch of invoices and asks business owner to show them records in cash register. If there are multiple invoices with the same JIR/ZKI/number then the business owner must be very careful which one he will show to inspectors. But, in the end, inspectors have no way to detect fraud *unless* they have at least two invoices with the same JIR/ZKI/number.
- For receipts that reuse JIR/ZKI numbers inspectors might notice that there is some discrepancy between dates on receipts and the actual time they were issued. But, there is no requirement on time synchronization on cash registers.
- The specification of the fiscal system defines that tax administration might ask business owner to recreate (or restore) ZKI. But it is very hard to verify that ZKI was generated using right data and, more importantly, the right certificate.

To conclude, without TA's inspections business owners have opportunities for manipulations even though they are not as easy as they were before. To which extent this manipulations can be done is a topic of a further research, especially if business owners collude. Additional problem is that TA's inspectors have to be properly equipped in order to be able to detect fraud. Finally, some fraud can be detected via advanced techniques like data mining on TA's servers.

B. Attacks by malicious individuals

Malicious individuals have enough resources to attack one, or at most several cash registers (CRs). Looking again on the Figure 1 individuals are a significant threat to business owners, and a lot less to TA's servers. Some of their motives can be the following ones:

- To harm competition by manipulating competition's receipts and in that way incur penalties by TA.
- To reuse invoices by competition and in that way no to register their invoices.
- To monitor what competition has been doing.
- Individuals that just want to do it because they can, to show off themselves.

In order to attack business owner and their CRs individuals have to be either:

- Somewhere on the communication channel, i.e. trying to perform MITM type of attacks.
- Trying to compromise cash register machine itself with a final goal of obtaining the secret key belonging to the business owner.
- Denial of service attack on Internet connection and/or cash register machine.

The communication channel is protected using HTTPS, so in case there are no bugs in the implementations it is very hard for the attacker to break into that channel. Note that two controls are of utmost importance here. The first one is that communication is performed via HTTPS (i.e. no fallback to HTTP) and second that the certificate check is properly implemented. The only way attacker can break into the channel is by exploiting bugs in the implementation. Since we assumed that there are no bugs, than this isn't an issue. Still, we'll return back to this possibility in Section V.

The second attack vector is by exploiting the client machine, i.e. cash register, itself. The grand prize in this case is stealing private key. The moment the attacker has control of the machine he is basically in a possession of private key. There could be protection in form of a password on a file but this password has to be stored somewhere. The ways in which an attacker can achieve that are usual attack vectors, of which the most dangerous one is social engineering attack. What makes things even worse here is that cash registers were old machines with old hardware and not maintained well. Now, when those machines are on the Internet, with employees that will probably use them to surf the Web which opens up a lot of possibilities to attack the machine itself. This is, in a way, *game over* situation in which attacker can do whatever he/she likes.

The third attack can prevent business owner from operating and can degrade him to the mode where it only issues ZKI, not JIR. The additional problem with this type of attack is that it manifests itself indirectly (e.g. error message failed to establish connection) and business owner can not know that he is actually under the DoS attack.

To conclude, malicious individuals are a very serious threat and to protect themselves from this attacks business owners have to have properly maintained machines as well trained stuff. Unfortunately, in a situation in which business owners, for whatever reason, try to save as much as possible it is highly likely they will not invest in security. Additionally, they don't have a habit of maintaining machines. What TA has to do, it has to educate business owners and warn them about threats they face.

C. Crime organizations

Crime organizations have enough resources to attack potentially many business owners and their primary goal is a financial gain. Basically, what they can do is attack many business owners simultaneously and for that purpose they have same attack vectors at their disposal as individual attackers. But, additionally, they have one more attack vector and that is malicious software specifically tailored for this purpose. The problem with such approach, i.e. tailored malicious software, is that standard antivirus software is lot less efficient and this poses a significant problem.

Additionally, it is possible to attack TA's servers via some innocent clients and in that way to hide real attacker. This is viable threat under the assumption that there is some implementation error in TA's server, as we further discuss in the Section V.

D. Activist groups

Activist groups, like Anonymous, are attacking for the primary purpose of publicity, not financial gains. Thus, attacking a single business owner doesn't give them sufficient pay offs. It is more likely they will try to attack TAs servers with the primary goal of causing disruptions to the service.

This is actually very real threat because it is relatively cheap to by services from some bot owner and do prolonged DDoS attacks on the TA's servers themselves.

V. IMPLEMENTATION BASED PROBLEMS

In the previous analyses we assumed that the implementations are perfect, both on the client side as well as on the server side, i.e. TA's servers. Unfortunately, it is very likely that there will be many errors, especially on the client side as there are a number of different implementations done by people that don't usually do security related protocols. In this section we are going to list some of the potential problems that might arise from different mistakes done by implementors, but in general this is open to further research.

