شماره: SIP003-1
تاریخ: ۱۴۰۰/۰۷/۰۶

به نام خدا

سند استاندارد SIP003-1

شرکت‌های اپراتور احراز هویت اشخاص حقیقی و حقوقی

مقدمه

بسیاری از دپ‌های بلاکچینی به مناسبت فعالیتی که انجام می‌دهند، نیاز دارند تا کاربران خود را احراز هویت کنند. در روش استاندارد احراز هویت کاربران حقیقی و حقوقی مبتنی بر استاندارد SIP001 شرکت‌های واسطه برای اپراتوری احراز هویت کابران دیده شده است. سند حاضر به شرایط شرکت‌های پذیرفته‌شده برای ارائه‌ی این خدمات و روشمند کردن این خدمات می‌پردازد.

۱- تاریخچه

سند حاضر اولین نسخه از این استاندارد است.

۲- هدف و دامنه‌ی کاربرد

هدف از تدوین این استاندارد، ایجاد روشی یکپارچه برای پذیرش شرکت‌های متقاضی اپراتوری احراز هویت و تبیین وظایف آنان می‌باشد.

۳- اصطلاحات و تعاریف

قرارداد هوشمند: یک برنامه‌ی کامپیوتری است که روی بلاکچین پیاده‌سازی می‌شود. این برنامه می‌تواند شامل داده‌ها، توابع پرس‌وجوی داده و توابع حاوی تراکنش باشد.

دپ: یک برنامه‌ی کامپیوتری است که روی موبایل یا وب سایت نصب می‌شود و امکان دسترسی کاربران به یک قرارداد هوشمند خاص یا مجموعه‌ای از قراردادهای هوشمند را به وجود می‌آورد.

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

احراز هویت: فرآیندی است که تضمین می‌کند یک کاربر خاص دارای مشخصات هویتی خاص است.

شماره‌ی حساب سوری: شماره حسابی است که قالب خاص خود را دارد و هر حساب در شبکه‌ی بلاکچین سور با این شماره شناخته می‌شود. این قالب دقیقا نظیر شماره حساب اتریومی در شبکه‌ی بلاکچین اتریوم است.

کلید اختصاصی: متناظر با هر شماره‌ی حساب سوری یک کلید اختصاصی وجود دارد که فقط باید در اختیار صاحب حساب باشد. قالب این کلید اختصاصی نیز دقیقا نظیر شماره حساب اتریومی در شبکه‌ی بلاکچین اتریوم است. اگر کلید اختصاصی یک شخص در اختیار کاربر دیگری باشد، می‌تواند تراکنش‌هایی را به جای شخص اصلی امضا کند و موجب سوء استفاده شود.

امضای دیجیتال: هر شخص با داشتن کلید اختصاصی خود می‌تواند یک متن را امضا کند و در نتیجه‌ی آن یک رشته از کاراکترها ایجاد شود. افراد دیگر با داشتن متن و امضای آن، می‌توانند با استفاده از یک الگوریتم خاص، صحت امضا و انتساب آن به شماره‌ی حساب سوری مورد نظر را بررسی کنند.

۴- وظایف شرکت اپراتوری احراز هویت

یک شرکت اپراتوری احراز هویت، فرم‌های پرشده‌ی اشخاص حقیقی و حقوقی را که در دفترخانه‌ی اسناد رسمی گواهی امضا شده است، دریافت می‌کند و اطلاعات آن را در قرارداد هوشمند مربوطه که از طرف «بنیاد سور» در اختیارش قرار گرفته است، ثبت می‌کند.

