



به نام خدا  
سند استاندارد SIP002-1  
استفاده از خدمات احراز هویت توسط دپ‌ها

## مقدمه

بسیاری از دپ‌های بلاکچینی به مناسبت فعالیتی که انجام می‌دهند، نیاز دارند تا کاربران خود را احراز هویت کنند. استاندارد حاضر به دنبال آن است که روش استفاده از خدمات احراز هویت کاربران حقیقی و حقوقی توسط دپ‌های بستر بلاکچین سور را قانونمند سازد.

## ۱- تاریخچه

سند حاضر اولین نسخه از این استاندارد است.

## ۲- هدف و دامنه‌ی کاربرد

هدف از تدوین این استاندارد، ایجاد روشی جهت استفاده از خدمات احراز هویت ارائه شده در شبکه‌ی بلاکچین سور مبتنی بر استاندارد SIP001 توسط دپ‌ها روی این شبکه می‌باشد. هر یک از دپ‌ها در بلاکچین سور، در صورت نیاز و با رعایت شرایط می‌توانند از این استاندارد استفاده کنند و به این ترتیب کاربران خود را احراز هویت کنند. بدیهی است که دپ‌ها مجازند تا در صورت نیاز خودشان بدون استفاده از روش‌های این استاندارد، کاربران خود را احراز هویت کنند و این استاندارد هیچ گونه اجباری در این راستا به دپ‌ها اعمال نمی‌کند.

## 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.

**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 دقیقاً نظیر شماره حساب اتریوم 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 دقیقاً نظیر شماره حساب اتریوم 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- ارتباط با قرارداد هوشمند احراز هویت

قرارداد هوشمند احراز هویت، قراردادی است که:

- توسط «بنیاد سور» روی بلاکچین سور پیاده‌سازی شده است.
- داده‌های آن توسط شرکت‌های ارائه دهنده‌ی خدمات احراز هویت در بلاکچین سور ثبت می‌شود.
- داده‌های این قرارداد کاملاً محرمانه است.



- دپ‌های مجاز به دسترسی به خدمات احراز هویت می‌توانند توسط توابع پرس‌وجوی داده که در آن پیاده‌سازی شده است، به این خدمات دسترسی پیدا کنند. ارتباط با این قرارداد هوشمند توسط فراخوانی توابع دسترسی به این قرارداد هوشمند انجام می‌شود.

## ۵- دپ‌های مجاز

دپ‌هایی که علاقمند به استفاده از سطوح مختلف احراز هویت هستند، لازم است که مشخصات خود را در صفحه‌ی مخصوص به این کار در سایت «بنیاد سور» ثبت کنند. علاوه بر آن این دپ‌ها موظفند فرم پیوست ۱ یا ۲ (وابسته به حقیقی یا حقوقی بودن شخصیت مالک دپ) را پر کنند و آن را در دفترخانه‌ی اسناد رسمی گواهی امضا نمایند و آن را برای «بنیاد سور» ارسال نمایند. دپ‌های ثبت شده برای دریافت اجازه‌ی استفاده از سیستم پرس‌وجوی مربوط به احراز هویت لازم است که مبلغی را که به صورت پرداخت ماهانه یا سالانه هر سال توسط «بنیاد سور» تعیین می‌شود، به بنیاد بپردازند. این مبلغ پس از کسر کسورات قانونی، تماماً در اختیار شرکت‌های اپراتور احراز هویت (موضوع استاندارد SIP003) قرار می‌گیرد.

## ۶- پرس‌وجوی داده‌ها

سطوح دسترسی به عملیات پرس‌وجوی داده‌ها از قرارداد هوشمند اصلی شامل موارد زیر می‌شوند:

### ۶-۱- دسترسی آزاد

هر کاربر در شبکه‌ی بلاکچین سور یا هر یک از دپ‌های پیاده‌سازی شده روی این شبکه به این سطح از پرس‌وجو دسترسی دارند.  
برای اشخاص حقیقی و حقوقی

داده‌های ورودی	داده‌های خروجی	شرح
----------------	----------------	-----



بنیاد نوآوری و توسعه  
فناوری زنجیره‌ی بلوک سور  
www.surnet.org

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۷/۰۶

شماره‌ی حساب سوری	False یا True	آیا داده‌های این شماره‌ی حساب سوری ثبت شده یا خیر؟
-------------------	---------------	--

## ۲-۶- دسترسی سطح اول

فقط دپ‌هایی که طبق بند ۵ اجازه‌ی دسترسی به پرس‌جوی داده‌های احراز هویت دارند، می‌توانند در این سطح از پرس‌وجو شرکت کنند.

### برای اشخاص حقیقی

داده‌های ورودی	داده‌های خروجی	شرح
شماره‌ی حساب سوری کد ملی	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نام و نام خانوادگی کامل	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نام پدر	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری جنسیت	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری تاریخ تولد	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری شماره‌ی تلفن همراه	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟

### برای اشخاص حقوقی

داده‌های ورودی	داده‌های خروجی	شرح
شماره‌ی حساب سوری شناسه‌ی ملی	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نام شخصیت حقوقی	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نوع شخصیت حقوقی	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری شماره‌ی ثبت	False یا True	آیا این داده‌ها با هم مطابقت دارند یا خیر؟

## ۷- نیاز به اطلاعات هویتی جدید

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

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



بنیاد نوآوری و توسعه  
فناوری زنجیره‌ی بلوک سور  
www.surnet.org

هر یک از دپ‌هایی که متقاضی اطلاعات بیشتر هویتی (مانند آخرین مدرک تحصیلی، وضعیت تأهل یا ...) از کاربران خود باشند، می‌توانند پیشنهاد خود را برای «بنیاد سور» ارسال کنند، تا استاندارد جدیدی برای آن تنظیم شود یا استانداردهای موجود توسعه داده شود.

## ۸- 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

- استاندارد شرکت‌های اپراتور احراز هویت اشخاص حقیقی و حقوقی در شبکه‌ی

بلاکچین سور:

SIP003

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



بنیاد نوآوری و توسعه  
فناوری زنجیره‌ی بلوک سور  
www.surnet.org

## پیوست ۱

### فرم گواهی امضای قبول مسئولیت دپ برای اشخاص حقیقی

اینجانب ..... فرزند ..... دارای کد ملی .....  
دارای جنسیت مذکر/مؤنث متولد تاریخ ...../...../..... به این وسیله مراتب زیر را گواهی  
می‌کنم:

۱- اعلام می‌کنم که مسئولیت کامل دپ با عنوان ..... با آدرس  
..... در شبکه‌ی بلاکچین سور با اینجانب  
می‌باشد.

۲- متعهد می‌شوم که به هیچ وجه از قانون اساسی و سایر قوانین موضوعه‌ی جمهوری اسلامی  
ایران در این دپ تخلف نکنم.

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

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

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





## پیوست ۲

### فرم گواهی امضای قبول مسئولیت دپ برای اشخاص حقوقی

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- اعلام می‌کنم/می‌کنیم که مسئولیت کامل دپ با عنوان ..... با  
آدرس ..... در شبکه‌ی بلاکچین سور با  
اینجانب/اینجانبان می‌باشد.

۲- متعهد می‌شوم/می‌شویم که به هیچ وجه از قانون اساسی و سایر قوانین موضوعه‌ی  
جمهوری اسلامی ایران در این دپ تخلف نکنم/نکنیم.

۳- متعهد می‌شوم/می‌شویم اطلاعات احراز هویت‌شده‌ی کاربران دپ را در اختیار هیچ  
شخص ثالث یا دپ 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 دپ خود را به طور  
کامل می‌پذیرم/می‌پذیریم.