The first and foremost question is whether clients require https connection to server and do they correctly check server's certificate. If either of those isn't fulfilled, then MITM attack is possible. At minimum, an attacker that successfully intercepts communication channel can see messages between client and server and in that way confidentiality of the business owner is violated. The next thing the attacker can achieve is to disrupt communication, either by not forwarding messages or by modifying them. Note that we assume that modifications will be detected by server or client, depending who's receiving them.

There is also question about covert channels which are very dangerous as they allow information leak. In the extreme, it would allow someone to deduce TA's secret key which would be the ultimate attack on this whole system. Note that attacks on TA's servers are supposedly protected by having each business owner sign an agreement with TA/FINA. But, this doesn't preclude some attacker from compromising business owner's machine and performing attacks using it as a proxy.

Many other potential problems here exists, like proper XML processing, schema validation, etc. To conclude, there are many potential dangers here and this is a topic for further research.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we presented initial analysis of a fiscal system introduced by Republic of Croatia's Tax Administration. It is only a partial analysis, based on publicly available information, which doesn't include testings on live systems due to being illegal by the new Criminal law in Croatia. Also, we assumed that the implementations are perfect, i.e. there are no software bugs.

The finding is that on the server side the system is relatively well protected. On the client side, the things are quite different. This is Achilles' heel of the whole system. We think that by introducing this whole fiscal system, without warning and proper education of business owners many of them are brought into a dangerous situation. It is the truth that it is the consequence of irresponsible behavior of individuals, which don't care about security, but it is also a Government's irresponsible behavior that neglects the other side. So, some actions have to be taken here.

There is also a weaknesses in the control part of the system are, the one that forces business owners to issue receipts, and as usual, the weakness is on the humans. Namely, it is questionable how much customers will be willing to type JIR or ZKI to check the receipt. Furthermore, it is mandatory that TA's inspectors be properly educated and equipped.

During the threat analysis we identified two technical weaknesses. First, there is possibility to reuse JIR's by manipulation

the date and sum on receipts. That one is very hard to prevent without rigorous controls, which are infeasible. The second weakness is ZKI, which by itself is useless. There is no way for TA's inspectors to *prove* it has a correct without having private key, which by definition they are not allowed to have!

Fortunately, this systems uses a lot of advanced technology, primarily cryptography, which many people don't know much about, and this for the time being acts as a barrier for more frauds.

As for the future work, we think that the main research should be done on live systems to identify weaknesses they have. More specifically, it is our intention to build a proxy that would automatically test certain implementation for correctness. Next, a motive for attackers is not elaborate enough, but this requires financial along with technical knowledge. Finally, we think that the introduction of advanced statistical analyses on TAs servers might help in detecting some manipulations described here, i.e. in order to spot strange behavior in the registration process. But, this is a topic for a further research.

REFERENCES

- [1] "Odluka o proglašenju Zakona o fiskalizaciji u prometu gotovinom (in Croatian)," Nov. 2012. [Online]. Available: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2822.html
- [2] "Financial agency," last checked: February 6th, 2013. [Online]. Available: <http://www.fina.hr/Default.aspx?sec=1134>
- [3] "Fiskalizacija - Tehnička specifikacija za korisnike - Verzija 1.2 (in Croatian)," Dec. 2012. [Online]. Available: http://www.porezna-uprava.hr/fiskalizacija/dokumenti/Fiskalizacija%20-%20Tehnicka%20specifikacija%20za%20korisnike_v1.2.pdf
- [4] "Web application for invoice checking," last checked: February 6th, 2013. [Online]. Available: <http://www.provjeri-racun.hr/provjeraracuna>

Analiza bezpieczeństwa systemu rejestracji i weryfikacji paragonów w Chorwacji

Stjepan Groš
University of Zagreb, Faculty of Electrical and Computing Engineering,
Unska 3, 10000 Zagreb, Croatia
E-Mail: stjepan.gros@fer.hr

Abstrakt – W 2013 roku w Chorwacji weszło w życie prawo, które wymaga od właścicieli restauracji, kawiarni i tym podobnych działalności operujących gotówką rejestracji paragonów na serwerze Administracji Podatkowej przed wydaniem ich klientowi. Aby zaimplementować nowe prawo chorwacka firma informatyczna APIS-IT opracowała protokół oparty na XML, SOAP i kryptograficznym kluczu publicznym. Zaimplementowany również został system operacji na serwerze. Powszechnie wiadomo, że opracowywanie protokołów, a w szczególności protokołów bezpieczeństwa jest bardzo problematyczne, zdarza się, iż nawet specjaliści od bezpieczeństwa popełniają błędy. Niniejsze opracowanie opisuje analizę bezpieczeństwa rejestracji paragonów, komponenty systemu jak również jego implementację. Należy zwrócić uwagę, iż jest to jedynie częściowa analiza, oparta na informacjach ogólnie dostępnych, nie obejmuje ona testów na funkcjonującym systemie gdyż jest to niezgodne z chorwackim prawem. Zidentyfikowane zostały dwa słabe punkty w istniejącym systemie. Głównym problemem jest fakt, iż wielu właścicieli biznesów jest zagrożonych atakami i nic nie zostało zrobione aby temu zapobiec. Jest to szerszy problem ponieważ przy stale rosnącej liczbie usług internetowych nie są podejmowane żadne działania w celu zwiększenie świadomości ludzi w sprawach bezpieczeństwa.

