به کارگیری سند PSD2 [1] و بهره‌مندی از منافع حاصل از آن

Applying the PSD2 and benefiting from its use

فائزه نیک بین، کارشناس برنامه‌ریزی شرکت مهندسی سیستم یاس ارغوانی، nikbin.f9009@gmail.com
Faezeh Nikbin, Planning expert in Yaas Arghavani System Engineering

چکیده

ظهور هر روندی که در هر نقطه از جهان، بی تردید موجب تغییر و نوآوری در کسب‌وکارهای آن صنعت خواهد شد. از این رو ضروری است تا با بررسی ابعاد روندهای فراگیر مانند PSD2، آمادگی لازم در مواجهه با نوآوری‌های برخاسته از آن فراهم شود تا بتوان از فرصت‌های حاصل از آن بهره مند شد. حوزه های اصلی که سند PSD2 بر آن تمرکز نموده است عبارتند از: توسعه و یکپارچه سازی بازار پرداخت اتحادیه اروپا، ایجاد نوآوری و رقابت میان بانک ها با استفاده از بازیگران جدید، بهبود امنیت و احراز هویت، امکان دسترسی به اطلاعات حساب و شفافیت در ارائه اطلاعات. ورود بازیگران جدید در حوزه پرداخت سبب باز تعریف روش رویارویی بانک‌ها با نوآوری‌ها و فناوری‌های نوین مالی و نیز ایجاد ساختار تعاملی جدید خواهد شد. چنانچه این ساختارها و چارچوب‌های جدید در صنعت پرداخت و بانکداری ایران پیاده‌سازی گردد، فرصت‌های ایجاد ارزش برای مشتریان، پذیرندگان و نیز افزایش مشتری و تراکنش برای بانک‌ها به ارمغان خواهد آمد. همچنین روش‌های نوین احراز هویت ارائه شده در سند PSD2 سبب شده تا این ساختار تعاملی جدید با الزامات و استانداردهای امنیتی انطباق یافته و نیز از تکنیک‌ها و فناوری‌های امنیتی نوین استفاده کند تا تعامل با نهادهای ثالث ارائه دهنده فناوری های نوین مالی در بستری امن به وقوع بپیوندد و از بروز تقلب و تخلف در پرداخت الکترونیکی جلوگیری به عمل آورد. این پژوهش با معرفی فرصت‌های حاصل از به گارگیری سند PSD2 به بررسی چارچوب‌های تعامل با ارائه‌دهندگان فناوری‌های نوین مالی در بستری امن خواهد پرداخت، بدین ترتیب صنعت پرداخت ایران قادر خواهد بود با به کارگیری آن همگام با دیگر کشورهای جهان از فرصت‌های پیش‌روی سند PSD2 بهره مند گردد.

واژگان کلیدی: سند PSD2، فناوری‌های نوین مالی، احراز هویت، بازیگران جدید صنعت پرداخت

[1] Payment System Directive

Abstract

The emergence of any process anywhere in the world will undoubtedly change and innovate in the business of that industry. Therefore, it is necessary to provide the necessary readiness to deal with the innovations that come from it by examining the dimensions of inclusive trends, such as PSD2, in order to benefit from the opportunities it has gained. The main areas that the PSD2 focuses on are: to develop and integrate the EU payment market, to innovate and compete among banks by using new actors, improve security and authentication, access to account information and transparency in providing information. The introduction of new player will redefine the way banks meet with innovations and new financial technologies, as well as create a new interactive structure. If these new structures and frameworks are implemented in the payment and banking industry of Iran, there will be opportunities for creating value for customers, merchant as well as increasing customer and transaction for banks. Also, the new authentication methods presented in the PSD2 have led the new interactive structure to be adapted to the requirements and standards of the security industry, as well as modern security techniques and technologies to interact with third-party providers of new financial technologies takes place in a safe place and prevents fraud and electronic payment violations. This study, with the introduction of the opportunities provided by the PSD2, will explore the framework for interaction with the providers of modern financial technologies in a safe environment, thus, the Iranian payment industry will be able to use it in synchronous with other countries The world will benefit from the development of the PSD2.

Key words: PSD2, new financial technologies, authentication, new players

.

مقدمه

روند کنونی ارائه خدمات بانکی به مشتریان نشان دهنده این است که انتظارات مشتریان در حال افزایش چشمگیری است و اتکای بانک بر خدمات کنونی دستاوردی جز نارضایتی و کاهش مشتریان را نخواهد داشت. برآورده نمودن انتظارات مشتریان مستلزم شکل گیری چشم اندازها و استراتژی های مقتضی توسط بانک و موسسات مالی می باشد. اما از یک سو بانکداری سنتی به علت نوع ساختار و حجم فعالیت های خود قادر به شناسایی و پاسخگویی کلیه نیازهای مشتریان نبوده و از سوی دیگر کسب و کارها و فناوری های جدید در حوزه مالی، با خدمات نوین و نوآوری خود نیازهای پیچیده و گسترده مشتریان را مرتفع کرده و همچنین تقاضاهای جدیدی برای مشتریان ایجاد کرده اند که ارائه این خدمات مستلزم اتصال به سامانه یکپارچه بانک می باشد. لذا چگونگی اتصال کسب و کارهای مالی نوین به سامانه های بانک و نیز بهره‌مندی بانک از نوآوری های این کسب و کارها چالشی است که نیازمند راه حلی جامع می باشد. این مهم از رهگذر تغییر در مدل های کسب و کار بانک و برآورده خواهد شد. از آن جا که مدل های کسب و کار جدید الگوهای تعامل و بازیگران فعال درعرصه مالی را دچار تحول می کند، نیاز است تا مقررات و دستورالعمل هایی تدوین شود تا پاسخگوی تحولات جدید باشد. در واکنش به این تحولات جدید، اتحادیه اروپا سند PSD2 را ارائه داده است تا به معرفی بازیگران جدید در حوزه پرداخت و نیز اصلاح دستورالعمل های موجود و تعریف مقررات جدید مرتبط با تعامل آن ها بپردازد. لازمه به کارگیری این سند تعریف چارچوب های مکمل اجرایی است که توسط دیگر فعالان این حوزه پیشنهاد شده است و در ادامه به شرح آن پرداخته خواهد شد. شناخت سند PSD2، بازیگران جدید حوزه پرداخت، مدل های کسب و کار جدید جهت بهره مندی از نوآوری های این بازیگران جدید و الگوهای تعامل بانک با این بازیگران جدید، مسائل حائز اهمیتی می باشد که بدون در نظر گرفتن آن ها برآورده نمودن انتظارت مشتری و رضایت آن ها حاصل نخواهد شد. هدف از انجام این پژوهش این است که صنعت بانکداری و پرداخت ایران قادر باشد همگام با سایر کشورها خود را با الگوهای جدید منطبق کند و از فرصت های حاصل از آن بهره مند گردد. به کارگیری این فرصت ها در نهایت، برای بانک ها سودآوری، برای کارآفرینان فرصت ایجاد کسب و کارهای جدید در حوزه پرداخت و برای مشتریان ارائه ارزش های جدید را به ارمغان خواهد آورد.

