بانک توسعه صادرات ایران

شرایط و الزامات امنیتی مشتریان جهت استفاده از بانکداری باز

ماده 1- تعاریف

1-کاربر نهایی :

مشتری بانک توسعه صادرات ایران است که متقاضی استفاده از خدمات ریالی ، ارزی و اعتباری در قالب بانکداری باز می باشد.

2-نهاد ثالث :

نهادی است واسط بین ارائه کننده بستر بانکداری باز و مشتری بانک (کاربر نهایی) که از طریق Applicationهای خود، خدمات بانکداری باز را در اختیار کاربران نهایی قرار می دهد. مانند توسعه دهندگان نرم افزارهای اداری ، مالی ، سازمانی و ...

تبصره مهم : آندسته از مشتریانی که خود تامین کننده نرم افزارهای سازمانی و مالی مورد استفاده می باشند نهاد ثالث به شمار می آیند.

به موجب این پیوست، صیانت و حفظ امنیت اطلاعات بستر بانکداری باز شامل عدم افشای اطلاعات طبقه‌بندی شده و رعایت شرایط، حدود، مالکیت، محدودیت‌ها و جزئیات اطلاعاتی که از جانب بانک یا کاربر نهایی به منظور ارائه خدمات یا امور محوله در اختیار نهاد ثالث قرار داده می‌شود، بر عهده نهاد ثالث خواهد بود.

3- عناصر احراز هویت:

مطابق PSD2 Specification تمامی بانک‌ها بایستی برای تمامی تراکنش‌هایی که به صورت remote یا proximity بر روی هر کانالی انجام میشود SCA[1]را پیاده سازی نمایند. مطابق SCA سیستم احراز هویت بایستی مبتنی بر دو یا چند روش از انواع زیر باشد. این روش‌ها بایستی به صورت مستقل از همدیگر پیاده سازی شوند تا دانستن یکی منجر به لو رفتن دیگری نشود:

- دانش (Knowledge) مانند پسورد، شماره ملی، PIN Code
- دارایی (Possession) مانند توکن، گوشی موبایل، Smart card
- ذات (Inherence) مانند اثر انگشت و عنبیه.

4- مدارک امنیتی شخصی(Personalized Security Credentials):

می تواند شامل هر یک از عناصر احراز هویت باشد

5- داده های شخصی امنیتی:

مهر و امضای مجاز مشتری (کاربر نهایی)	مهر و امضای نهاد ثالث

می تواند شامل اطلاعات پروفایل مشتری مانند نام، آدرس، شماره موبایل و همچنین اطلاعات رمزها و تاریخچه تراکنش‌های آن باشد.

6- مجوز دسترسی (Access Token):

بر اساس راه‌حل‌هایی مانند ایجاد و اعتبارسنجی one-time password، امضاهای دیجیتال یا سایر روش‌های رمزنگاری پایه با استفاده از کلیدها و یا مواد رمزنگاری ذخیره شده در عناصر احراز هویت تولید می‌شود تا جایی که نیازمندی‌های امنیتی تأمین شوند.

ماده 2- الزامات امنیتی ارتباط با بستر بانکداری باز

1- نهاد ثالث موظف است تمامی استانداردها و مسائل امنیتی لازم را برای حفظ امنیت هر نوع سامانه‌ای که برای دسترسی به خدمات بانکداری باز ذیل این قرارداد مورد استفاده قرار می‌گیرد، پیاده‌سازی کند.

2- با توجه به اینکه بالاترین دسترسی به انجام خدمات مالی از جمله رؤیت صورت‌حساب، ایجاد دستور پرداخت و انجام عملیات مالی از طریق سرویس‌های بانکداری باز در اختیار راهبر کنسول بستر بانکداری باز است، لذا به نهاد ثالث توصیه می‌شود پیش از فعال‌سازی خدمات، فردی امین و مورد اعتماد را به عنوان راهبر کنسول سامانه بانکداری باز انتخاب نماید.

3- از آنجاییکه با دسترسی به کلیدهای رمزنگاری و مجوزهای مربوطه، امکان دسترسی به خدمات بستر بانکداری باز فراهم می‌شود، لذا در صورتیکه بطور عمدی یا غیرعمدی این اطلاعات افشا شود و یا در اختیار افراد غیر مجاز قرار گیرد، مسئولیت جبران زیان مالی یا غیرمالی وارده به فرادیس گستر، بانک و یا کاربر نهایی، با نهاد ثالث می باشد.

4- مسئولیت حفظ و نگهداری مدارک امنیتی که بستر بانکداری باز در اختیار نهاد ثالث قرار می دهد و هر گونه سوء استفاده از آنها، با نهاد ثالث می باشد.