I. Wstęp

W 2013 roku w Chorwacji weszło w życie prawo, które wymaga od właścicieli restauracji, kawiarni i tym podobnych działalności operujących gotówką do rejestracji paragonów na serwerze Administracji Podatkowej przed wydaniem ich klientowi. Aby zaimplementować nowe prawo chorwacka firma informatyczna APIS-IT opracowała protokół oparty na XML, SOAP i kryptograficznym kluczu publicznym. Zaimplementowany również został system operacji na serwerze. Powszechnie wiadomo, że opracowywanie protokołów, a w szczególności protokołów bezpieczeństwa jest bardzo problematyczne, zdarza się, iż nawet specjaliści od bezpieczeństwa popełniają błędy. Niniejsze opracowanie opisuje analizę bezpieczeństwa rejestracji paragonów, komponenty systemu jak również jego implementację.

Artykuł podzielony został na 6 sekcji. W sekcji II przedstawiamy umotywowanie dla wprowadzenia systemu rejestracji paragonów. Prezentujemy również wgląd w jego architekturę i protokoły używane do komunikacji. Na końcu podajemy przegląd elementów

sterujących używanych do ochrony systemu przed oszustwami. Następnie w sekcji III podajemy model zagrożenia, tj. model, w którym przeanalizowane zostało bezpieczeństwo systemu. W Sekcji IV podane zostały przykłady różnych ataków na system, które umożliwiły *czynnikom zagrożenia* obejść kontrolę i uzyskać przewagę. Analiza ta została przeprowadzona przy założeniu „*perfekcyjnej implementacji*”, co oznacza brak błędów w konfiguracji i implementacji. W sekcji V przyglądamy się problemom, które mogą zaistnieć w przypadku błędów lub niedopatrzeń w procesie wdrażania. Opracowanie kończy sekcja VI, w której podajemy wnioski, zalecenia i kierunek dalszych prac.

II. System objęty analizą bezpieczeństwa

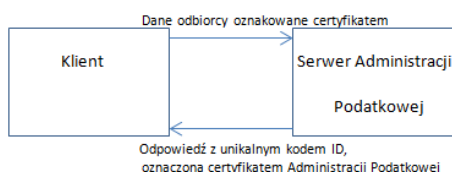
System Fiskalny opracowany został w celu zapobiegania manipulacjom paragonami, które dokonywane były przez nieuczciwe podmioty gospodarcze. Istotom problemu był fakt, iż paragony nie były wystawiane, lub były usuwane z kas fiskalnych ponieważ były one przechowywane jedynie lokalnie. Istniały pewne mechanizmy kontroli np. klient mógł wysłać numer paragonu do Administracji Podatkowej, która weryfikowała czy dany paragon został w rzeczywistości zgłoszony. Administracja Podatkowa mogła kontrolować zarówno przedsiębiorcę jak i klienta, z uwagi na fakt, iż klient był prawnie zobligowany do wzięcia paragonu. Mechanizm ten był jednak nieefektywny. Klienci nie rejestrowali paragonów, a nawet jeśli, Administracja Podatkowa miała problemy z weryfikacją zgłoszonych paragonów z uwagi na fakt różnych sposobów ich wykazywania. Ponadto wymagało to ogromu pracy fizycznej, co sprawiało, iż kontrole były drogie i nieefektywne.

W związku z tym *System Fiskalny* zobligowany został do realizacji następujących celów:

- Rejestracji każdego paragonu na serwerach Administracji Podatkowej w chwili gdy paragon zostaje wystawiony. Ma to na celu zapobieżenie manipulacjom i zagwarantowanie integralności i autentyczności.
- Ujednolicenie schematu numerowania paragonu co umożliwi łatwiejszą i zautomatyzowaną ich kontrolę.

Należy zwrócić uwagę, iż kontrole przeprowadzane przez Administrację Podatkową są nadal konieczne w celu egzekwowania wystawiania paragonów. Co więcej, z powodu ograniczenia środków kontroli w postaci inspektorów klienci nadal zachęceni są do wysyłania numerów paragonów do Administracji Podatkowej. Zachętą dla klientów są różnego rodzaju nagrody, które mogą wygrać rejestrując paragon. W oparciu o te wymagania opracowano odpowiednią architekturę wraz z protokołami. Zasadniczo architektura *Systemu Fiskalnego* jest relatywnie prosta. Składa się ona z dwóch podmiotów: lokalnego urzędu wysyłającego dane i serwera Systemu Fiskalnego, który przyjmuje i archiwizuje paragon, po czym wysyła oznaczone potwierdzenie (rys. 1).