در این پژوهش ابتدا به بیان ادبیات موضوع پرداخته خواهد شد. از آن جا که اساس پژوهش حاضر یک دستورالعمل می باشد، اجرای آن مستلزم تحلیل و تفسیر مخاطبان این سند است لذا ضروری است تا رویکردهایی که در تحلیل این دستورالعمل به کارگرفته شده بیان گردد. همچنین بررسی و واکاوی اسناد و استانداردهایی که به عنوان مکمل این دستورالعمل ارائه شده اند نیز حائز اهمیت است که بخش مبانی نظری به این مهم پرداخته است. به دلیل اینکه به اعتقاد صاحبنظران PSD2، این دستورالعمل مختصات صنعت پرداخت را دچار تحول خواهد کرد، این پژوهش در پی یافتن فرصت هایی در این تحول است که صنعت پرداخت ایران را قادر می سازد تا از پتانسیل های موجود بهره‌مند گردد. همچنین این پژوهش به نحوه دستیابی به این فرصت ها نیز خواهد پرداخت.

ادبیات موضوع

در این بخش ابتدا به بررسی تحقیقات پیشین در حوزه PSD2 پرداخته خواهد شد و سپس مبانی نظری مرجع در این پژوهش بیان خواهد شد.

پیشینه تحقیق

از آن جا که از زمان ابلاغ سند PSD2 توسط اتحادیه اروپا تا نگارش این پژوهش زمان طولانی نمی گذرد، پژوهش های اندکی پیرامون این موضوع در سطح جهان انجام شده است. به دلیل گستردگی و حجم بالای این سند، دسته اول این پژوهش ها مربوط به معرفی حوزه های تحت پوشش سند PSD2 و نیز ترسیم چشم انداز فرصت های پیش روی این سند پرداخته اند. با توجه به اینکه سند PSD2 نسخه دوم سند PSD می باشد، خاستگاه و اهداف تدوین نسخه دوم این سند مورد توجه ویژه ای قرار گرفته است. از این روی در تحقیقات پیشین چنین عنوان شده است که اگرچه PSD1 به قانونمند کردن بازار واحد پرداخت اتحادیه اروپا پرداخته است اما نقش واسطی که کسب وکارهای نوآور در حوزه پرداخت (پرداخت کارتی، اینترنت، موبایل و..) ایفا می کنند را در نظر نگرفته و تعامل و دسترسی این کسب و کارها با عدم وجود قانون مواجه است. همچنین حضور کسب و کارهای جدید در پردازش های مالی و نیز دسترسی آن ها به اطلاعات مشتریان امنیت اطلاعات مشتریان را با خطر خواهد انداخت که خود نیازمند تعریف استانداردها و اجرای خط مشی های جدید امنیتی می باشد. لذا سند PSD2 بر آن شد تا این خلل را جبران کند و به جهت دستیابی به اهداف زیر تدوین گردید:

- توسعه و یکپارچه سازی بازار پرداخت اتحادیه اروپا
- ایجاد نوآوری و رقابت میان بانک ها با استفاده از بازیگران جدید
- بهبود امنیت و احراز هویت و حفاظت از اطلاعات کاربران
- امکان دسترسی به اطلاعات حساب
- شفافیت در ارائه اطلاعات [2]

در نهایت به کارگیری سند PSD2 برای مشتریان، شرکت های پرداخت و بانک منافع زیر را به همراه خواهد داشت:

- بانک: تعامل با محیط بیرونی و فعالیت در خارج از فضای بسته کنونی- تغییر در مدل کسب و کار و دستیابی به منافع حاصل از نوآوری های کسب و کارهای جدید- از آن جا که پرداخت درگاه ارائه خمت یا محصول به مشتری است، تجربه بهتر مشتری سبب افزایش فروش و بهره‌مندی بیشتر از کیف پول مشتری خواهد شد.- تعداد بیشتری از مشتریان به یک زیرساخت دسترسی دارند و در نتیجه یک پلتفرم برای بانک حاصل خواهد شد.

- کسب و کارهای پرداخت: دستیابی به یک رویکرد استراتژیک در تحول دیجیتال- تعریف محصولات جدید در حوزه پرداخت- دریافت نیازمندی های جدید مشتریان.

- مشتریان: سهولت و گزینه های بیشتر در انجام پرداخت- حفاظت و امنیت بالاتر اطلاعات- دریافت پیشنهادهای بیشتر از سایر خدمات و کسب و کارهای غیر پرداخت با توجه به نیاز خود.[3]

دسته دوم پژوهش های انجام شده در این حوزه نیز توسط شرکت هایی می باشد که به منظور به کارگیری سند PSD2،

به بانک ها و کسب و کارهای پرداخت راهکار پیشنهاد می دهد و با تعریف سرویس های جدید تعامل این دو بخش از صنعت پرداخت را تسهیل و ساختارمند می کند. از آن جا این پژوهش ها با رویکرد بهره‌مندی از پتانسیل و فرصت های تحول ناشی از اجرای PSD2 شکل گرفته اند، در بخش های بعدی به معرفی راهکارهای و ارزش های پیشنهادی این شرکت ها پرداخته خواهد شد.

مبانی نظری تحقیق

مفاد دستورالعمل PSD2

سند PSD2 مشتمل بر ۱۱۷ ماده است که در ۶ عنوان تنظیم شده است. هر عنوان از این سند متمرکز بر تنظیم مقرارت و دستورالعمل در یک حوزه خاص شده است. این عناوین شش‌گانه عبارتند از:

۱- یکپارچگی پرداخت در اتحادیه اروپا

۲- رجیستری شرکت ها پرداخت

۳- شفافیت در اطلاعات

۴- حقوق و امنیت در پرداخت

۵- سندهای تکمیلی برای جزئیات فنی

۶- مقررات بازبینی، گذار و اصلاحیه دستورالعمل

بخش اول این سند به بیان موضوعات اصلی و حوزه های تحت پوشش این سند می پردازد. همچنین حالت های سه گانه-ای را در معاملات ارزی منطقه اتحادیه اروپا در نظر می گیرد و قوانین مرتبط به هرکدام را بیان می دارد تا اتحادیه اروپا به یک بازار واحد و یکپارچه دست یابد. همچنین در این عنوان حوزه هایی که از مقررات PSD2 معاف می شوند نیز معرفی کرده است.

