شـــرکت خدمات انفورماتیک
informatics services corporation

راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه

تهیه‌کننـــده: شرکت خدمات انفورماتیک_ واحد بلاکچین

شناسه سند: BRN03_1.3

طـبقه‌بندی: عادی

تـــاریـــخ: ۱۴۰۱/۰۵/۰۱

بـه‌نـام خـدا

تمامی حقوق مادی و معنوی این اثر متعلق به شرکت خدمات افق رهانیت است.

مشخصات سند		
نام سند: راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه		
شناسه سند: BRN03_1.3	**شماره ویرایش:** 1.3	**تاریخ:** ۱۴۰۱/۰۵/۰۱
تعداد صفحات:	**پیوست:**	**مالکیت سند:** شرکت خدمات انفورماتیک_ واحد بلاکچین

طبقه‌بندی و دسترسی	
طبقه‌بندی: عادی	**دسترسی مجاز:** ☒ درون‌سازمانی ☒ برون‌سازمانی ☐ موارد خاص (با مجوز)
کاربران مجاز: ---	

خلاصه تغییرات	شکل مجاز قابل‌استفاده
ایجاد تطبیق با آخرین نسخه توسعه بکند (BRN02_1.3) شامل موارد زیر: افزوده شدن فرمت امضاء تغییر فرآیند دشارژ حذف شماره حساب از درخواست ها تغییر نام پارامتر tokenID به mintID اضافه کردن الگورتیم Luhn برای کنترل صحت شناسه کیف پول	☐ چاپ‌شده (کاغذی) ☐ بر روی شبکه اینترانت شرکت (الکترونیکی) ☐ بر روی وب‌سایت اینترنتی شرکت (الکترونیکی) ☒ سایرموارد:

	وضعیت اعتباردهی		
	تهیه‌کننده	**تاییدکننده**	**تصویب‌کننده**
نام و نام خانوادگی	جواد توکلی پاریزی	حسین یعقوبی	
رده سازمانی	کارشناس	رئیس	
امضا			

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

فهرست مطالب

عنوان **صفحه**

مقدمه ۵

شکل کلی درخواست ۷

فرمت امضاء ۷

ایجاد کیف رمزپول ۸

ارتقاء کیف رمزپول کاربر به سطح دو ۹

بازیابی کیف رمزپول ۹

دریافت مشخصات کیف‌رمزپول ۱۰

دریافت موجودی ۱۰

تراکنش انتقال رمزپول ۱۱

شارژ و دشارژ کیف رمزپول ۱۲

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

مقدمه

منظور از نرم‌افزار همراه، همان کیف رمزپول موبایلی می باشد که جهت سرویس‌دهی به کاربران حقیقی برنا، پیاده سازی میگردد.

از آنجا که بسیاری از سازوکارهای نرم‌افزار همراه برنا وابسته به نوع پیاده‌سازی نرم‌افزار سمت میزبان (Back-End) است، در این مستند، تنها به فرآیندهای کلی نرم‌افزار همراه پرداخته می‌شود و جزئیات و چگونگی ارتباط با سرور و بک‌اند همگی به عهده و تصمیم بانک عامل می باشد.