Wiadomości są wymieniane przy użyciu SOAP przez HTTPS, podczas gdy dane są serializowane są w formacie XML. Aby zapewnić autentyczność i integralność wiadomości zastosowano publiczny klucz kartograficzny. Każdy podmiot w tym systemie otrzymuje certyfikat wydawany przez Agencję Finansową (FINA) [2], która działa jako Rządowy Urząd Certyfikacji. Wiadomości są oznaczane przed wysłaniem a oznaczenie to jest generowane zgodnie ze specyfikacją XML Security. Aby zapewnić poufność i integralność wiadomości podczas przesyłania używana jest obsługa protokołu SSL / TLS.



Rys. 1 Architektura systemu fiskalnego

Zdefiniowanych zostało 6 wiadomości:

- Żądanie/reakcja na żądanie – rejestracja paragonu w Administracji Podatkowej
- Żądanie/reakcja na żądanie – rejestracja lokalizacji
- Żądanie/reakcja na żądanie – komunikat echo używany do testowania dostępności serwera

Rejestracja lokalizacji jest prawdopodobnie wykorzystywana w dwóch celach. Po pierwsze aby poinformować Administrację Podatkową gdzie paragon został wystawiony oraz aby uniemożliwić wystawienie paragonu w innej lokalizacji.

Spośród powyższych wiadomości przeanalizujemy jedynie pierwszą parę używaną do rejestracji paragonów w Administracji Podatkowej. Przed przekazaniem klientowi każdy wystawiany paragon musi zostać wysłany do Administracji Podatkowej w celu nadania unikalnego numeru ID. W niniejszym opracowaniu użyte zostaną skróty, i tak JIR odnosi się do unikalnego numeru ID, tak jest on oznaczany w stosownej dokumentacji. Przykładowy nr JIR: *6b7749c6-56c1-4cf5-b7f7-9f29cebc9f7f*

Jest to standardowy format UUID. Wraz z JIR każdy paragon posiada kod zabezpieczający wystawiającego, dla którego zastosowano skrót ZKI, tak jak w chorwackiej dokumentacji. Kod ten jest połączeniem: OIB, znacznika czasu, identyfikatora paragonu, identyfikatora lokalizacji, identyfikatora kasy fiskalnej, kwoty całkowitej. Następnie jest on oznaczany, a w ostatnim etapie wyciągany zostaje MD5 z danych oznaczenia. Należy zwrócić uwagę, iż ZKI generowany jest przez kasę fiskalną, bez ingerencji serwera Administracji Podatkowej. Przykład ZKI: *a1e6b1428f0cc755f0c82aa7a1327e35*

Wprowadzenie powyżej opisanego kodu motywowane jest ochroną podmiotu wystawiającego przed ingerencją strony trzeciej [3]. W przypadku gdy wystawiający nie ma łączności z Administracją Podatkową może użyć tego kodu zamiast JIR.

Istnieją dwa elementy kontroli, które zmuszają przedsiębiorców do prawidłowego wystawiania paragonów:

1. Klient ma możliwość sprawdzenia danych paragonu w Administracji Podatkowej
2. Bezpośrednia kontrola Inspektorów Administracji Podatkowej

Klienci są prawnie zobligowani do pobrania paragonu. Mogą oni sprawdzić JIR poprzez rejestrację kodu na stronie Administracji Skarbowej lub wysyłając go poprzez wiadomość SMS. Dzięki temu przedsiębiorcy zmuszeni są do wystawiania paragonów, zapobiega to również fałszowaniu kodów JIR. Ponadto inspektorzy stanowią potencjalną kontrolę dla obu podmiotów - przedsiębiorców, którzy prawnie zobligowani są do wystawiania paragonów jak również klientów, którzy prawnie zobligowani są do ich pobierania. W rzeczywistości jednak liczba inspektorów jest niewystarczająca, a ich wiedza niedostateczna. Klienci natomiast zazwyczaj nie pobierają paragonów. Sprawia to, że mechanizmy kontroli funkcjonują słabo.

Klienci mogą zweryfikować paragon poprzez SMS lub korzystając z aplikacji internetowej [4] opracowanej specjalnie do tego celu. W obu przypadkach klient wysyła następujące dane:

- JIR lub ZKI
- Data i godzina wystawienia paragonu
- Całkowita kwota

Jeśli wprowadzone dane są prawidłowe, a Administracja Skarbowa zarejestruje dane paragonu aplikacja prześle informację, iż paragon jest poprawny. Jeśli Administracja nie odnajdzie paragonu w bazie danych wyśle informację do klienta aby spróbował ponownie później. Z powodu długości kodu JIR i ZKI kontrola jest nieefektywna. Wysyłanie długiego kodu, zwłaszcza przez SMS jest problematyczne, a częste pomyłki zniechęcają klientów do kolejnych prób rejestracji paragonu. Jest jednak jeden interesujący fakt. Kod ZKI jest trudniejszy do odczytu ale krótszy, w przeciwieństwie do kodu JIR, który jest dłuższy ale łatwiejszy do przepisania. Można więc założyć, iż klienci chętniej wpisywać będą kod ZKI, pomimo, że ilość cyfr i liter jest taka sama, a jedyną różnicą są myślniki.

