АНАЛИЗ НА РИСКОВЕТЕ В ОБМЕНА НА ФИСКАЛНИ ДАННИ ЧРЕЗ КАСОВИ АПАРАТИ

Ясен Танев[1], Мирослав Стефанов[2], Драгош-Каталини Барбу[3]
[1, 2]Университет по библиотекознание и информационни технологии
[3]National Institute for Research & Development in Informatics

Резюме: Данните за фискални трансакции в касовите бележки са основа за контрола на фиска в момента. За да могат да бъдат правилно анализирани, те трябва да съдържат идентичността на източника, криптирани при преноса и достъпни без възможност за промяна. Данните, съдържащи обобщени фискални данни за оборотите, реферират към първичните документи, създаващи тези задължения, като целостта на данните трябва да бъде гарантирана в дългосрочен аспект,и следваща принципите а интегритет, конфиденциалност и достъпност на целия обем от информация. Сегашния модел съдържа високо ниво на риск, който ще покажем, и ще предложим алтернатива чрез въвеждане на електронно подписани фискални документи.

Ключови думи: фискализация, данни, риск, защита.

Въведение

Системата за регистриране на приходи от данък добавена стойност (ДДС) от продажби в търговски обекти е посредством фискални устройства с фискална памет. Тези устройства съхраняват данните за продажба в детайли на електронната контролна лента, като към НАП се изпращат данни съдържащи обобщена информация в XML формат за оборотите по данъчни групи и начините на плащане за съответната продажба. Данните се съхраняват и изпращат чрез технология от 2006 г. (Наредба № Н-18 от 13.12.2006 г.)[1]. През последните 16 години многократните промени не вземат предвид променящата се среда и рисковете при съхранение и предаване на данни на ниво касов апарат и сървър на Националната агенция по приходите (НАП). Промените влияят на преносната среда и времето на обмен, но резултатът за достъпността до данните и употребата им за анализ е с голямо закъснение и с ниско ниво на контрол, с риск от компрометиране на данните при изпращача, по трасето и впоследствие – при получателя НАП. Тази статия ще разгледа рисковете за конфиденциалността, интегритета и достъпността на информацията за фискални задължения, възникнали при продажба на

стоки и услуги и регистрирани с касов апарат. На базата на анализа на риска ще предложим модел за защитено предаване в близко до реалното време и с ясна идентичност на получателя и изпращача.

Методология на изследването

Имайки предвид обекта на изследване – процесите и технологиите за предаване на фискални данни и рисковете, свързани с това, регламентирани от нормативни документи, част от националното законодателство, – избраната методика за изследване е базирана на качествения метод. Събраните данни са продукт на анализ на техническите изисквания към касовите апарати и на експертните дискусии, провеждани в НАП и Министерството на финансите. В анализа са включени доказателства за слабости в системата от публични източници, реферирящи към данни за пробив и теч на данни в контекста на фискалните данни.