تعاریف

- **بک‌اِند(Backend)**: برنامه کاربردی است که به عنوان ارائه‌دهنده سرویس توسط سرورهای مستقر در بانک‌های تجاری میزبانی می‌شود. این برنامه وظیفه اتصال به گره همتا (Peer) را داشته و انجام تراکنش بر روی شبکه برنا را ممکن می‌سازد.
- **گره همتا (Peer)**: گره همتا معادل بانک‌های متولی در زیست بوم رمزریال می‌باشد. این اعضا دفتر کل را میزبانی نموده و امکان توسعه قراردادهای هوشمند را دارند.
- **قرارداد هوشمند**: مجموعه‌ای از دستورالعمل‌های نرم‌افزاری است که در شرایط مشخص تعیین شده در زمان به‌روزرسانی اطلاعات دفترکل اجرا و ضمن به‌روزرسانی اطلاعات، در صورت اجماع دارندگان دفترکل بر صحت نتیجه، منجر به تغییر اطلاعات آن می‌گردد. این کد به درخواست عضو متولی (گره همتا) اجرا می‌شود. Chaincode در این مستند به معنای قرارداد هوشمند رمزریال می باشد.
- **بلاکچین (Blockchian)**: شبکه‌ای است که با استفاده از توزیع‌شدگی و رمزنگاری، تاریخچه تمام تراکنش‌های انجام شده در آن شبکه را در دفتر کلی که امکان تغییر در آن وجود ندارد و تمام اطلاعات ثبت شده در آن به صورت شفاف در اختیار کاربران قرار دارد، ذخیره می‌کند. این بخش در زیرساخت رمزریال از طریق بک‌اند به نرم‌افزار همراه مشتریان متصل می‌شود.

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

- **زیست‌بوم رمزریال**: مجموعه‌ای شامل زیرساخت فناورانه مبتنی بر دفاتر کل توزیع شده، بانک مرکزی، بانک‌ها و کاربران نهایی رمزریال است.
- **نرم‌افزار همراه**: ابزاری است دارای شناسه یکتا که زوج کلیدهای عمومی و خصوصی کاربران را نگهداری می‌نماید و پس از فعالسازی، انواع تراکنش رمزریال از طریق آن قابل انجام است. دارنده این ابزار برای بهره‌مندی از آن نیازمند برقراری ارتباط با زیست بوم رمزریال است.
- **توکن یا دارایی دیجیتال**: توکن یک موجودیت دیجیتال است که یک ارزش مجازی یا واقعی را روی یک بستر نمایندگی می‌کند و معمولا با کاربرد و اهداف مختلف انتشار می‌یابد.
- **دفتر کل توزیع شده**: نوعی فناوری است که با استفاده از روش‌های اجماع بین دارندگان نسخه‌ای از دفترکل، تضمین می‌نماید که اطلاعات دفترکل بین آنها به صورت کامل، همگام و تقلب ناپذیر، توزیع شده و هرگونه تغییر در اطلاعات دفترکل، در تمامی نسخه‌ها به‌روزرسانی گردد.
- دفتر کل (Ledger): یک مفهوم کلیدی در شبکه توزیع شده است و وضعیت نهایی دارایی‌ها و تاریخچه تمام تراکنش‌ها را ذخیره می‌کند. داده‌های دفتر کل قابل تغییر نیستند.
- **کیف رمزپول**: محلی در دفترکل که دارایی‌های فرد را ثبت و نگهداری می‌کند.

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

شکل کلی درخواست

قالب کلیه درخواست های ارسالی به سمت بک‌اند به شکل زیر می‌باشد.

```
{
    "data": "Stringified Request Params",
    "sign": "Signed Data",
    "cert": "User Certificate"
}
```

ردیف	نام فیلد /مشخصه	نوع	شرح مشخصه	مقادیر / نمونه	ساختار
۱	data	اجباری	Strigified شده پارامتر های مورد نیاز درخواست	mobileNo":"09122346575""}' ,"identificationNumber":"012 3456789","identificationType" '{":"nationalCode	رشته
۲	sign	اجباری	امضا بر روی data	iHO/PlhyShWDy47YcZ32SzysuHiQi...	رشته
۳	cert	اجباری	گواهی کاربر	BEGIN CERTIFICATE-----\n MIIFGTCCBAGgAwIBAgISAL4z1r3EKMrgJbFanNRYZzgHMA0GCSqGSIb	رشته

ارسال درخواست‌های مختلف (که در ادامه سند به آنها پرداخته شده است) می‌بایست از طریق ایجاد یک شی، از پارامترهای مورد نیاز درخواست و قرارگیری رشته JSON Striginfied شده آن شی، فیلد data و سپس امضای آن رشته با زوج کلید کاربر و قرارگیری نتیجه آن بر روی sign و قرارگیری certificate کاربر در cert صورت گیرد.