عنوان دوم که نقطه عطف این سند است، به مقررات دریافت مجوز نهادهای شخص ثالث یا TPP[۱] پرداخته است. در این بخش دو نوع لایسنس اصلی را برای خدمات پرداخت به نام AISP[۲] (ارئه دهنده خدمات اطلاعات حساب) و PISP[۳] (ارائه دهنده خدمات شروع پرداخت) معرفی کرده است که کسب و کارها می توانند مطابق مندرجات این سند مجوز ارائه این خدمات را دریافت کنند. این بخش از سند به شرح الزامات دسترسی به سیستم پرداخت و دسترسی به حساب می پردازد. در نهایت سند PSD2 تحت این عنوان دو نوع دسترسی و خدمات پرداخت را تعریف می کند.

از آن جا که این دستورالعمل بر آن است تا برای نهادهای شخص ثالث امکان دسترسی به اطلاعات حساب مشتریان و نیز انجام خدمات شروع پرداخت را فراهم کند نیاز است تا به پرداخت کننده و دریافت کننده اطلاعات کافی داده شود، لذا عنوان

---

[۱] Third Party Provider

[۲] Account Information Service Providers

[۳] Payment Initiation Service Providers

سوم از سند الزامات مرتبط با محتوا، زمان و هزینه اطلاعات منتقل شده توسط ارائه دهنده خدمات به کاربر را شرح می دهد.

عنوان چهارم از این دستورالعمل حقوق و وظایفی که ارائه دهندگان خدمات پرداخت در برابر کاربران به عهده دارند را به تفضیل بیان می دارد. این عنوان تضمین کننده حفاظت از مشتریان است از نقاط برجسته این سند می باشد. ۶ بخش اصلی در این عنوان عبارت است از: ۱)مفاد کلی، معرفی و شرح هزینه های قابل اعمال در این بخش. ۲) شرح شرایط و ضوابط دریافت مجوز انجام پرداخت و نیز نحوه رضایت و یا لغو رضایت کاربران جهت انجام تراکنش. ۳) الزامات مرتبط با نحوه انجام تراکنش، شامل: اعمال دستور پرداخت، برگشت مبلغ پرداخت، چگونگی منظور کردن مبلغ پرداخت از حساب پرداخت کننده به دریافت کننده، زمان انجام دستور پرداخت ۴) حفاظت از داده های شخصی کاربران در پردازش و نگهداری آن ها ۵) ریسک های عملیاتی و امنیتی و نحوه احراز هویت کاربران: احراز هویت قوی و چند عاملی کاربران، نحوه گزارش دهی رخدادهای امنیتی ۶) رویه های حل اختلاف میان کاربران و ذینفعان.

به دلیل اینکه این پیاده سازی این دستورالعمل به سند تکمیلی نیاز دارد تا در آن به شرح تفضیلی فنی بپردازد، در عنوان پنجم مقررات واگذاری وظیفه تنظیم استانداردهای فنی در احراز هویت بیان شده است. همچنین مقررات مرتبط با مطلع کردن کاربران از حقوق خود نیز در این عنوان بیان گردیده است.

در پایان نیز عنوان ششم به بیان مقررات نهایی جهت بازنگری و نیز زمان به کارگیری این سند پرداخته است چرا که این سند یک دستورالعمل جامع در اتحادیه اروپا می باشد که نیاز است کشورهای عضو مقررات خود را با آن منطبق کنند PSD2 این فرآیند را به عنوان گذار یاد کرده است. [4]

سند استاندارد فنی (RTS[1])

این سند که توسط مقامات بانکی اروپا (EBA[2]) تنظیم گردیده است، به بیان الزامات اجرایی امنیتی می پردازد. این سند در ۵ عنوان تنظیم شده است. که در بخش اول به بیان شرایط کلی احراز هویت و اعمال قوانین می پردازد و ۴ بخش بعدی عبارتند از:

(الف) اعمال روش احراز هویت قوی مشتری شامل: معرفی کد احراز هویت، طریقه اعمال و اتصال کد به صاحب حساب و مبلغ پرداخت، معرفی عناصر موجود در کد احراز هویت.

(ب) معافیت از به کارگیری الزامات امنیتی احراز هویت قوی مشتری که بر اساس سطح ریسک، مقدار تراکنش و کانال پرداخت تعیین می شود.

(ج) حافظت از محرمانگی و یکپارچگی مشخصات امنیتی هویتی کاربران خدمات پرداخت؛ شامل ایجاد و انتقال مشخصه ها، تجیهزات و نرم افزارهای احراز هویت، تمدید، لغو یا غیر فعال کردن مشخصه ها.

(د) ایجاد استانداردهای باز و امن برای ارتباط بین بانک، PISP، AISP، پرداخت کنندگان، دریافت کنندگان و سایر ارائه دهندگان خدمات پرداخت، در ارتباط با ارائه و استفاده از خدمات پرداخت. این بخش به بیان الزامات مرتبط با واسط های ارتباطی عمومی و اختصاصی می پردازد، همچنین مقررات مرتبط با امنیت تبادل داده میان بخش های ارتباطی را نیز بیان می

[1] Regulatory Technical Standards
[2] European Banking Authority

دارد. [5]

روش تحقیق

تحقیق حاضر از نظر هدف کاربردی و از حیث جمع آوری اطلاعات، توصیفی و از نوع تحلیلی می باشد. این پژوهش با استفاده از توصیف پژوهش ها و اسناد تکمیلی مرتبط با سند PSD2 به تحلیل و ارائه راهکار در به کارگیری این سند می پردازد و چالش ها و فرصت های حاصل از آن را مورد بررسی قرار می دهد. هدف از پژوهش حاضر بررسی تحولات ناشی از اجرای دستورالعمل PSD2 است و در جست و جوی یافتن پاسخ سوالات زیر است:

- تحولات اصلی ناشی از به کارگیری سند PSD2 چیست؟
- تعامل بانک با بازیگران و تازه واردان عرصه پرداخت چگونه خواهد بود؟
- فرصت های ایجاد ارزش ناشی از تعامل با بازیگران و تازه واردان عرصه پرداخت چیست؟
- تهدیدهای ناشی از حضور بازیگران و تازه واردان عرصه پرداخت چیست؟

به دلیل اینکه مدت زیادی از صدور اجرای این دستورالعمل در اتحادیه اروپا نمی گذرد، هنوز پیاده سازی این دستورالعمل به تجربه عملی دست نیافته است و کلیه پژوهش های انجام شده تا کنون نیز در مرحله ارائه راهکار پیشنهادی و ترسیم چشم انداز می باشد. همچنین به دلیل اینکه محدوده به کارگیری این سند اتحادیه اروپا می باشد، کشور ایران هنوز اقدامی در راستای بهره‌مندی از فرصت های آن ننموده و در جهت تعریف و اصلاح مقررات مورد نیاز الگوی جدید پرداخت نیز بررسی به عمل نیامده است. این امر دقت پژوهش حاضر را با محدودیت روبه رو نموده است. از این روی متن دستورالعمل PSD2 و نیز اسناد، چارچوب ها و استانداردهای مکمل آن به عنوان بخش اصلی پژوهش مورد بررسی قرار گرفت و به منظور یافتن فرصت های ایجاد ارزش حاصل از این دستورالعمل، راهکارهای ارائه شده توسط شرکت های ارائه دهنده سرویس و نیز مدل های کسب و کار بررسی شد. در پایان نیز به منظور افزایش دقت و صحت در یافته های پژوهش با تکیه بر روش تحقیق دلفی، پنلی از صاحب نظران این حوزه تشکیل شد و یافته های پژوهش از نقطه نظر آن ها مورد بررسی قرار گرفت. در نهایت نیز به منظور حصول اطمینان از پایایی داده ها نیز ضریب کاپا محاسبه گردید.