5- نهاد ثالث موظف است هر گونه رخداد امنیتی را به فرادیس گستر اعلام نماید.

ماده 3- الزامات مدارک امنیتی و ابزارهای سخت‌افزاری یا نرم افزاری لینک شده به مدارک امنیتی

1- نهاد ثالث باید محرمانگی و یکپارچگی مدارک امنیتی شخصی کاربر نهایی و مجوز دسترسی را در تمام مراحل احراز هویت شامل نمایش، انتقال و ذخیره تضمین کند. به همین منظور، نهاد ثالث باید الزامات زیر را تضمین نماید:

مهر و امضای مجاز مشتری (کاربر نهایی)	مهر و امضای نهاد ثالث

- مدارک امنیتی شخصی موقع نمایش پنهان شده هستند و هنگام وارد شدن توسط کاربر نهایی در طول احراز هویت به طور کامل قابل خواندن نیستند.
- مدارک امنیتی شخصی، بصورت ساده و بدون رمزنگاری ذخیره نمی شوند.

2- نهاد ثالث باید تضمین کند که پردازش و هدایت داده های شخصی امنیتی و مجوز دسترسی های تولید شده، در محیطی امن و طبق استانداردهای شناخته شده و قوی انجام شود.

3- نهاد ثالث باید وجود محیطی امن برای چرخه عمر مدارک امنیتی شخصی (ایجاد، تخصیص، نگهداری و امحاء) را تضمین نماید.

4- نهاد ثالث باید تضمین کند که کاربر نهایی از طریق ابزارهای سخت‌افزاری یا نرم افزاری احراز هویت، فقط به مدارک امنیتی شخصی خود دسترسی امن دارد.

5- اجرای اقدامات لازم جهت کاهش مخاطرهٔ آشکار شدن عناصر احراز هویتی به وسیله نرم‌افزار و یا تجهیزات مربوطه

6- نهاد ثالث باید تضمین کند که مشتری برای تجدید و فعالسازی مجدد مدارک امنیتی شخصی، روال ایجاد، انتصاب و تحویل مدارک و دستگاه های احراز هویت را مجدداً طی کند.

7- نهاد ثالث باید تضمین نماید که امکان حذف، غیرفعالسازی یا لغو مدارک امنیتی شخصی، ابزارهای سخت‌افزاری یا نرم افزاری احراز هویت، بصورت امن فراهم می‌باشد.

8- نهاد ثالث باید تضمین نماید، هنگامی که ابزارهای سخت‌افزاری یا نرم افزاری احراز هویت قابل استفاده مجدد را توزیع می‌کند، قبل از ارائه آن به کاربر نهای دیگر، امکان استفاده مجدد امن از ابزارهای مذکور فراهم شده باشد.

ماده 4- Certificate ها و مجوزها

1- نهاد ثالث برای تعیین هویت، باید جهت رمزنگاری های الکترونیکی و یا احراز هویت وب سایت خود، به Certificateهای معتبر تکیه نموده و از صحت گواهی TLS سرورهای تحت مدیریت خود بصورت دوره ای اطمینان حاصل کند.

2- نهاد ثالث پس از دریافت مجوز دسترسی باید اطلاعات مورد نیاز را برداشته و سپس کاربر را به آدرسی که در آن هیچ اطلاعات حساسی وجود نداشته باشد هدایت نماید.

مهر و امضای مجاز مشتری (کاربر نهایی)	مهر و امضای نهاد ثالث

3- درصورتی‌که پارامترهایی به دست نهاد ثالث رسید که برای آن تعریف نشده یا نامفهوم یا نامعتبر هست، باید آن‌ها را کاملاً نادیده گرفته و از آن‌ها استفاده نکند. مثلاً اگر نوع مجوز دسترسی برای نهاد ثالث قابل‌قبول یا مفهوم نیست نباید آن مجوز را دریافت کند.

4- نهاد ثالث باید برای مقابله با هر گونه حمله، اعتبار مقادیر دریافتی را مورد ارزیابی قرار دهد.

5- نهاد ثالث باید همه فرآیندها، ابزارها و تکنیک‌های مدیریت ریسک و مدیریت تقلب را به کار گیرد.

6- نهاد ثالث باید نگهداری امن مجوزها را تضمین نماید و از هرگونه انتقال مجوز بپرهیزد. (مسئولیت هرگونه سوءاستفاده از مجوزها در صورت افشای آنها به عهده نهاد ثالث است)

7- نهاد ثالث باید کل فرایند مربوط به رمزنگاری اطلاعات حساس کاربران خود را مستند کرده و ارائه نماید.