شکل کلی این شی میتواند بنابه صلاحدید بانک عوض شود. حتی ممکن است بانک بخواهد از فرمت PKCS7 استفاده کرده و کلیه اطلاعات را در قالب یک CMS به سمت بک‌اند ارسال نماید. اما بک‌اند می‌بایستی اطلاعات را با فرمتی که در مستند راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه ذکر شده به سمت قرارداد هوشمند ارسال نماید.

فرمت امضا ء

مواردی که می‌بایست درهنگام تولید جفت کلید (KeyPair) و امضا رعایت شوند:

- اندازه کلید (KeySize) می بایست بر روی ۲۰۴۸ تنظیم شود.
- در رمزنگاری می بایست از الگوریتم RSA استفاده شود.
- برای درهم سازی (Encryption) باید از تابع SHA256 استفاده شود.

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

ایجاد کیف رمزپول

جهت ایجاد کیف رمزپول ابتدا می‌بایست کاربر احراز هویت گردد و یک جفت کلید و گواهی به وی اختصاص داده شود. بنابه دستور بانک مرکزی، احراز هویت کاربران در دو سطح (یک و دو) صورت می‌گیرد. در سطح یک احراز هویت، احراز هویت کاربر تنها با استفاده از شماره موبایل و شناسه‌هویتی که میتواند کدملی یا شماره پاسپورت باشد، امکان‌پذیر است. اما در این سطح از احراز هویت محدودیت هایی بر روی سقف مجموع تراکنش های روزانه و سقف موجودی کیف رمزپول، وجود دارد.

چگونگی انجام فرآیند احراز هویت، بنا بر نظر و سلیقه بانک پیاده سازی و اجرا میشود. بانک می‌بایست بعد از احرازهویت کاربر و دریافت اطلاعات مورد نیاز و صحت سنجی آنها، یک زوج کلید تولید کرده و برای آن یک گواهی درخواست بدهد. پیشنهاد می‌شود این زوج کلید (زوج کلید کاربر) در سمت کاربر نگهداری شود و تمامی امضاها بر روی نرم‌افزار سمت کاربر انجام شوند. طبق آخرین تغییرات برنا، بانک میتواند از CA اختصاصی خود جهت صدور گواهی استفاده کند. هرچند ذکر این نکته حائز اهمیت است که گواهی تولید شده می‌بایست، مختص کیف رمزپول برنا باشد و ترجیحا برای مقاصد دیگری استفاده نگردد. به دلیل مسائل امنیتی، پیشنهاد میگردد نگهداری زوج کلید، بر روی keystore انجام شود.

درنهایت با امضای کاربر بر روی اقلام اطلاعاتی مورد نیاز و ارسال آنها به سمت بک‌اند و سپس امضا و ارسال بک‌اند به سمت قرارداد هوشمند، کیف رمزپول کاربر ایجاد میشود. در زیر نمونه‌ای از درخواست ایجاد کیف رمزپول آورده شده است. این نمونه فقط جهت پیشنهاد می‌باشد و میتواند با توجه به نیاز بانک تغییر کند.

```
{
    "mobileNo": "mobileNoVal",
    "identificationNumber": "identificationNumberVal",
    "identificationType": " nationalCode "
}
```


تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

ردیف	نام فیلد /مشخصه	نوع	شرح مشخصه	مقادیر / نمونه	ساختار
۱	mobileNo	اجباری	شماره‌موبایل	۰۹۱۲۳۴۵۶۷۸۹	رشته ۱۱ کاراکتری
۲	identificationNumber	اجباری	شناسه هویتی	۰۱۲۳۴۵۶۷۸۹	رشته
۳	identificationType	اجباری	نوع شناسه هویتی	nationalCode	nationalCode-passportNumber