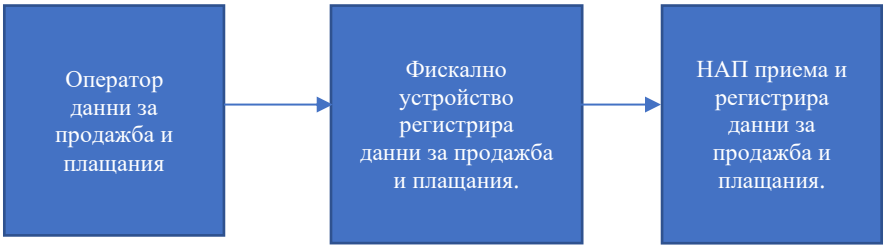
Резултати

Методологията за данъчен контрол при продажбите регистрира събития за плащане или издаване на фактура в търговските обекти, собственост на лицата по чл. 3 от Закона за ДДС[2]. Ако има настъпило плащане, различно от такова по банков път (чл. 3, ал. 1 от Наредба № Н-18), има задължение за издаване на фискален бон. Данните в бона са съгласно Приложение № 17 от Наредба № Н-18, т. 13, в XML формат и се предават НАП в рамките на 72 часа. Ако имаме документ тип фактура, се предават данни до 14-о число на месеца, последващ месеца на издаване, като данните са в текстов вид. Двете задължения се комбинират при състояния на едновременно настъпване. Фискалният контрол трябва да получи данните за продажбите по касови бележки и тези с фактури бързо, без риск от промяна, с възможност за обслужване на комуникациите с издателите и с гаранция за интегритета и съхранението на информацията. Изследването на процеса чрез използване на касови апарати и отчети за продажби на фактури ще бъде разгледан по-долу от технологична гледна точка, за да се идентифицират рисковете, като фокусът е върху предаването на касовите бележки.

Рискове при използване на касови апарати за издаване на касови бележки

Фискалното устройство само по себе си е устройство, което чрез клавиатура или по машинен интерфейс (RS2323, USB или TCP/IP

протоколи)[3] регистрира във временна памет данни за оборотите по начините на плащане и данъчните групи. В допълнение на тази функционалност записва пълнотекстов журнал с данните от касовите бележки, като ги разпечатва на хартиен носител или ги предоставя като текст. Данните се предават към сървърите на НАП до 72 часа в XML съобщения. Обобщени данни за оборотите се записват в края на деня в защитена FLASH памет съгласно изискванията на Наредба № Н-18 и отново се предават обобщено към НАП в XML структура. Моделът за сигурност на комуникацията между касовия апарат и НАП е базиран на идеята, че всяка продажба се регистрира и предава през защитена среда до НАП, което е допускане, но не е гаранция и последващите анализи на риска ще покажат пробив във веригата на доверие и висок риск от компрометиране, модификация и теч на данни.



Фиг. 1. Опростен модел за подаване на данни за плащания и обороти по данъчни групи, регистрирани през фискално устройство

Съвременната бизнес реалност променя този модел в доста по сложен, в който данните за плащане и продажби се въвеждат в потребителски софтуер (намясто или в облака), предават се по машинен интерфейс към фискалното устройство, то ги предава през защитена мобилна мрежа до мрежово устройство на мобилния оператор, а той – към сървъра на НАП за регистрация. Реалният модел на комуникация може да бъде видян на фиг. 2.

Фиг. 2. Реален модел за комуникация при предаване на данни за плащания и обороти по данъчни групи и използване на фискални устройства

Посочената на фиг. 2 архитектура на свързаност е идентифицирана чрез анализ на публичната документация за изискванията към касовите апарати, процедурите по сервиз и настройка на устройствата, участието ми като експерт в работните групи на НАП по въвеждане/отменяне на СУПТО, но и като част от екипа експерти, подготвящи проекта за въвеждане на алтернативен режим чрез онлайн касови апарати.

Твърдението на НАП за защитена и сигурна връзка по веригата софтуер – сървър с данни за продажби и касови апарати противоречи на факта, че тя бе доказано компрометирана на базата на следните примери от работата на агенцията:

- инициатива за въвеждане на контрол върху софтуерите за продажби СУПТО и генериране на уникален код на продажбата – добра концепция, но грешно управляван процес по идентифицирането на рисковете, което доведе до нейното отпадане;
- отказ на сървърите на НАП да приемат фискални данни поради липса на идентичност на изпращача и контрол над структурите с данни – 2019.03.16 (Доклад на НАП в работна група);
- отказ от обслужване на касовите апарати във верига бензиностанции поради получени команди за промяна на конфигурацията без контрол на идентичността на изпращача на командите за преконфигуриране – 3.2022 (Доклад на НАП в работна група);

- множество сигнали за работа на фискални устройства, които не са предали данни към сървърите на НАП повече от регламентираните 72 часа;
- възможност за използване на карта за мобилна комуникация на произволен доставчик на телекомуникационна услуга и свобода за конфигуриране на параметрите за връзка със сървъра на НАП (включително тестови такива, предоставени от НАП или частни компании).