فرم‌های موضوع این بند که در پیوست‌های ۱ تا ۶ از استاندارد SIP001 آمده‌است، عبارتند از:

- فرم گواهی امضای ثبت مشخصات اشخاص حقیقی
- فرم گواهی امضای ثبت مشخصات اشخاص حقوقی
- فرم گواهی امضای از دست دادن کلید اختصاصی اشخاص حقیقی
- فرم گواهی امضای از دست دادن کلید اختصاصی اشخاص حقوقی

نشانی: تهران، بلوار دلاوران، تقاطع سراج، خیابان صاحب‌الزمان، پلاک ۱۱۵، طبقه‌ی ۶، واحد ۲۷
تلفن: ۷۴۳۸۵۴۰۰

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

- فرم گواهی امضای سوزاندن کلید اختصاصی اشخاص حقیقی
- فرم گواهی امضای سوزاندن کلید اختصاصی اشخاص حقوقی

شرکت اپراتور احراز هویت موظف است، در موارد زیر بررسی‌های لازم را انجام دهد و از تطابق آن مطمئن شود:

- بررسی عدم مغایرت درونی در اطلاعات فرم‌های گواهی امضا شده
- بررسی تطابق کامل اطلاعات فرم‌ها با بارکد روی فرم
- بررسی مطابقت کامل اطلاعات فرم‌ها با سوابق قبلی که از متقاضی در سیستم استاندارد احراز هویت شبکه‌ی بلاکچین سور موجود است
- بررسی مطابقت امضای دیجیتال فرم با شماره‌ی حساب سوری متقاضی

شرکت اپراتور احراز هویت همچنین در صورت صحت بررسی‌های انجام شده، اطلاعات فرم‌های گواهی امضا شده را در قرارداد هوشمند احراز هویت استاندارد بنیاد که دسترسی‌های لازم از سوی بنیاد به وی داده شده، ثبت می‌کند و قبل از ثبت نهایی از تطابق کامل آن با اطلاعات فرم اطمینان حاصل می‌کند.

شرکت اپراتور احراز هویت می‌تواند جهت حصول اطمینان در احراز هویت، تصویر مدارک هویتی و تصویر پرسنلی اشخاص حقیقی و تصویر مدارک ثبتی یا روزنامه‌ی رسمی اشخاص حقوقی و تصویر مدارک هویتی و تصویر پرسنلی صاحبان امضای اشخاص حقوقی را نیز از متقاضیان احراز هویت دریافت کند.

شرکت اپراتور احراز هویت موظف است اصل یا تصویر مدارک گواهی امضا شده را به صورت مناسب بایگانی نماید.

شرکت اپراتور احراز هویت همچنین موظف است جهت تسهیل در ارتباط با کاربران برای این امور وب‌سایت یا اپ موبایل بسازد و از این طریق ارتباط کاربران را تسهیل نماید.

۵- مسئولیت شرکت اپراتوری احراز هویت

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

شرکت اپراتوری احراز هویت در موارد زیر مسئول شناخته می‌شود:

- مغایرت درونی در اطلاعات فرم‌های گواهی امضا شده
- عدم مطابقت کامل اطلاعات فرم‌ها با بارکد روی فرم
- عدم مطابقت اطلاعات فرم‌ها با سوابق قبلی که از متقاضی در سیستم استاندارد احراز هویت شبکه‌ی بلاکچین سور موجود است
- عدم مطابقت امضای دیجیتال فرم با شماره‌ی حساب سوری متقاضی
- عدم مطابقت اطلاعات وارد شده در قرارداد هوشمند بلاکچین سور با اطلاعات فرم‌های گواهی امضا شده
- عدم بایگانی مناسب فرم‌های گواهی امضا شده در دفاتر اسناد رسمی
- در اختیار گذاشتن اسناد بایگانی شده برای محاکم صالحه‌ی جمهوری اسلامی بنا به تقاضای کتبی
- افشای اطلاعات هویتی و غیر هویتی کاربران احراز صلاحیت شده به هر صورت
- استفاده‌ی شرکت اپراتور احراز هویت یا هر شخص حقیقی سا حقوقی دیگر از اطلاعات کاربران احراز صلاحیت شده، برای امور تبلیغاتی یا کسب‌وکاری یا سوء استفاده از آن