ارتقاء کیف رمزپول کاربر به سطح دو

جهت ارتقاء کیف رمزپولی کاربر به سطح دو، می‌بایست اطلاعات پایه هویتی فرد، مورد تایید قرار بگیرد و سپس تراکنش بروزرسانی نوع کیف پول کاربر که در مستند راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه به آن پرداخته شده با تنظیم پارامتر *walletType* بر روی *CUTOMER_ELEVATED* فراخوانی شود. در این تراکنش نیازی به امضا از سوی کاربر نمی‌باشد و تنها امضاء بانک مورد نیاز است. در انتها، کیف رمزپول فعلی کاربر که در سطح یک احراز هویت ایجاد شده است ارتقاء داده می‌شود. فرآیند احراز هویت سطح دو به سلیقه و صلاحدید بانک خواهد بود.

بازیابی کیف رمزپول

جهت بازیابی کیف رمزپول، ابتدا گواهی قبلی کاربر می‌بایستی باطل شود تا دسترسی قبلی مسدود گردد. بنابراین کاربر می‌بایست از طریقی از بانک خود درخواست ابطال Certificate پیشین خود را بدهد. این درخواست میتواند بصورت حضوری در شعبه و یا بنابر تشخیص بانک به روش های دیگر صورت بپذیرد. پس از ابطال گواهی، کاربر می‌بایست تمامی مراحل احرازهویت سطح یک را مجددا طی نماید تا بتواند کیف رمزپول خود را مجددا بازیابی نماید. بنابراین حتی اگر کیف رمزپول کاربر سطح دو باشد، بعد از طی مراحل سطح یک همان کیف رمزپول سطح دو برایش بازگردانی میگردد. در نهایت از طریق تراکنش بروزرسانی گواهی دیجیتال کاربر که در مستند راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

ذکر شده است میتوان گواهی جدید کاربر را به کیف رمزپول مربوط به او متصل نمود. در این تراکنش به امضاء کاربر نیازی نمی‌باشد.

دریافت مشخصات کیف‌رمزپول

دریافت مشخصات توسط بک‌اند از قرارداد هوشمند انجام میشود و نتایجی که (از نظر بانک) لازم است به سمت نرم‌افزار همراه ارسال میشود. بنابراین در این تراکنش نیازی به دریافت امضای کاربر نمی‌باشد.

دریافت موجودی

جهت دریافت موجودی کیف‌رمزپولی کاربر، با توجه به مستند راهنمای ایجاد کیف رمزپول – نرم‌افزار همراه مقادیر خواسته شده توسط زوج کلید کاربر امضا شود و به سمت بک‌اند ارسال شود، حال بک‌اند بانک میتواند بنابر صلاحدید به هر شیوه‌ای که لازم بود موجودی و اطلاعات کیف رمزپول کاربر را به سمت نرم‌افزار همراه برگرداند.

به عنوان مثال، در زیر یک نمونه شی که از سمت نرم‌افزار همراه میباست به بک‌اند، جهت دریافت موجودی ارسال شود آورده شده است.

```
{
   "walletID": " walletIDVal",
   "tokenSymbol": "tokenSymbolVal",
   "mintID": " mintIDVal"
}
```

ردیف	نام فیلد /مشخصه	نوع	شرح مشخصه	مقادیر / نمونه	ساختار
۱	walletID	اجباری	شناسه کیف فرستنده		رشته ۱۶کاراکتری
۲	tokenSymbol	اختیاری	نماد رمزپول		رشته کاراکتری
۳	mintID	اختیاری	شناسه سری انتشار رمزپول		رشته کاراکتری

از آنجا که بستر برنا، قابلیت پشتیبانی از چند نوع رمزپول را دارد، نماد رمزپول می‌بایستی در این تراکنش ذکر شود. اما در حال حاضر تنها رمزپول موجود، رمزریال بانک مرکزی می‌باشد. بنابراین نماد رمزپول، همان نماد رمزریال، بر روی بلاکچین می‌باشد.