یافته ها و نتایج

معرفی نهادهای ارائه دهنده خدمات پرداخت شخص ثالث به عنوان بازیگران جدید صنعت پرداخت و نیز ارائه الزامات امنیتی جهت حفاظت از اطلاعات کاربران، اجزای اصلی دستورالعمل PSD2 می باشد که موجب تحول صنعت پرداخت خواهد شد. لذا در این بخش از پژوهش ابتدا به بیان فرصت های حاصل از ورود نهادهای شخص ثالث می پردازد. متعاقب باز شدن دسترسی شرکت های شخص ثالث به اطلاعات حساب مشتریان و نیز امکان شروع پرداخت توسط آن ها، انجام عملیات و نیز اطلاعات مشتریان با ریسک هایی مواجه خواهد شد، از این روی قسمت دوم این بخش به بیان تهدیدات اصلی ناشی از به کارگیری PSD2 می پردازد و به منظور کاهش و جلوگیری از بروز تهدیدات الزامات امنیتی مورد نیاز نیز معرفی خواهد شد. در پایان این بخش نیز چارچوبی جهت دسترسی نهادهای شخص ثالث به بانک ارائه خواهد شد.

بخش ۱: فرصت های حاصل از به گارگیری PSD2

واگذاری دو نوع از خدمات مهم بانک به نهادهای ثالث می تواند به تحول در مناسبات صنعت پرداخت منجر گردد. از

فعالیت های مهم AISP ارائه اطلاعات تلفیقی یک یا چند حساب پرداخت مختص یک کاربر است که در یک یا چند شرکت پرداخت (PSP[1]) دیگر نگهداری می شود. همچنین نحوه ارائه خدمات توسط PISP بدین طریق می باشد: ۱) شروع پرداخت با درخواست کاربر انجام می شود. ۲) این درخواست به یک حساب پرداخت در یک شرکت پرداخت (PSP) منظور می شود. ۳) دریافت کننده اطمینان حاصل می کند پرداخت شروع شده و بلافاصله به ارائه کالا و خدمات می پردازد.

بانک ها بنا به استراتژی های خود از نهادهای شخص ثالث استفاده می کنند و در نهایت با توجه به آن ها مدل کسب وکار و شرکای تجاری خود را انتخاب خواهند نمود. سطوح استفاده از نهادهای شخص ثالث عبارتند از:

۱- پشتیبانی از سرویس ها و استفاده عملیاتی؛ این سطح به چابکی فرآیندها و یکپارچگی معماری منجر خواهد شد.

۲- استفاده از ابزارها و تکنولوژی؛ مانند موبایل یا اینترنت اشیاء

۳- افزایش و جذب مشتریان جدید توسط دسترسی به کانال های نهادهای شخص ثالث

۴- نوآوری و ارائه سرویس جدید؛ از طریق پورتال توسعه دهندگان و همکاری با دیگری کسب و کارها

مدل های کسب و کار در تعامل با نهادهای شخص ثالث

تحول در قواعد و روابط حاکم بر صنعت پرداخت، منجر به تحول در مدل های کسب وکار خواهد شد. چرا که بانک ها با شرکای جدیدی در تعامل هستند و قادر خواهند بود تا محصولات و خدمات جدیدی را تعریف کنند و از رهگذر تعاملات جدید ارزش های جدیدی را ارائه دهند. لذا تحولات و منافع حاصل از اجرای سند PSD2 بیشتر از آنکه از تکنولوژی های جدید نشأت گرفته باشد، ناشی از تغییر در مدل کسب و کار می باشد. از همین روی در ادامه دو مدل کسب کار که در اجرای PSD2 به کارگرفته می شود معرفی خواهد شد.

۱- مدل اگریگیتور:

در این مدل بانک تبدیل به یک توزیع کننده محصولات و خدمات می شود. بنابراین بانک مجبور نیست هزینه تولید محصول با تطبیق را متحمل شود و بدین منظور از اکوسیستم شرکای خود استفاده می کند. همچنین بانک می تواند مشتریان را به دسترسی به طیف گسترده ای از محصولات ترغیب کند، بدین منظور نیاز است تا بانک به داده های مشتریان دسترسی داشته باشد تا بتواند به طور موثری به مشتریان توصیه کند و از طریق کانال مناسب آن را ارائه دهد. از ویژگی های مهم این مدل دسترسی به منابع داده ای می باشد. در این مدل بانک قادر خواهد بود با کسب و کارهای غیر مالی نیز همکاری کند، چرا که تحلیل داده های حساب مشتریان و تراکنش های آن ها می تواند برای کسب و کارهای غیر مالی منبع خوبی برای ارائه پیشنهاد متناسب به مشتری باشد. بنابراین دسترسی به اطلاعات حساب یا تراکنش های خرید می تواند فرصتی را برای تحلیل داده و پیرو آن ایجاد ارزش جدید فراهم کند.

۲- مدل پلتفرم:

بانک ها نیاز دارند تا کانال های توزیع خود را باز کنند. بدین منظور می بایست اثرات شبکه ای بیشتر شود و پلتفرم های جدیدی ایجاد شود، دارایی های زیادی باید به دست آورده شود و یکپارچگی عمودی شود. تفاوت این مدل با مدل اگریگیتور این است که یکپارچگی عمودی ایجاد می شود و سبب ارائه سریع و هموارتر می شود. اما در مدل اگریگیتور مسیر

[1] Payment Service Provider

طولانی و سلسه مراتبی از داده به سایر کسب و کارهای طی می شود. در مدل پلتفرم اکوسیستمی از توسعه دهندگان (از طریق پورتال توسعه دهندگان)، فین‌تک ها و کسب و کارهای نوین ایجاد شده که یا زنجیره تأمین جدیدی با مالکیت بانک پدید می آید و یا اینکه با ترکیب محصولات ارزش جدیدی ارائه گردد. [6] و [7]

سه مورد از ارزش هایی که بانک می تواند در تعامل با سایر کسب و کارها ارائه دهد عبارت است از:

پیشنهادات حمایتی:

- بانک ها می توانند از پیشنهاد وام به مشتریان دیگر صنایع بهره برند، مانند تبلیغات خودرو برای وام های خودرویی که قبلا ثبت شده است.
- موسسات آموزشی برای افرادی که وام دانشجویی دریافت می کنند و پیشنهاد املاک برای دریافت کنندگان وام مسکن. بازنشستگی، تعطیلات و سایر اتفاقات پر هزینه زندگی، فرصت هایی را برای خدمات بانکی فراهم می کند.