III. Model Zagrożenia

Pierwszym etapem jest opracowanie modelu zagrożenia, tj. takiego modelu, który definiuje źródła i powiązane z nimi zagrożenia, które mogą mieć wpływ na funkcjonowanie systemu.

Źródła zagrożeń poddane analizie:

- Przedsiębiorcy próbujący uniknąć płacenia podatków poprzez manipulowanie wystawianiem paragonów, tak jak miało to miejsce dotychczas.

- Osoby fizyczne i zorganizowane grupy przestępcze próbujące czerpać korzyści finansowe.
- Grupy polityczne i organizacje takie jak np. *Anonymous* próbujące obalić system dla celów PRu.

Przedsiębiorcy mają motywację do manipulacji w systemie w postaci uniknięcia podatków. Nadrzędnym celem jest uniknięcie sytuacji, w których rejestrowane są mniejsze sumy niż w rzeczywistości występowały. Sytuacja taka może być rezultatem dwóch nadużyć: (i) nie wystawienie paragonów, (ii) wystawianie zmanipulowanych paragonów. Ponieważ nie wystawianie paragonów nie jest ujęte w analizie bezpieczeństwa systemu punkt ten zostaje pominięty. Analiza skupia się na przedsiębiorcach manipulujących paragonami. Pominięte zostaną również kwestie nietechniczne, takie jak oszustwa przy użyciu fałszywych paragonów. Zakładamy również, iż przedsiębiorcy mają pełną kontrolę nad kasami fiskalnymi, zarówno sprzętem jak i oprogramowaniem.

Należy zauważyć, iż przedsiębiorstwa różnią się wielkością co wpływa na ich topologię sieci i kontrole, które wdrażają. Analizie poddane zostaną małe firmy takie jak restauracje, kawiarnie, bary itp. Niewątpliwie kasa fiskalna musi być podłączona do Internetu z uwagi na konieczność łączenia się z serwerami Administracji Podatkowej. Niektóre z nich mają bezpośredni dostęp do Internetu (poprzez publiczny adres IP), wiele jednak uruchamianych jest poprzez system Windows, co naraża je na dodatkowe zagrożenia takie jak np. malware. Ponadto właściciele oferują klientom dostęp do Internetu poprzez tą samą sieć LAN, której używają do komunikacji z Administracją Podatkową. Łączność ta ma wpływ na ilość potencjalnych hakerów, których podzieliśmy na dwie kategorie, w zależności od motywów ataku.

Pierwsza kategoria obejmuje osoby fizyczne i organizacje. Różnicę stanowi ilość zasobów dostępnych do przeprowadzenia ataku. Niewątpliwie osoby fizyczne dysponują bardziej ograniczonymi zasobami niż organizacje przestępcze. Co za tym idzie, osoba fizyczna może próbować przeprowadzić ataki jedynie na kilka kas fiskalnych, podczas gdy organizacja przestępcza może zaatakować dowolną ich ilość.

Drugą grupę stanowią organizacje polityczne, które nie są zainteresowane o tyle zyskami finansowymi o ile wydarzeniami na tle PRu, takimi jak np. ataki *DoS* – „*odmowa dostępu*”.

W niniejszym opracowaniu przyjmujemy zasadę „*perfekcyjnej implementacji*”, która zakłada brak błędów programowania zarówno po stronie klienta jak i serwera. Na końcu opracowania wyszczególnione zostały błędy, które mogły zostać popełnione przez programistów i co one oznaczają w kontekście potencjalnego ataku. Jest to jednak temat do oddzielnych badań.

IV. Ataki

A. Ataki dokonywane przez przedsiębiorców

Jak wykazane zostało w Sekcji II istnieją dwa mechanizmy kontroli paragonów wystawianych przez przedsiębiorców – klienci i inspektorzy. Klienci nie mogą uzyskać dostępu do kasy fiskalnej w celu weryfikacji poprawności wystawianego paragonu, do czego w pewnym stopniu uprawnieni są inspektorzy. Poniższe przykłady przedstawiają możliwości wygenerowania przez przedsiębiorcę nieprawidłowego paragonu, jednocześnie unikając zgłoszenia tego faktu do Administracji Podatkowej przez klienta.