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

اما شناسه سری انتشار بصورت اختیاری و در صورتی که تمایل به دریافت موجودی یک سری خاص رمزپول وجود داشته باشد ، میتواند تکمیل گردد.

تراکنش انتقال رمزپول

پیاده‌سازی تراکنش انتقال رمزپول، مشابه با تراکنش دریافت موجودی به عهده بانک میباشد، نمونه شی پیشنهادی پیاده‌سازی انجام این تراکنش ذیل این بند، ذکر شده است.

```
{
   "tokenSymbol": "tokenSymbol-3",
   "mintID": "mintId-3",
   "senderID": "10003",
   "receiverID": "20003",
   "amount": 1,
   "tag": "tagVal",
   "trxRef": "trxRefID",
   "bornaTrxID": "bornaTrxIDVal"
}
```

ردیف	نام فیلد /مشخصه	نوع	شرح مشخصه	مقادیر / نمونه	ساختار
	tokenSymbol	اجباری	نماد رمزپول	IRDR	رشته کاراکتری
۱	mintID	اختیاری	شناسه سری انتشار رمزپول	۱۲۴۳	رشته کاراکتری
۲	senderID	اجباری	شناسه کیف رمزپول ارسال کننده	۱۲۳۴۵۶۵۴۸۷۹۸۷۵۴۵۵۴۷	رشته ۱۶کاراکتری
۳	receiverID	اجباری	شناسه کیف رمزپول دریافت کننده	۱۲۳۴۵۶۵۴۸۷۹۸۷۵۴۵۵۴۷	رشته ۱۶ کاراکتری
۴	amount	اجباری	مبلغ تراکنش	۲۰۰	رشاه رقمی
	tag	اختیاری	برچسب		رشته کاراکتری
۵	trxRef	اختیاری	شناسه تراکنش	۴۴۶۶۲۱۷۴۴۱	رشته کاراکتری

در صورت نیاز میتوان از الگورتیم Luhn جهت صحت سنجی شناسه کیف پول مقصد در سمت نرم افزار همراه استفاده کرد.

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.

برچسب‌ها جهت رهگیری و یا مدیریت تراکنش‌ها استفاده می‌شوند که در آینده نزدیک پیاده سازی خواهند شد و در حال حاضر نیازی به پرکردن این فیلد نیست. شناسه تراکنش اختیاری بوده و میتواند جهت بررسی های نرم‌افزاری مورد استفاده قرار گیرد.

شارژ و دشارژ کیف رمزپول

فرآیند شارژ کیف رمزپول توسط بانک توسعه داده میشود. بنابراین نیازی به امضای کاربر موبایلی در این زمینه نیست . بعنوان مثال، کاربر میتواند از نرم‌افزار همراه بانک (یا از هرطریق دیگری) درخواست برداشت از حساب ریالی و شارژ حساب رمزریالی اش نماید و بانک تنها با انتقال مبلغ به حساب واسط (یا هر سازوکار دیگری بنابر صالحدید) و انتقال پول از کیف رمزپولی خودش به کیف رمزپولی کاربر فرآیند شارژ را انجام دهد. لازم به ذکر است این مثال فقط جنبه پیشنهادی دارد و بانک می‌تواند به هر شیوه ی دیگری حتی شیوه ی حضوری، این عمل را انجام دهد.

در فرآیند دشارژ نیز، کاربر مبلغ مورد نظر را به کیف خزانه انتقال میدهد. فرآیند انتقال به خزانه همانند یک فرآیند انتقال معمولی که در پیش شرح داده شد ، قابل اجراست اما بانک می‌تواند به صلاحدید شیوه خاصی برای اجرای آن در سمت کاربر مد نظر قراردهد (مانند ایجاد یک زیرفرآیند جداگانه از انتقال). سپس بعد از انتقال بانک می‌تواند مبلغ مورد نظر را به حساب ریالی کاربر واریز کند

تمامی حقوق مادی و معنوی این اثر، متعلق به شرکت خدمات انفورماتیک است.