След анализирането на фиг. 2, на изложените примери, събрани по време на оперативната ми работа като техник на фискални устройства и опита ми като участник в експертните групи на НАП, и като се има предвид липсата на криптиране или подписване на данните по целия им път, може да бъдат идентифицирани следните рискове, пряко свързани с активи и процеси, описани в таблица 1. За улеснение и краткост фискалното устройство ще бъде съкращавано като ФУ, а „софтуер“ ще бъде наричана всяка система, намираща се извън ФУ и предаваща данни за продажби и плащания към ФУ. Оценката на рисковете цели да покаже посоката, в която трябва да се развива наредбата, и освен практическия опит взема предвид и данните от доклада на OECD – Implementing Online Cash Registers: Benefits, Considerations and Guidance (OCR), провеждащ анализ и разглеждащ рисковете при класическите касови апарати (ECR).

Таблица 1. Реален модел на комуникация при предаване на данни за плащания и обороти по данъчни групи и използване на фискални устройства

№	Актив	Слабост в актива и възможност за компрометиране на данните	Стойност на риска, 1 – 10
1	Софтуер	Данните не се подписват от софтуера или производителя му, с което не може да се гарантира източникът.	8
2	Софтуер	Липсва сигурна идентичност на ФУ.	9
3	ФУ	Липсва сигурна идентичност на изпращача на данните.	8
4	ФУ	Липсва сигурна идентичност на сървъра на НАП.	10
5	Пренос на данни	Данните излизат от APN на телеком и влизат във VPN на НАП, като се предават некриптирани.	9
6	НАП	Липсва сигурна идентичност на ФУ.	10
7	НАП	Приема данни само от продавача.	8
8	Бизнес процес	Зависимост от връзка с облачна услуга, физически разположен касов апарат.	8
9	Бизнес процес	Зависимост от консумативи в касовия апарат и надеждност на физическата среда.	6

Предвид горните слабости може да се констатира, че сегашната технология и описаните нейни слабости не могат да гарантират автентичност и цялостност на данните за продажба поради липса на идентичност на изпращача, Гарантирана цялост на подадените данни също е заплашена поради липса на алгоритми за проверката и защитата и с което интегритета на информация е в риск не само от подмяната или модификация по пътя, но и изпращането и до крайни сървъри различни от тези на НАП поради липса на проверка на идентичността на получателя.

Слабостите са възможност за атака. Всяка една атака има своята вероятност и генерира риск.

Атаките и вероятностите в процеса по предаване на фискални данни с фискални устройства са представени в таблица 2.

Таблица 2. Реален модел за комуникация при предаване на данни за плащания и обороти по данъчни групи и използване на фискални устройства

№	**Актив**	**Вектор на атака**	**Вероятност**
1	Софтуер	Използване на слабости в софтуера и подмяна на компоненти	Висока
2	Софтуер	Човек по средата – подмяна на ФУ със симулатор	Средна
3	ФУ	Човек по средата – получаване на команди от нелегитимен софтуер	Средна
4	ФУ	Неполучаване на данни от софтуер	Средна
5	ФУ	Човек по средата – комуникация с нелегитимен данъчен сървър	Средна
6	Пренос на данни	Възможност за наблюдение, теч или модифициране на данни между APN и VPN	Ниска
7	НАП	Получаване на данни от симулатор на ФУ	Средна
7	НАП	Атаки отказ от обслужване	Средна
8	НАП	Подаване на грешни конфигурации	Ниска
9	Бизнес процес	Атака отказ от обслужване или компрометиране на физическа локация с ФУ	Средна

За да намалим риска и да гарантираме предаването на данни от фискални устройства, да подобрим бизнес средата и да гарантираме висока сигурност на данните с висока степен на доверие, е необходимо да предложим нов, алтернативен подход за комуникацията търговец – НАП.