- Przedsiębiorca generuje jedynie kod ZKI, następnie obserwuje czy klient pobiera paragon. Jeśli klient pobierze paragon przedsiębiorca rejestruje go w Administracji Podatkowej, w przeciwnym wypadku usuwa go z systemu. ZKI jest kodem losowym, nie ma możliwości weryfikacji jego poprawności ani przez klienta ani przez Administrację Podatkową. Co za tym idzie, jeśli Administracja Podatkowa otrzyma paragon jedynie z kodem ZKI nie jest w stanie zweryfikować przedsiębiorcy, który go wystawił. W przypadku weryfikacji takiego paragonu przez Internet lub SMS wielu przedsiębiorców może koordynować generowanie paragonów z takim samym kodem ZKI, kwotą, datą i godziną. Alternatywnie mogą ponownie wykorzystać ten sam paragon. Należy zwrócić uwagę, iż jest to relatywnie proste aby nakłonić klienta do użycia kodu ZKI zamiast JIR. Wystarczy jedynie wydrukować kilka przypadkowych kodów JIR. Podczas rejestrowania przez klienta kodu JIR wystąpi błąd, co w rezultacie skłoni klienta do użycia kodu ZKI.
- Metoda, którą Administracja Podatkowa stosuje do kontroli paragonów pozostawia możliwość ponownego wykorzystania kodu JIR. Paragon wystawiony przez przedsiębiorcę rejestrowany jest na serwerze Administracji Podatkowej. Kody JIR i ZKI z tego paragonu mogą zostać ponownie wykorzystane dla innego paragonu opiewającego na taką samą kwotę. Jest jedynie pewne ograniczenie czasowe.
- Zarówno kod JIR jak i ZKI są wpisywane podczas gdy paragon jest weryfikowany. Oznacza to, że nie muszą one być skorelowane. Innymi słowy, można wpisać kody JIR i ZKI należące do innych paragonów. W obecnej chwili wątpliwe jest czy stwarza to możliwość uniknięcia rejestracji paragonu w Administracji Podatkowej.

Należy pamiętać, iż w przypadku wystawiania wielu paragonów z takim samym kodem JIR i ZKI trzeba zachować ostrożność przy wystawianiu faktur, gdyż muszą one zachować sekwencję numeracji.

Kontrola inspektora Administracji podatkowej w niewielkim stopniu komplikuje procedurę. Taktyka nr 1 z powyższej listy niesie za sobą największe ryzyko, ponieważ opiera się na założeniu, że paragony nie są porównywane. Jeśli jednak inspektor Administracji podatkowej

porówna kilka paragonów i stwierdzi, iż kody JIR i ZKI na jakichkolwiek dwóch się pokrywają, oczywistym będzie fakt, iż przedsiębiorca próbował obejść system. Zasadnicza różnica pomiędzy klientem a inspektorem jest taka, iż ten drugi może w pewnym stopniu kontrolować kasę fiskalną.

Mogą wystąpić następujące sytuacje:

- Inspektor przychodząc z dużą ilością paragonów prosi przedsiębiorcę o udostępnienie rejestrów w kasie fiskalnej. Jeśli istnieją paragony z takimi samymi kodami JIR i ZKI wówczas przedsiębiorca musi bardzo uważać który z nich pokaże inspektorowi. W rezultacie inspektor nie ma możliwości wykrycia oszustwa, chyba że dysponuje przynajmniej dwoma paragonami z takimi samymi kodami JIR i ZKI.
- W przypadku paragonów, na których ponownie wykorzystano kody JIR lub ZKI, inspektor może zauważyć, że istnieje pewna rozbieżność między datami na paragonach a faktycznym czasem ich wystawienia. Nie ma jednak wymogu synchronizacji czasu w rejestrach kas fiskalnych.
- Specyfikacja systemu podatkowego określa, że Administracja Podatkowa może poprosić właściciela firmy o odtworzenie (lub przywrócenie) kodu ZKI. Jednak bardzo trudno jest zweryfikować czy kod ZKI został wygenerowany przy użyciu właściwych danych, a co ważniejsze właściwego certyfikatu.

Podsumowując, bez inspekcji ze strony Administracji Podatkowej przedsiębiorcy mają możliwości manipulacji, chociaż nie jest to tak łatwe jak wcześniej. To w jakim stopniu można dokonać podobnych manipulacji jest przedmiotem dalszych badań, szczególnie w przypadku zmywy przedsiębiorców.

B. Ataki ze strony wrogich jednostek

Wrogie jednostki (osoby) mają wystarczającą ilość zasobów aby zaatakować jeden lub co najwyżej kilka kas fiskalnych. Ponowna analiza rys. 1 dobitnie pokazuje, iż jednostki są o wiele większym zagrożeniem dla przedsiębiorców niż dla Administracji Podatkowej.