هدف گیری مشتری:

- توانایی هدف قرار دادن مشتریان خاص بانک را برای دیگر صنایع فراهم می کند. به طور مثال بانک یک دسترسی به کسب و کارهای محلی ارائه می دهد تا به مشتریان نزدیک محل خودپرداز بانک پیشنهاد دهد. به نحوی که زمانی که خودپرداز مشتری را در نزدیکی خود می یابد، کسب و کار آن منطقه می تواند یک پیشنهاد به او ارائه دهد.

داده به عنوان سرویس:

- بانک ها، به اطلاعات مالی مشتری که برای شرکت ها و دیگر صنایع ارزشمند است دسترسی دارند. بانک ها نه تنها داده های مشتریان، بلکه تحرکات بازار را نیز گردآوری می کند.
- دسترسی به چنین داده هایی، می تواند در استراتژی های ورود به بازار ارزشمند باشد، به طور خاص در محلی خاص از شهر که مشتریان هدف در آن جا زندگی می کنند. [8]

بخش ۲: تهدیدات و الزامات امنیتی در به کارگیری PSD2

به دلیل اینکه روندهای پرداخت بیشتر به سمت پرداخت با موبایل متمایل شده است و بسیاری از راهکارهایی که به پیاده سازی PSD2 می پردازند در بستر موبایل اجرا شده است، شناخت تهدیدات امنیتی در بستر موبایل از اهمیت ویژه ای برخوردار است.

الف) تهدیدات در پرداخت اینترنتی و پرداخت موبایلی: با وجودی که میان کانال های پرداخت اینترنتی و موبایلی ارتباط می باشد، رویکردها و ابزارهای آن ها متفاوت است. به دلایل زیر در کانال های پرداخت موبایل تقلب کمتری وجود دارد:

- حجم تراکنش های موبایلی از تراکنش های اینترنتی پایین تر است.
- کانال های موبایلی نیاز دارند تا کاربر در یک سرویس پرداخت در یک اپلیکیشن موبایلی ایجاد حساب کند و پروفایل کاربر و تاریخچه تراکنش ها در اپلیکیشن موبایل قابلیت مشاهده بیشتری دارد، در حالی که دسترسی به کانال های اینترنتی به سرویس های رجیستری وابسته است و میزان داده هایی کمتری در آن موجود می باشد.

- به دلیل اینکه محیط اینترنت مبتنی بر مرورگر می باشد، و کانال های موبایل از چندین کانال استفاده می کنند، نظیر گوشی، سیستم عامل، شبکه وایرلس، اپلیکیشن موبایل و مرورگر موبایل، تقلب موبایلی پیچیده تر و مشکل تر می باشد. علی رغم این پیچیدگی پرداخت موبایلی در معرض ریسک هایی چون بدافزار موبایل، اپلیکیشن جعلی، تقلب در کیف پول دیجیتال و تصاحب حساب[1] می باشد.

با توجه به رشد روزافزون پرداخت های موبایلی و تفاوت در کانال های آن ها، پذیرندگان می بایست تقلب را در تمام کانال های ردیابی کنند و میان روندهای تقلب شناخته شده در کانال های آنلاین و موبایلی تمایز قائل شوند.

حوزه های تهدید: تهدید هایی که پرداخت موبایلی را هدف قرار می دهد عموما در حوزه های زیر متمرکز شده اند:

تهدیدهای کاربران موبایل: نصب برنامه های مخرب و بدافزار، فیشینگ و مهندسی اجتماعی

تهدید دستگاه موبایل: دسترسی غیر مجاز، دستگاه مفقودی یا سرقت شده

تهدید اپلیکیشن پرداخت و کیف پول: مهندسی معکوس، دستکاری اپلیکیشن پرداخت و استفاده از روکیت

تهدید پذیرنده: بدافزار، حمله مرد میانی و حملات بازپخش

تهدیدهای ارائه دهندگان خدمات پرداخت و بانک پذیرنده: در معرض خطر قرار گرفتن سیستم پرداخت و اتصال داده ها

تهدید ارائه دهندگان شبکه پرداخت: در معرض خطر قرار گرفتن سرویس توکن و انکار سرویس

تهدید صادر کننده: در معرض خطر قرار گرفتن فرآیند ارائه مجوز، و داده های توکن

تهدید ارائه دهندگان اپلیکیشن پرداخت: در معرض خطر قرار گرفتن داده های حساس، در معرض خطر قرار گرفتن پروفایل کاربر در ابر، در معرض خطر قرار گرفتن توکن و انکار حمله های سرویس [9]

حوزه هایی که از منظر کارشناسان امنیت شامل ریسک های بزرگ عبارتند از:

ایجاد/ افتتاح حساب؛ فرآیند ایجاد حساب باید به صورت امن پیاده سازی سازی شود تا از تقلب تصاحب حساب جلوگیری شود. می بایست قابلیت های چندگانه دستگاه موبایل (شناسایی هویت، مکان جغرافیایی، بیومتریک و...) به کارگرفته شود، همچنین پیاده سازی KYC [2] ضروری می باشد. شرکت ها باید پروفایل مشتریان را نگهداری کنند تا با استفاده از الگو های شناسایی، قوانین و ماشین یادگیری، نمونه های تصاحب حساب را دریابند.

نفوذ در داده ها؛ مهاجمان به جای اینکه اطلاعات کارت را به دست آورند اطلاعات شخصی هویتی را سرقت می کنند. ارائه دهندگان راهکارهای امنیتی می بایست، روش هایی که آن ها می توانند این اطلاعات را به دست آورند را شناسایی کنند و از آن بروز آن جلوگیری کنند.

پذیرندگان کسب و کارهای کوچک؛ جلوگیری از تقلب را بخشی از کسب و کار خود نمی دانند و در آن سرمایه گذاری نمی کنند و تمایل دارند تا راهکارها را خریداری کنند یا به ارائه دهنده شخص ثالث برون سپاری کنند. بنابراین می بایست راهکارهایی توسعه یابند که آن ها هدف قرار داده و برای آن ها به صرفه باشد. [10]

روند روش های تقلب: روش های تقلبی که در سال ۲۰۱۸ رو به رشد اعلام شده است عبارت اند از:

- اپلیکیشن های مخرب: تحقیقات نشان می دهد که حداقل ۵۰ برنامه مخرب در گوگل پلی تا ۴ میلیون بار دانلود شدند و ۳۶ میلیون دستگاه را آلوده کرده اند.