Предложение за дискусия и прилагане на алтернативен подход при предаване на данни, свързани с данъчни събития, от данъчните субекти към НАП

Анализирайки предизвикателствата от т. 3, които може да бъдат обобщени с дефицит на конфиденциалността на данните, сигурната идентичност на обектите в процеса на обмен и възможността за работа в хибриден онлайн (облачен) или офлайн (без гарантирана свързаност) процес, предлагаме да се вземат предвид следните базови технологии и да се реализира следният оптимизиран процес:

1. Технологии:

А) идентифициране на субекта – подател на данъчните съобщения, с електронна идентификация (електронен сертификат);

Б) идентифициране на софтуера – софтуерен сертификат на производителя;

В) съхранение на ключовете и трансакциите в защитена памет тип Secure Memory device – secure storage и/или OFC Compliant[5];

Г) ясна идентичност на сървъра на НАП чрез електронен сертификат;

Д) схема за сигурен обмен на данни чрез комбинация от публични и частни ключове;

Е) разширяем модел на съдържанието на данни чрез обособяване на опционални секции в съобщението. Тези секции могат да бъдат със собствени структури, криптография и защита.

– получател;

– издател;

– публични;

– НАП;

Ж) цифрово подписани съобщения или такива с времево клеймо / timestamp което ще гарантира времето за възникване на транзакцията и ще предоставя опция за отложено, но задължително окончателно подписване.

2. Управление на риска и постигане на нов, оптимизиран модел чрез:

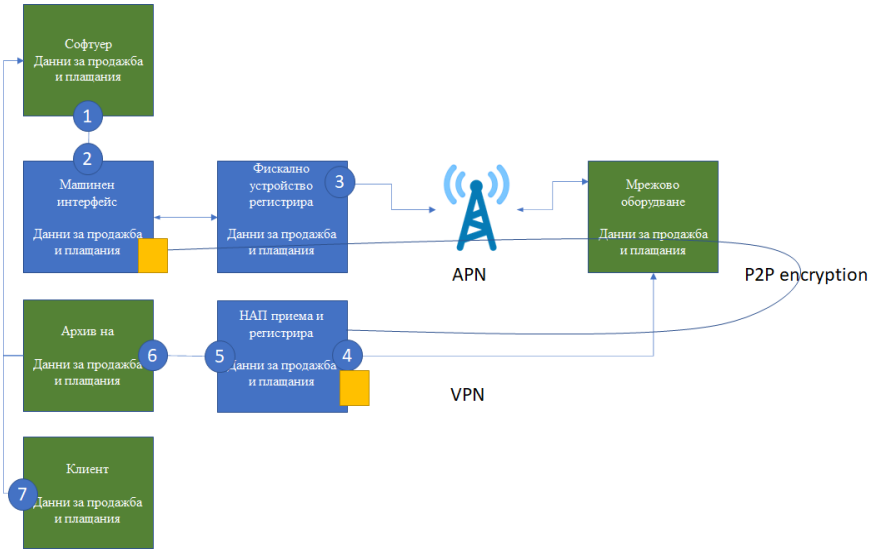
А) въвеждане на идентичност на всички участници;

Б) цифрово подписани съобщения във всеки от моментите на създаване или модифициране на съобщенията;

В) криптиране от точка до точка;

Г) добавена стойност на базовата услуга.

3. Обновен модел за обмен на данни чрез новата реализация е предложен на фиг. 3.



Фиг. 3. Модел за сигурно предаване на данни с ясна идентичност на участниците в процеса и добавена стойност за бизнес процеси

Разяснения:

- Софтуерът подписва всяко свое съобщение с частен ключ на производителя в т. 1 от процеса;
- Т. 2: ФУ, наричано в новия модел „виртуално данъчно устройство“, се представя и проверява идентичността на изпращача, за да гарантира приемане на валидни фискални данни;
- Т. 3: виртуалният данъчен терминал подписва данните и впоследствие ги криптира с публичен ключ на НАП, и проверява идентичността на сървъра 4, като в т. 4 данните се декриптират и се проверява идентичността на изпращача 3;
- Данните се записват в архив 6, като се проверява идентичността на подателя 5, изпращача 1 и подателя 3. Данните са достъпни за изпращача 1 и за потвърждение от изпращача 7, като в тях може да се съдържат и данни с добавена стойност за получателя 7, добавени от субектите в комуникацията, подписани с техните ключове и криптирани с публичния ключ на получателя 7;

- Ако изпращачът 3 не разполага със собствена инфраструктура за подписване, може да използва времево клеймо / timestamp за временно удостоверяване, да изпраща данните до сървъра 4 временно и впоследствие – окончателно, като ги подпише блоково между операции 4 и 5;
- Процесът по предаване на данни не е свързан с момента или начина на плащане, а с момента на възникване на данъчно задължение съгласно ЗДДС и е идентичен независимо дали става дума за фактура (идентифициран потребител с въведени данни) или документ за данъчно събитие на неидентифицирани крайни клиенти (отчет, протокол и др).