Potencjalne motywy ich działania:

- Szkodzenie konkurencji poprzez manipulowanie ich paragonami co może spowodować nałożenie kar przez Administrację Podatkową
- Ponowne wykorzystywanie tych samych paragonów bez konieczności ich rejestracji
- Śledzenie poczynąń konkurencji
- Własnej satysfakcja

Aby zaatakować właściciela firmy i jego kasę fiskalną jednostka musi:

- Mieć dostęp do kanału komunikacji, tj. Próbować przeprowadzić ataki typu man-in-the-middle.
- Próbować uzyskać dostęp do rejestru kasy fiskalnej aby przejąć tajny klucz należący do właściciela firmy
- Przeprowadzić atak typu „*odmowa dostępu*” na połączenie internetowe i / lub rejestr kasy

Kanał komunikacji chroniony jest przy użyciu HTTPS, więc w przypadku braku błędów w implementacji bardzo ciężko jest włamać się do tego kanału. Należy zauważyć, że dwa elementy mają tutaj ogromne znaczenie. Pierwszy polega na tym, że komunikacja odbywa się za pośrednictwem HTTPS (tzn. nie ma powrotu do HTTP), a po drugie, że kontrola certyfikatu jest poprawnie zaimplementowana. Jedynym sposobem w jaki atakujący może włamać się do kanału jest wykorzystanie błędów w implementacji. Ponieważ założyliśmy, że nie ma takowych nie stanowi to problemu. Ewentualność taka opisana została w sekcji V.

Drugi wektor ataku polega na wykorzystaniu urządzenia, czyli samej kasy fiskalnej. Głównym bonusem w tym przypadku jest kradzież tajnego klucza. W momencie gdy atakujący ma kontrolę nad urządzeniem jest już w zasadzie w posiadaniu klucza. Plik może mieć ochronę w postaci hasła, ale to hasło musi być gdzieś zapisane. Są różne metody ataku spośród których najbardziej niebezpieczny jest atak w oparciu o socjotechniki. Co ułatwia sprawę urządzenia są często stare, w złym stanie technicznym. Gdy są podłączone do Internetu pracownicy często używają ich do korzystania z sieci, co z kolei rodzi wiele możliwości ataku na to konkretne urządzenie. Jest to w pewnym sensie sytuacja bez wyjścia gdzie atakujący ma już w zasadzie wolną rękę.

Trzeci rodzaj ataku to uniemożliwienie przedsiębiorcy właściwego funkcjonowania firmy. Powoduje sytuację, w której przedsiębiorca będzie ograniczony jedynie do możliwości generowania kodu ZKI, bez możliwości generowania kodu JIR. Dodatkowym problemem związanym z tego typu atakami jest fakt, iż nie ma bezpośrednich symptomów. Pojawia się komunikat o przykładowej treści „*nie udało się nawiązać połączenia*”, a przedsiębiorca nie jest świadomy, że właśnie stał się ofiarą ataku DoS – „*odmowa dostępu*”.

Podsumowując, wrogie jednostki (osoby) stanowią bardzo poważne zagrożenie. Aby ochronić się przed nimi przedsiębiorcy muszą pilnować aby sprzęt był w dobrej kondycji technicznej, a personel odpowiednio przeszkolony. Niestety, w sytuacjach gdy przedsiębiorcy szukają oszczędności można stwierdzić z dużym prawdopodobieństwem, że nie będą oni inwestować w bezpieczeństwo. Ponadto nie mają oni nawyku utrzymywania urządzeń w dobrej kondycji technicznej. Rolą Administracji Podatkowej jest edukacja przedsiębiorców i uświadamianie ich z jakimi zagrożeniami przyjdzie im się zmierzyć.

C. Organizacje przestępcze

Organizacje przestępcze mają wystarczające środki aby dokonać potencjalnego ataku na wiele firm, a ich głównym celem są korzyści finansowe. Organizacje mają możliwość dokonać ataku na wiele biznesów jednocześnie wykorzystując do tego podobne metody jak w przypadku jednostek. Dysponują one jednak jeszcze jednym wektorem ataku w postaci złośliwego oprogramowania, specjalnie zaprojektowanego do tego celu. Zasadniczy problem polega na tym, iż środki ochrony w postaci oprogramowania antywirusowego nie są wystarczająco wydajne. Istnieje również możliwość dokonania ataku na serwery Administracji Podatkowej wykorzystując do tego celu nieświadomych klientów, jednocześnie skutecznie ukrywając atak. Przy założeniu, iż serwery Administracji Podatkowej mają błędy w implementacji może to stanowić realne zagrożenie. Kwestia ta zostanie omówiona w Sekcji V.

V. Problemy związane z implementacją

W poprzednich rozdziałach przyjmowaliśmy zasadę „perfekcyjnej implementacji” zarówno po stronie przedsiębiorcy jak również serwerów Administracji Podatkowej. Niestety występowanie błędów, szczególnie po stronie przedsiębiorcy, jest wysoce prawdopodobne z uwagi na fakt, iż implementacji dokonują osoby, które z reguły nie stosują protokołów bezpieczeństwa. W poniższym rozdziale przeanalizujemy niektóre potencjalne problemy, które mogą być wynikiem błędów w implementacji. Temat ten jednak wymaga dalszych badań.