[1] استفاده از اعتبارها و هویت سرقت شده جهت ایجاد حساب

[2] know your customer

- ربات حمله کننده: ربات ها به طور مداوم پیشرفت می کنند و با استاده از تکنولوژی های پیشرفته، کاربران قانونی و رفتار افراد را جعل می کنند تا به طور متقاعد کننده ای از دفاع سایبری و کنترل های تقلب عبور می کنند.
- شبیه سازها: مهاجمان نمونه یک اپلیکیشن را در دستگاه موبایل شبیه سازی شده اجرا می کنند تا با تقلید از کاربران قانونی در موبایل های واقعی حملات را انجام دهند.
- مهاجمان با هک کردن یک دستگاه کنترل آن را به دست گیرند تا حمله را انجام دهد. در واقع این حمله شامل یک دستگاه و اپلیکیشن قانونی است که بدون دانش کاربر انجام می شود. [11]

ب) الزامات امنیت اطلاعات

از آن جا که امنیت و حفاظت از اطلاعات کاربران از اهداف اصلی سند PSD2 می باشد این بخش به معرفی کلیه الزامات مورد جهت تأمین امنیت کاربران پرداخته شده است. کسب و کارهایی که در سطح جهان دستورالعمل های PSD2 را در راهکارهای خود به کار گرفته اند جهت تضمین حفظ امنیت کاربران به رعایت الزامات ۱ تا ۴ اشاره نموده اند. در پایان نیز یکی از استانداردهای امنیتی مرجع در ایران ذکر گردیده است. جهت هر گونه تبادل داده مربوط به مشتریان نیاز است تا الزامات امنیتی زیر اجرا گردد.

۱- PSD2- استانداردهای فنی در احراز هویت قوی مشتری (SCA[1])

از جمله موضوعاتی که در این دستورالعمل به آن پرداخته شده است الزامات احراز هویت قوی مشتری است که بر احراز هویت دوعاملی (انتخاب حداقل دو عامل از عناصر سه گانه زیر به عنوان عناصر مورد نیاز جهت احراز هویت کاربران) تأکید دارد و برای عامل ها را در دسته های زیر طبقه بندی می کند:

۱) عناصر احراز هویت قوی مشتری طبقه بندی شده به عنوان دانش (چیزی که فقط کاربر می داند)، مانند طول یا پیچیدگی، ۲) عناصر طبقه بندی شده به عنوان مالکیت (چیزی که تنها کاربر دارد): مانند مشخصات الگوریتم، طول کلید و آنتروپی اطلاعات، و ۳) دستگاه ها و نرم افزار های عناصر طبقه بندی شده به عنوان ویژگی وجودی (چیزی که کاربر می باشد): مانند مشخصات الگوریتم، سنسور بیومتریک و ویژگی های حفاظت قالب.

بنا به این استاندارد در تمامی دفعاتی که یک پرداخت کننده به حساب آنلاین خود دسترسی پیدا می کند، یک تراکنش پرداخت یا هر فعالیتی که از طریق یک کانال از راه دور اجرا می شود که در آن ریسک تقلب یا سایر سوء استفاده ها وجود دارد را انجام می دهد از کد احراز هویت استفاده می کند، کد احراز هویت باید تنها یکبار توسط PSP پذیرفته شود. کد احراز هویت باید دارای ارتباط پویا باشد به نحوی که مختص به میزان تراکنش بوده و دریافت کننده مشخص باشد. همچنین کدهای احراز هویت تا زمانی که الزامات امنیتی برآورده می شوند، باید براساس چنین راهکارهایی باشد: ایجاد و تأیید اعتبار پسورد یک بار مصرف، امضاهای دیجیتال یا سایر مدارک معتبر مبتنی بر رمزنگاری با استفاده از کلیدها و / یا مواد رمزنگاری ذخیره شده در عناصر احراز هویت.

این استاندارد همچنین بر حفظ محرمانگی و یکپارچگی اعتبارهای امنیتی شخصی تأکید دارد و بنا به آن رعایت الزامات امنیتی در تحویل، تجدید، لغو ضروری می باشد.

[1] Strong Customer Authentication

جهت بهبود اعتماد در تراکنش های اینترنتی، این استانداردهای فنی باید بین منافع افزایش امنیت در پرداخت های از راه دور و نیازهای کاربر پسندانه و قابلیت دسترسی تعادل برقرار کند. لذا در این استاندارد معافیت هایی برای احراز هویت در نظر گرفته شده است تا در راستای سهولت کاربران، در تراکنش های با ریسک پایین همه یا بخشی از الزامات احراز هویت شامل معافیت شود.

از آن جا که بنا به قوانین PSD2 سرویس های مالی گسترده ای از طریق ارائه دهندگان شخص ثالث ارائه می شود، به ایجاد ارتباط از طریق واسط هایی نیاز می باشد، بنابراین ضروری است تا در ارتباط میان دستگاه ها و برنامه ها الزامات مرتبط با واسط های ارتباطی، رابط های اختصاصی، امنیت بخش های ارتباطی برقرار شود.

۲- eIDAS- مقررات سرویس های اعتماد و شناسایی الکترونیکی

eIDAS مجموعه ای از استانداردها برای شناسایی هویت الکترونیک و الزامات سرویس اعتماد می باشد، شامل الزامات امنیتی ارائه دنده سرویس اعتماد، سازمان های نظارتی بر آن، سرویس های اعتماد واجد شرایط، امضای الکترونیکی، مهر الکترونیکی و اعتبار سنجی آن، برچسب زمانی و ... می باشد که این مقررات بر قابلیت همکاری و شفافیت تأکید دارد.

۳- GDPR- قوانین حفاظت از اطلاعات شخصی کاربران

این مقررات در مورد حفاظت از داده و محرمانگی آن ها باشد و شامل الزامات مرتبط با پردازش اطلاعات شخصی می باشد. بدین ترتیب فرآیندهای کسب و کار که اطلاعات شخصی را اداره می کنند باید مبتنی بر "حفاظت از اطلاعات از طریق طراحی و به طور پیش فرض باشد" به این معنی که اطلاعات شخصی باید با استفاده از مستعارسازی یا بی نام سازی ذخیره شود و حداکثر محرمانگی به طور پیش فرض در نظر گرفته شود.