Изводи/Дискусия

Приложеният анализ на риска при обмен на данни за данъчни задължения в т. 3 и предложеният модел за оптимизация чрез въвеждане на съвременна криптографска технология, базирана на публични и частни ключове, както и промяната в бизнес процеса за регистриране и предаване на данни към НАП, като този момент не е свързан с момента и начина на плащане, а с настъпване на данъчни задължения и регистрацията им с документ. Тази промяна ще намали нивото на риск и създаде основа за допълнителни анализи на данните с употребата на техники за анализ на аномалиите [1], изграждане на графове на свързани трансакции [2] и повишено доверие в комуникацията бизнес – клиент, бизнес – бизнес и бизнес – държава.

Като допълнение към технологичните и бизнес предимствата от прилагането на иновативния подход, може да се вземе предвид прилагането на стандартите ISO 27001[6] и наредбата МИМИС.

Бъдещето на избрания подход е предизвикателство и за включването на нови технологии, предоставящи опция за децентрализация на журналите с данъчни събития и документите на базата на blockchain в P2P мрежа от фискални посредници и търговци. Въвеждането на фискалните посредници (както е приложено в Корея – доклад на OECD) за верифициране на данъчните документи ще намали разходите на данъчната администрация, ще ускори процеса по получаване на отговор за потвърждение, ще намали зависимостта на процеса от една точка (инфраструктурата на НАП) и ще предостави сигурност и доверие на оптимална цена. Ако данъчната администрация реши да предостави възможност за стимулиране на гражданите и бизнеса за активен контрол над обмена на фискални документи, то е възможно реализиране на държавна криптовалута със стойност върху данъчните документи.

Потенциалът за развитие на токенизираните и доверени записи без възможност за промяна (регистрирания данъчен документ) в комбинация със съвременните технологии ще даде възможност на държавата и бизнеса да реализират проекти, свързани с:

- вторична търговия на данъчни задължения чрез използването на NFT в контекста на уникален идентификатор на данъчния документ;
- портфейли с данъчни документи и референции към гаранционни карти, права за ползване и др.;
- лоялни програми и софтуери за управление на отношенията с клиентите;
- и др., като изследването в тази посока ще бъде задълбочено съвместно с представители на научната общност и представено в следващи доклади.

Данъчният риск нараства с ускоряването на бизнеса, глобализирането, технологиите, които го обезпечават, и скоростта на трансакциите в секунда, както и компенсирането на стойността на сделката с класически или иновативни модели за плащане.

Класическият модел за защита на фискалните данни е изчерпан. Време е да се приложи научен и системен подход, за да се изгради новата технологична фискална рамка. Ролята на университетската среда е да предложи модела. А задължение на държавата е да отвори дискусия за най-добрия и след обоснован избор да го предложи.

Бележки

[1] **Naredba** № N-18 ot 13.12.2006, https://www.tita.bg/laws/44
[Наредба № N-18 ot 13.12.2006, https://www.tita.bg/laws/44].

[2] **Zakon** za danak varhu dobavenata stoynost, v sila ot 01.01.2007 g., https://www.lex.bg/laws/ldoc/2135533201
[Закон за данъка върху добавената стойност в сила от 01.01.2007 г. https://www.lex.bg/laws/ldoc/2135533201].

[3] **EIA RS-464.** Electronic Industries Association. 1981 [December 1979]. p. insert. "Recommended Standards are adopted by EIA without regard to whether or not their adoption may involve patents on articles, materials, or processes. By such action, EIA does not assume liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Recommended Standard. This EIA Recommended Standard is considered to have international standardization implications, but there is no known IEC (or ISO) activity in this product area".