ماده 5- الزامات مانیتورینگ

1- برای پیاده سازی معیارهای امنیتی، نهاد ثالث باید مکانیزمهای مانیتور تراکنش داشته باشد که به آن امکان شناسایی تراکنشهای غیرمجاز و کاربران متخلف را بدهد.

2- نهاد ثالث تضمین می‌کند که مکانیزم‌های مانیتور تراکنش، حداقل یکی از فاکتورهای زیر را در نظر گرفته و ثبت نماید:

- لیست عناصر احراز هویت دزدیده شده یا لو رفته.
- مبلغ هر تراکنش پرداخت.
- سناریوهای تقلب شناخته شده در سرویس‌های پرداخت.
- نشانه‌های آلودگی بدافزار در هر نشست روال احراز هویت.
- الگوهای رفتاری غیرعادی پرداخت کاربر در مقایسه با تاریخچه تراکنش‌های پرداخت.
- لاگ استفاده‌های عادی و غیرعادی از ابزارهای سخت‌افزاری و نرم افزاری ارائه شده توسط نهاد ثالث.

3- نهاد ثالث تعهد می‌کند که محرمانگی مدارک امنیتی شخصی کاربران، در مراحل مختلف مانیتورینگ محافظت شود.

4- نهاد ثالث تعهد می‌کند که فرآیندهای قابل تعقیب شکایت کاربران نهایی، در خصوص هر یک از مراحل ارائه خدمات از جمله تراکنش نادرست، مغایرت یا فعالیت بدون اخذ رضایت کاربران را تعریف و به فرادیس گستر ارائه نماید.

مهر و امضای مجاز مشتری (کاربر نهایی)	مهر و امضای نهاد ثالث

بانک توسعه صادرات ایران

ماده 6- قابلیت پیگیری

1- نهاد ثالث باید روالهای مشخصی داشته باشد که تضمین کند همه تراکنشهای کاربر نهایی، در زمینه ارائه سرویسهای پرداخت، قابل پیگیری هستند.

2- برای تحقق بند فوق، نهاد ثالث باید تضمین کند که هر نشست ارتباطی، موارد زیر را در بر دارد:

a. یک شناسه یکتا برای هر نشست.

b. مکانیزم‌های امنیتی برای لاگ کردن جزئیات تراکنشها، شامل تعداد تراکنشها، Timestampها و همه داده‌های تراکنش مرتبط.

c. Timestampها باید بر اساس یک سیستم زمانبندی یکپارچه و رسمی باشد.

ماده 7- الزامات امنیتی نهاد ثالث در ارتباط با کاربر نهایی

مسئولیت موراد امنیتی که در ذیل به آنها اشاره شده است کاملا بر عهده نهاد ثالث می باشد:

1- دستکاری و یا افشای اطلاعات حساس، حیاتی و محرمانه (از جمله، مجوزها و اطلاعات شخصی و حساب کاربر نهایی) به دلیل ناامن بودن فرایندها، تکنولوژی و نیروی انسانی.

2- هرگونه سوء استفاده یا بهره‌برداری از اطلاعات تراکنش‌های کاربران نهایی فراتر از خدمات سامانه بانکداری باز.

3- ایجاد تراکنش‌های تقلبی یا بدون مجوز کاربر نهایی.

4- نقص در بسترهای نهاد ثالث جهت دریافت اطلاعات کاربران نهایی که منجر به احراز هویت نادرست و دسترسی کاربران نهایی غیر مجاز به اطلاعات حساس، حیاتی و محرمانه شود.

5- وقوع ریسک‌های سیستماتیک، آبشاری یا زنجیره‌ای در سرویس بانکداری باز با سرمنشأ نهاد ثالث (به هر دلیل از جمله رعایت نکردن الزامات امنیتی، از جانب نهاد ثالث).

6- دسترسی غیرمجاز نهاد ثالث به اطلاعات کاربران نهایی از جمله حساب‌های بانکی کاربران نهایی، اطلاعات شخصی، صورتحساب و غیره.

7- عدم انطباق با قوانین بالادستی مرتبط با بانکداری باز.

تبصره: چنانچه در اثر قصور نهاد ثالث از رعایت شرایط و الزامات امنیتی فوق، خسارتی متوجه فرادیس گستر، بانک یا کاربر نهایی گردد، نهاد ثالث موظف است بر اساس اعلام نظر کارشناس رسمی دادگستری، کلیه خسارات مادی و معنوی وارده را جبران نماید.

مهر و امضای مجاز مشتری (کاربر نهایی)	مهر و امضای نهاد ثالث