



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 نسخه‌ی تصویب شده 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 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 دقیقاً 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- 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 بنیاد سور در بلاکچین سور ثبت می‌شود.
- داده‌های این قرارداد کاملاً محرمانه است.
- دپ‌های مجاز به دسترسی به خدمات احراز هویت می‌توانند توسط توابع پرسوجوی

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۹/۱۰

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.

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

### ۶-۲- 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	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نام و نام خانوادگی کامل	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری نام پدر	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری جنسیت	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری تاریخ تولد	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟
شماره‌ی حساب سوری شماره‌ی تلفن همراه	True یا False	آیا این داده‌ها با هم مطابقت دارند یا خیر؟

### برای اشخاص حقوقی

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

## ۷- نیاز به اطلاعات هویتی جدید

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.

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۹/۱۰



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

## ۸- مراجع‌ها

- 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



## پیوست ۱

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

اینجانب ..... فرزند ..... دارای کد ملی .....  
و شماره شناسنامه ..... متولد تاریخ ...../...../..... به نشانی محل اقامت  
..... به این وسیله در کمال آزادی اراده و صحت قصد 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 حسب دستور کتبی مقام  
قضایی قرار ندهم.

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

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

۶- مسئولیت عدم رعایت تعهدات فوق یا نقص اطلاعات یا خلاف واقع بودن آنها را بر عهده  
می‌گیرم و جبران خسارات شبکه بلاکچین سور یا اشخاص ثالث را در این موارد می‌پذیرم و  
سور را در قبال ادعاهای ثالث مصون می‌دارم.





## پیوست ۲

### فرم گواهی امضای قبول تعهدات 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 ..... محل ثبت ..... با  
مشخصات مذکور در فوق به این وسیله در کمال آزادی اراده و صحت قصد 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 حسب دستور  
کتبی مقام قضایی 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 جبران خسارات ناشی از هرگونه عملیات هک یا نفوذ در پایگاه داده‌ی مربوط به  
دپ خود را به طور کامل می‌پذیرم/می‌پذیریم.

شماره: SIP002-1  
تاریخ: ۱۴۰۰/۰۹/۱۰



بنیاد نوآوری و توسعه  
فناوری زنجیره بلوک سور  
[www.surnet.org](http://www.surnet.org)

۶- مسئولیت عدم رعایت تعهدات فوق یا نقص اطلاعات یا خلاف واقع بودن آنها را مجتمعا منفردا بر عهده می گیرم/می گیریم و جبران خسارات شبکه بلاکچین سور یا اشخاص ثالث را در این موارد می پذیرم/می پذیریم و سور را در قبال ادعاهای ثالث مصون می دارم/می داریم.