[4] **Implementing** Online Cash Registers: Benefits, Considerations and Guidance, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/implementing-online-cash-registers-benefits-considerations-and-guidance.pdf

[5] **OCF** Security Specification, https://openconnectivity.org/specs/OCF_Security_Specification.pdf.

[6] **Balgarski** institut po standartizatsia, https://bds-bg.org/bg/standartizatsiia_c27.
[Български институт по станртизация, https://bds-bg.org/bg/standartizatsiia_c27].

References/Литература
1. **Hilal**, Waleed, **Gadsden**, S. **Andrew**, **Yawney**, John. Financial Fraud. A Review of Anomaly Detection Techniques. Expert Systems with Applications. – In: *International Journal*, May 2022, Volume 193, Issue C, https://doi.org/10.1016/j.eswa.2021.116429
2. **Mao, Xuting, Sunc, Hao, Zhuc, Xiaoqian, Li, Jianping**. Financial fraud detection using the related-party transaction knowledge graph. – In: Procedia Computer Science, 2022, Volume 199, pp. 733 – 740.

За авторите

Ясен Танев е инженер с диплома от Техническия университет, София. Понастоящем е докторант в УниБИТ. Преподавател е по киберсигурност в УниБИТ и ПУ „Паисий Хилендарски“. Съавтор е на проекта за промени в ЗДДС, въвеждащ алтернативата за софтуерна фискализация. Председател е на Консултативния съвет по киберсигурност към БСК.

За контакт с автора: q.tanev@unibit.bg

Мирослав Стефанов е експерт по информационна и киберсигурност. Сертифициран инструктор за подготовка по курс СЕН. Докторант в УниБИТ и ПУ „Паисий Хилендарски“.

За контакт с автора: m.stefanov@unibit.bg

Драгош-Каталин Барбу е ръководител на облачните изчисления в Националния институт за изследвания и разработки в областта на информатиката. Бивш председател на Техническия комитет на специалистите (TCS), част от Технико-икономическия комитет (TCE) – държавен орган, който подпомага Министерството на комуникациите и информационното общество в процеса на разработване, наблюдение и изпълнение на държавната политика. Хоноруван преподавател към University of Bucharest, факултет „Математика и компютърни науки“.

За контакт с автора: dragos.barbu@ici.ro

ANALYSIS OF RISKS IN THE EXCHANGE OF FISCAL DATA THROUGH CASH REGISTERS

Yasen Tanev[1], Miroslav Stefanov[2], Dragoş-Cătălin Barbu[3]
[1, 2] University of Library Studies and Information Technologies
[3]National Institute for Research & Development in Informatics

Abstract: The data from fiscal transactions are the basis for the fiscal control nowadays. To be properly analyzed, they must contain the identity of the source, be encrypted during transmission and accessible without the possibility of modification. Data containing aggregated fiscal data on VAT refer to the primary documents creating these obligations, and the integrity of the data must be protected in the scope which include them too and the guaranty integrity, confidentiality and accessibility of the entire volume of information.

The current model contains a high level of risk, which we will be exposed and discussion regarding alternative considering electronically signed documents will be introduced.

Keywords: fiscalisation, data, risk, protection.

About the authors

Yasen Tanev is an engineer from the Technical University of Sofia. PhD student at ULSIT. Lecturer in Cyber Security at ULSIT and PU "Paisii Hilendarski". Co-author of the project for changes in the VAT Act introducing the alternative for software fiscalization. Chairman of the Cyber Security Advisory Board at BIA.

To contact the author: q.tanev@unibit.bg

Miroslav Stefanov is an information and Cyber Security Expert. Certified instructor for preparation for the SEN course. PhD student at ULSIT and PU "Paisii Hilendarski".

To contact the author: m.stefanov@unibit.bg

Dragos-Catalin Barbu is head of Cloud Computing at the National Institute for Research and Development in Informatics. Former Chairman of the Technical Committee of Specialists (TCS) – part of the Technical and Economic Committee (TCE), a government body that assists the Ministry of Communications and the Information Society in the process of developing, monitoring and implementing public policy. Part-time lecturer at the University of Bucharest, Faculty of Mathematics and Computer Science

To contact the author: dragos.barbu@ici.ro