۴- ایزو ۲۹۱۱۵ DIS- تکنیک های امنیتی در چارچوب تضمین احراز هویت موجودیت ها

این استاندارد که توسط سازمان استانداردسازی بین المللی (ایزو) تدوین شده است، احراز هویت را از دو بعد فنی و سازمانی مورد بررسی قرار می دهد. در بعد فنی با رویکردی فرآیندی الزامات احراز هویت را در سه مرحله بیان می دارد: ۱) ثبت نام (شامل اپلیکیشن و شروع، اثبات هویت، تأیید هویت، ثبت سوابق، رجیستر) ۲) مدیریت اعتبار (شامل ایجاد اعتبار، پیش فرآیند اعتبار، مقدار دهی اولیه اعتبار ، پیوند و ملزومات اعتبار، تضمین اعتبار، فعال سازی اعتبار، ذخیره سازی اعتبار، تعلیق و غیرفعال سازی اعتبار، تجدید یا تعویض اعتبار، ثبت سوابق) ۳) احراز هویت موجودیت (شامل احراز هویت، ثبت سوابق). از سویی دیگر این استاندادر به بررسی احراز هویت کلیه موجودیت ها می پرازد و مانند سایر استانداردها و دستورالعمل ها به احراز هویت افراد بسنده نکرده است و از آن جا که طی فرآیند احراز هویت ضروری است تا از اصالت دستگاه ها و اعتبارها نیز اطمینان حاصل شود، پرداختن به این استاندراد نیز حائز اهمیت می باشد. این استاندارد همچین سطوح چهارگانه ای را برای اطمینان مطرح می کند که می تواند برای احراز هویت در سطوح مختلف ریسک به کار گرفته شود.

۵- استانداردهای زیرساخت کلید عمومی (PKI[۱]) در گواهی های الکترونیکی در ایران

از آن جا که انتقال و ارسال اطلاعات شخصی و اعتبارهای امنیتی شخصی که در دستورالعمل PSD2 به آن اشاره شده است نیازمند رمزنگاری می باشد، لذا ضروری است تا ملزومات گواهی های الکترونیکی و ماژول ها و الگوریتم های رمزنگاری

[۱] Public Key Infrastructure

اطلاعات و اعتبارها مدنظر قرار گیرد. این استاندارد که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه، به عنوان متولی صدور گواهی الکترونیکی در ایران، تنظیم گردیده است، می تواند به عنوان یک استاندار پایه و بالا دستی موجب استاندارد سازی روند رمزنگاری اطلاعات در فرآیند احراز هویت گردد که استفاده از این استاندارد سبب یکپارچگی زیرساخت کلید عمومی در راهکارهای احراز هویت می گردد. این استاندارد ملی در چند بخش تنظیم گردیده است: ابتدا پروفایلی از گواهی های الکترونیکی را معرفی کرده و پیرو آن ملزومات مرتبط با پروفایل ها را بیان نموده است، مانند ملزومات گواهی های باطل شده و یا نام های متمایز کننده. در این سند سپس الگوریتم ها و مکانیزم های رمز نگاری مرفی شده است. همچنین پورتکل های رمزنگاری و ماژول های سخت افزاری رمزنگاری نیز از جمله مواردی است که این سند به آن پرداخته است. [1]

بلاک چین و PSD2

به دلیل اینکه یکی از چالش های حضور و ارائه خدمات توسط نهادهای شخص ثالث تازه وارد بودن آن ها در فضای کسب و کار پرداخت است، اعتماد به آن ها با مسئله حائز اهمیتی می باشد. توسعه فناوری های مبتنی بر بلاک چین در سال های اخیر می تواند، برای ذینفعان زنجیره ای از اعتماد به نهادهای شخص ثالث فراهم آورد. همچنین تنظیم مقررات مبتنی بر دستورالعمل PSD2 میان اجزایی که با هم در تعامل هستند، می تواند توسط قابلیت های بلاک چین قابل اجرا باشد.

بخش ۳: نحوه دسترسی نهاد های شخص ثالث در به کارگیری PSD2

باز شدن دسترسی به حساب های بانک نیازمند کانال دسترسی به اطلاعات بانکی می باشد. لازمه استفاده از این کانال نیز وجود بستر یکپارچه می باشد به نحوی که اتصال نهادهای شخص ثالث و بانک ها به این بستر فراهم گردد. CAPS[1] چارچوبی است که به پیشنهاد این بستر یکپارچه می پردازد. از اهداف چارچوب CAPS موارد زیر قابل ذکر می باشد:

- ارائه زیرساخت عملیاتی جهت اجرا و پیاده سازی PSD2
- ارائه فرآیند و تکنولوژی استاندارد شده به اجزای PSD2
- ایجاد بستر رقابت میان تازه واردان و فین تک ها و بانک ها
- با توجه به روش های روش های دسترسی مجزای AISP و PISP مانع از جزیره ای شدن و آشفتگی خواهد شد.

اجزای CAPS شامل سه جزء قبلی بانک، AISP ، PISP و یک جزء جدید به نام ارائه دهنده خدمات CAPS[2] می باشد. چارچوب CAPS دارای سه لایه متفاوت می باشد که استفاده از هر کدام سطحی از منافع و قابلیت ها را برای اجزای متصل به لایه فراهم می کند. این سه لایه به ترتیب قابلیت عبارتند از:

۱- لایه انطباق با PSD2:

- ارائه راهکار اتصال مرکزی برای هر نهاد ثالث و بانک که یک سرویس استاندارد ایجاد می کند.
- کاهش یا حذف نیاز به اتصال چدگانه
- ارائه دسترسی مورد نیاز نهادهای ثالث موجود و جدید برای ایجاد سرویس های جدید و نوآورانه به منظور منافع

[1] **Convenient Access to PSD2/Payment-related Services**

[2] CAPS SP

کاربران

- تعهدات قراردادی در این لایه وجود نخواهد داشت
- بانک می تواند از این لایه استفاده کند تا نیازمندی های دسترسی در PSD2 را انجام دهد.
- راهی برای محدود کردن بانک و نهاد ثالث در جهت مطلوبیت های اضافی تمهیدات خود وجود ندارد.
- استانداردهای فنی قانونی در این لایه ایجاد می شود.

۲- لایه چارچوب CAPS:

- نیاز به ثبت نام نهادهای ثالث در چارچوب استانداردی که بر اساس قوانین مندرج در PSD2 ایجاد شده و نیز افزودن جزئیات بیشتری به آن
- تعریف واضح قوانین کسب و کار و عملیاتی به منظور ترویج بهتر سرویس و اعتماد بیشتر کاربر
- پوشش دهی با سطوح مورد قرارداد در سرویس (SLA[1])، احزار هویت و حقوق ذینفعان
- باز بودن و ترویج مشارکت

۳- لایه CAPS پلاس:

- این لایه شامل سرویس های اضافه بر آن چیزی است که در PSD2 مشخص شده است و منجر به نوآوری می شود.
- ارائه دامنه گسترده تری برای سرویس های جدید، به جز حساب های پرداخت. مانند تأیید سن و آدرس
- سرویس های CAPS می تواند در همه بانک ها با یک الگو نباشد و خدمات مختلفی در بانک های مختلف ارئه شود.