Podstawową kwestią jest pytanie czy klient wymaga połączenia https z serwerem i czy poprawnie sprawdza certyfikat serwera. Jeśli jeden z powyższych warunków nie jest spełniony atak „*man-in-the-middle*” jest realny. W najlepszym wypadku atakujący uzyska jedynie wgląd w komunikację między klientem a serwerem naruszając w ten sposób poufność danych przedsiębiorcy. Kolejnym etapem może być zakłócenie komunikacji poprzez blokowanie lub modyfikację wiadomości. Zakładamy, że modyfikacje zostaną wychwycone albo przez serwer albo przez klienta, w zależności której strony będą dotyczyć.

Kolejna kwestia dotyczy kanałów ukrytych, które stanowią bardzo poważne zagrożenie w postaci przecieku informacji. W najgorszym wypadku tajny klucz serwerów Administracji Podatkowej mógłby zostać odczytany, co w rezultacie może doprowadzić do ostatecznego ataku na cały system. Serwery Administracji Podatkowej są rzekomo chronione poprzez umowę, którą każdy przedsiębiorca zawiera z TA / FINA. Istnieje jednak możliwość ataku przy wykorzystaniu komputera przedsiębiorcy jako serwera proxy.

Istnieje również wiele innych kwestii takich jak prawidłowe przetwarzanie XML, sprawdzanie poprawności schematu, itp. Podsumowując, istnieje wiele potencjalnych zagrożeń, jest to jednak temat do dalszych badań.

VI. Wnioski i dalsza praca

W tym opracowaniu przedstawiona została wstępna analiza systemu fiskalnego wprowadzonego przez Administrację Podatkową Republiki Chorwacji. Jest to jedynie częściowa analiza oparta na informacjach ogólnie dostępnych, nie obejmuje ona testów na funkcjonującym systemie gdyż jest to niezgodne z chorwackim prawem. Przyjęta została również zasada „*perfekcyjnej implementacji*” zakładająca brak błędów w oprogramowaniu.

Reasumując, po stronie serwera system jest relatywnie dobrze chroniony. Inaczej kwestia wygląda po stronie klienta. Jest to swego rodzaju „pięta Achillesowa” całego systemu. Uważamy, iż implementacja całego systemu bez odpowiedniego przeszkolenia i uświadomienia przedsiębiorców narazi wielu z nich na potencjalnie niebezpieczne sytuacje. Faktem jest, że winą obarczyć można nieodpowiedzialne zachowanie przedsiębiorców, którzy nie dbają o bezpieczeństwo w należyтым stopniu. Po części winą można również obarczyć Rząd, który nieodpowiedzialnie lekceważy drugą stronę. Powinny zostać podjęte pewne działania na tym polu. Częściową winą należy również obarczyć system kontroli i jak zwykle wina leży w czynniku ludzkim. Wątpliwe jest ilu klientów będzie chętnych do rejestrowania kodów JIR lub ZKI w celu sprawdzenia paragonu. Konieczne jest również odpowiednie przeszkolenie inspektorów Administracji Podatkowej. Podczas analizy zagrożeń zidentyfikowano dwie słabości techniczne.

Pierwsza to możliwość ponownego wykorzystania kodu JIR poprzez manipulację datą i kwotą na paragonie. Bardzo trudno jej zapobiec bez rygorystycznych kontroli, które są praktycznie niemożliwe.

Drugą stanowi kod ZKI, który sam w sobie jest bezużyteczny. Administracja Podatkowa nie ma możliwości weryfikacji jego poprawności bez tajnego klucza, którego z definicji posiadać nie może. Korzystnie system wykorzystuje nowoczesną technologię, przede wszystkim kartografię. Brak powszechnej wiedzy na ten temat, jak na razie, stanowi pewną barierę przed oszustwami.

Co do przyszłości pracy skupić należy się na funkcjonujących systemach i identyfikować ich słabości. Mówiąc precyzyjniej naszym celem jest zbudowanie serwera proxy, który automatycznie testować będzie poprawność pewnych implementacji. Działania hakerów nie są zbyt wysublimowane, wymagają jednak pewnej wiedzy i zasobów finansowych. Na koniec uważamy, iż wprowadzenie zaawansowanych analiz statystycznych na serwerach Administracji Podatkowej może pomóc w wykryciu niektórych manipulacji, takich jak np. podejrzane zachowania w procesie rejestracji. Jest to jednak temat do dalszych badań.

Materiaty źródtłowe

- [1] "Odluka o proglašenju Zakona o fiskalizaciji u prometu gotovinom (in Croatian)," Nov. 2012. [Online]. Available: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2822.html
- [2] "Financial agency," last checked: February 6th, 2013. [Online]. Available: <http://www.fina.hr/Default.aspx?sec=1134>
- [3] "Fiskalizacija - Tehnicka specifikacija za korisnike - ~ Verzija 1.2 (in Croatian)," Dec. 2012. [Online]. Available: http://www.poreznauprava.hr/fiskalizacija/dokumenti/Fiskalizacija%20%20Tehnicka%20specifikacija%20za%20korisnike_v1.2.pdf
- [4] "Web application for invoice checking," last checked: February 6th, 2013. [Online]. Available: <http://www.provjeri-racun.hr/provjeraracuna>