۶- منافع شرکت اپراتوری احراز هویت

درآمد شرکت اپراتور احراز هویت از این محل عبارت است از:

- دریافت مستقیم از اشخاص حقیقی یا حقوقی متقاضی احراز هویت طبق تعرفه‌هایی که خود شرکت تعیین می‌کند. این تعرفه در یک سیستم رقابتی تضمین کننده‌ی منافع توأم شرکت‌های اپراتور احراز هویت و کاربران متقاضی احراز هویت می‌باشد.
- دریافت غیر مستقیم حق اشتراک دپ‌های متقاضی خدمات احراز هویت کاربران به صورت ماهانه یا سالانه که تعرفه‌ی آن هر ساله توسط «بنیاد سور» تعیین می‌شود. این مبالغ توسط بنیاد دریافت می‌شود و پس از کسر کسورات قانونی به نسبتی که توسط

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

بنیاد تعیین می‌شود، بین شرکت‌های اپراتور احراز هویت تقسیم می‌شود.

۷- فرآیند عملیات شرکت اپراتوری احراز هویت

هر کاربر متقاضی احراز هویت باید فرم گواهی امضا شده‌ی درخواست خود را همراه با مدارک مورد درخواست شرکت اپراتور احراز هویت برای شرکت ارسال نماید.

شرکت سپس موارد زیر را به ترتیب در مورد فرم ارسالی انجام می‌دهد:

- بررسی عدم مغایرت درونی در اطلاعات فرم‌های گواهی امضا شده
- بررسی تطابق کامل اطلاعات فرم‌ها با بارکد روی فرم
- بررسی مطابقت کامل اطلاعات فرم‌ها با سوابق قبلی که از متقاضی در سیستم استاندارد احراز هویت شبکه‌ی بلاکچین سور موجود است
- بررسی مطابقت امضای دیجیتال فرم با شماره‌ی حساب سوری متقاضی
- ورود اطلاعات فرم‌های گواهی امضا شده در قرارداد هوشمند بلاکچین سور
- بررسی مطابقت اطلاعات وارد شده در قرارداد هوشمند بلاکچین سور با اطلاعات فرم‌های گواهی امضا شده
- ثبت نهایی اطلاعات فرم‌ها در قرارداد هوشند احراز هویت استاندارد بلاکچین سور

۸- شرایط پذیرش برای شرکت‌های متقاضی اپراتوری احراز هویت

برای شرکت‌های متقاضی اپراتوری احراز هویت استاندارد کاربران بلاکچین سور، لازم است:

- در اداره‌ی ثبت شرکت‌ها ثبت رسمی شده باشند.
- عملیات احراز هویت با موضوع فعالیت ثبت شده‌ی شرکت همخوانی داشته باشد.
- دفتر ثبت شده‌ی شرکت در داخل ایران باشد.

در این صورت فرم موجود در پیوست ۱ این سند را پر می‌کنند و صاحبان امضای شرکت با

نشانی: تهران، بلوار دلاوران، تقاطع سراج، خیابان صاحب‌الزمان، پلاک ۱۱۵، طبقه‌ی ۶، واحد ۲۷
تلفن: ۷۴۳۸۵۴۰۰

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

حضور در یکی از دفترخانه‌های اسناد رسمی آن فرم را گواهی می‌کنند، سپس متن محتوای فرم را با استفاده از کلید اختصاصی خود امضای دیجیتال می‌کنند و آن فرم را همراه با امضای دیجیتال آن و مدارک برابر اصل شده‌ی شرکت شامل تمام روزنامه‌های رسمی شرکت و اسناد ثبت شرکت برای «بنیاد سور» ارسال می‌نمایند.

بنیاد سور با بررسی مدارک لازم، در صورت تأیید، آن شرکت را در فهرست شرکت‌های تأیید صلاحیت شده قرار می‌دهد.