وجود چندین ارائه دهنده خدمات CASP سبب وجود پویایی در دسترسی اجزای CAPS خواهد شد. از مزایای وجود ارائه دهندگان متعدد CAPS عبارتند از:

- امکان استفاده نهادهای ثالث از چند ارائه دهنده CAPS
- ارائه دهندگان CAPS به وسیله لایه انطباق PSD2 دارای خط مشی، واسط پایه و فرآیندهای مشابهی می باشند.
- ارائه دهندگان CAPS بر سطح سرویس، دسترسی، عملکرد و دیگر معیارهای کسب و کار رقابت می کنند.

قابلیت های چهارگانه ای که چارچوب CAPS ارائه می دهد شامل جعبه ابزار (انجمن توسعه دهندگان، محیط تست و..)، زیرساخت سرویس (چارچوب عملی انطباق)، زبان مشترک (ایجاد درک مشترک، ارائه استاندار مشترک در واسط های نرم افزاری، انتقال پیام و اطلاعات و...) [12]

[1] Service Level Agreement

جمع بندی

پژوهش حاضر در جستجوی منافع حاصل از پیاده سازی دستورالعمل PSD2 در صنعت پرداخت ایران است. از آن جا که این دستورالعمل در اتحادیه اروپا ارائه شده است، برخی از الزامات مندرج در آن ویژه آن منطقه می باشد؛ نظیر الزامات مرتبط با یکپارچگی ارز در معاملات صورت گرفته در اتحادیه اروپا. اما سایر الزامات مندرج در این سند خاستگاه عمومی دارد به تنظیم مقررات در حوزه هایی می پردازد که در صنعت پرداخت رواج یافته است اما با عدم یا نقص قانون مواجه است. حضور و فعالیت کسب و کارهای نوین که با فناوری های جدید و نوآوری خود (مانند فین‌تک ها) در صنعت پرداخت فعالیت می کنند، منجر به شکل گیری مناسبات جدیدی در صنعت پرداخت شده است. دستورالعمل PSD2 در پاسخ به حضور این کسب وکارها توسعه یافته است تا به تنظیم مقررات مرتبط با فعالیت بازیگران جدید صنعت پرداخت بپردازد. از آن جا که این کسب و کارها به دلیل شناخت نیازمندی های مشتریان و به کارگیری نوآوری قادر به سودآوری هستند، در صورتی که بانک بتواند از نوآروی های آن ها بهره مند گردد می تواند در سود حاصل از آن سهیم شود. اگرچه این خاستگاه در خارج از مرزهای ایران شکل گرفته است اما روندهای پیشین نشان می دهد که کسب و کارهای نوآور به سبب جذابیت، سودآوری و نیز برآورده نمودن نیازهای مشتریان، توسط کارآفرینان الگوبرداری شده و در ایران نیز توسعه می یابد. لذا ایجاد منفعت راهکارهای منطبق بر PSD2 از یک سوی و الگوبرداری از کسب و کارهای نوآوری توسط کارآفرینان ایرانی از سویی دیگر سبب شده است تا شناخت ابعاد دستورالعمل PSD2 و منافع حاصل از آن در صنعت پرداخت ایران نیز ضرورت یابد. اگرچه جهت اجرای راهکاری منطبق با این دستورالعمل، تنظیم قوانین ملی متناسب با آن در صنعت پرداخت ایران ضروری است اما بررسی مسائل حقوقی خارج از حوزه این پژوهش بوده و این پژوهش به شناخت فرصت ها و تهدیدهای ناشی از این دستورالعمل و نیز نحوه اجرای آن بسنده کرده است و پرداختن به مسائل قانونی مرتبط بر عهده مراجع ذیصلاح باقی خواهد ماند. یافته های این پژوهش نشان داد از مشخصه های مهم سند PSD2 حضور نهادهای شخص ثالث و دسترسی آن ها به اطلاعات حساب مشتریان در بانک و نیز اجرای خدمات شروع پرداخت توسط آن ها می باشد که این امر توسط اتصال و دسترسی به سامانه های بانکی فراهم می گردد. به دلیل اینکه نتیجه این اتصال می بایست برای بانک و نیز کسب و کارهای جدید سودآور باشد، ضروری است تا راه های ایجاد ارزش در این دسترسی ها شناخته شود و مدل های کسب و کار مبتنی بر ایجاد ارزش شکل گیرد. از همین روی این پژوهش به معرفی راه های ایجاد ارزش و نیز مدل های کسب و کار ناشی از به کارگیری PSD2 پرداخته است. از طرف دیگر ضروری تا نحوه دسترسی نهادهای شخص ثالث به بانک نیز مشخص گردد تا این کسب وکارها در چارچوبی ساختارمند و یکپارچه به بانک متصل شوند و از اتصال های از هم گسیخته جلوگیری به عمل آید، لذا در این پژوهش با معرفی چارچوبی به نام CAPS، نحوه اتصال نهادهای شخص ثالث به بانک نیز توصیف گردید. در نهایت به دلیل اینکه با باز شدن راه های اتصالی بانک به سمت کسب و کارهای جدید، سبب بروز ریسک و تهدید امنیتی بر اطلاعات حساس مشتریان خواهد شد. همچنین ابزارهای جدید دسترسی مانند موبایل نیز موجب بروز تهدیدهای امنیتی جدید شده است. در نتیجه در این پژوهش به معرفی تهدیدهای پیش روی اکوسیستم جدید پرداخت و نیز الزامات امنیتی جدید جهت مقابله با این تهدیدها پرداخته شد.

منابع

۱- معرفی استانداردهای زیرساخت کلید عمومی کشور، مرکز دولتی صدور گواهی الکترونیکی ریشه، ش. ۱/۰

۲- Moinian, Sh, Payment Services Directive2-Directive on Payment Services in the Internal Market "(EU) 2015/2366",Deutsche Bank (2016)

۳- Payments UK, The Second Payment Services Directive (PSD2) (2016)

۴- The European Parliament And The Council Of The European Union, Directive (EU) 2015/2366 Of The European Parliament And Of The Council, Official Journal of the European Union (2015)

۵- EBA,Draft Regulatory Technical Standards, on Strong Customer Authentication and common and secure, final report on draft rts on sca and csc (2017)

۶- Capgemini, Capgemini Open Banking Marketpace (2017)

۷- Capgemini, PSD2: An Open Banking Catalyst (2018)

۸- Oracle, PSD2 with Oracle API Platform Cloud Service (2017)

۹- Enisa, Security of Mobile Payments and Digital Wallets (2016)

10- Federal Reserve Bank Of Boston, Mitigating Fraud Risk in the Card-Not-Present Environment (2016)

11- SecuredTouch- Predictions for the mobile payment fraud landscape (2018)

12- CAPS, White Paper on CAPS Services (2016)