۱۱- فرآیند توسعه

اگر به دلیل درخواست دپ‌ها، استانداردهای موجود احراز صلاحیت تغییر کند، شرکت‌های اپراتوری احراز صلاحیت موظفند خود را با این تغییرات تطبیق دهند.

اگر به دلیل درخواست دپ‌ها استاندارد جدیدی برای سطح دیگری از احراز هویت تدوین شود، شرکت‌های اپراتوری احراز هویت اختیار دارند که آن سطح از احراز هویت را در برنامه‌های خود پیاده‌سازی کنند و از منافع آن بهره‌مند شوند.

۱۲- مرجع‌ها

- استاندارد آدرس اتریومی و روش تست اعتبار آن:

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-55.md

- استاندارد کلید اختصاصی اتریومی و روش استخراج آدرس اتریومی از آن:

http://gavwood.com/paper.pdf
https://etherworld.co/2017/11/17/understanding-the-concept-of-private-key-public-key-and-address-in-ethereum-blockchain

- استاندارد روش احراز هویت کاربران حقیقی و حقوقی در شبکه‌ی بلاکچین سور:

SIP001

نشانی: تهران، بلوار دلاوران، تقاطع سراج، خیابان صاحب‌الزمان، پلاک ۱۱۵، طبقه‌ی ۶، واحد ۲۷
تلفن: ۷۴۳۸۵۴۰۰

بنیاد نوآوری و توسعه‌ی
فناوری‌زنجیره‌ی‌بلوک‌سور
www.surnet.org

- استاندارد استفاده از خدمات احراز هویت توسط دپ‌ها در شبکه‌ی بلاکچین سور:

SIP002

نشانی: تهران، بلوار دلاوران، تقاطع سراج، خیابان صاحب‌الزمان، پلاک ۱۱۵، طبقه‌ی ۶، واحد ۲۷
تلفن: ۷۴۳۸۵۴۰۰

شماره: SIP003-1
تاریخ: ۱۴۰۰/۰۷/۰۶

پیوست ۱

فرم گواهی امضای قبول مسئولیت شرکت اپراتوری احراز هویت

مشخصات صاحبان امضای متعهد شخصیت حقوقی طبق آخرین مستندات ثبتی:

ردیف	کد ملی	نام	نام خانوادگی	نام پدر	سمت
۱					
۲					
۳					
۴					

اینجانب/اینجانبان صاحب/صاحبان امضای ..... با شناسه‌ی ملی ..... و شماره‌ی ثبت ..... با مشخصات مذکور در فوق به این وسیله مراتب زیر را گواهی می‌کنم/می‌کنیم:

۱- کلید اختصاصی مربوط به حساب شبکه‌ی بلاکچین سور به شماره‌ی ..... در اختیار اینجانب/اینجانبان و فقط در اختیار اینجانب/اینجانبان است.

۲- متعهد می‌شوم/می‌شویم در حفظ کلید اختصاصی شماره‌ی حساب فوق نهایت تدبیر و کوشش خود را به کار گیرم و آن را در اختیار احدی قرار ندهم /ندهیم.

۳- متعهد می‌شوم/می‌شویم اطلاعات احراز هویت‌شده‌ی کاربران احراز صلاحیت‌شده‌ی شرکت را در اختیار هیچ شخص ثالث یا اپلیکیشن دیگر به جز محاکم قضایی صالحه در جمهوری اسلامی با درخواست کتبی خودشان قرار ندهم/ندهیم.

۴- متعهد می‌شوم/می‌شویم اطلاعات احراز هویت‌شده‌ی کاربران دپ را در هیچ کسب‌وکار یا اپلیکیشن یا برنامه‌ی تبلیغاتی دیگری استفاده نکنم/نکنیم.

۵- مسئولیت هرگونه عملیات هک یا نفوذ در پایگاه داده‌ی مربوط به شرکت خود را به طور کامل می‌پذیرم/می‌پذیریم.