



به نام خدا  
سند استاندارد SIP001-1  
روش احراز هویت کاربران حقیقی و حقوقی

## مقدمه

بسیاری از دپ‌های بلاکچینی به مناسبت فعالیتی که انجام می‌دهند، نیاز دارند تا کاربران خود را احراز هویت کنند. این استاندارد به دنبال آن است که روشی را به وجود آورد تا برای هر کاربر هر یک از دپ‌های بلاکچین سور تنها نیاز به یک بار احراز هویت داشته باشد و در صورت استفاده‌ی همان کاربر از دیگر دپ‌های تابع این استاندارد، نیازمند احراز هویت مجدد نباشد.

## ۱- تاریخچه

سند حاضر اولین نسخه از این استاندارد است.

## ۲- هدف و دامنه‌ی کاربرد

هدف از تدوین این استاندارد، ایجاد روشی برای شناسایی کاربران دپ‌های بلاکچین سور در صورت نیاز آن دپ است تا هر دپ مجبور نباشد به طور جداگانه کاربران خود را احراز هویت کند.

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

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

**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- اطلاعات لازم برای احراز هویت

### ۴-۱- احراز هویت اشخاص حقیقی

اطلاعات پایه برای احراز هویت اشخاص حقیقی عبارتند از:

- کد ملی

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

- نام
- نام خانوادگی
- نام پدر
- جنسیت
- تاریخ تولد
- شماره‌ی تلفن همراه
- شماره‌ی حساب سوری

## ۲-۴- احراز هویت اشخاص حقوقی

اطلاعات پایه برای احراز هویت اشخاص حقوقی عبارتند از:

- شناسه‌ی ملی
- نام شخصیت حقوقی
- نوع شخصیت حقوقی
- شماره‌ی ثبت

## ۵- روش احراز هویت

هر یک از اشخاص حقیقی یا حقوقی که می‌خواهند در شبکه‌ی بلاکچین سور طبق این استاندارد احراز هویت شوند، باید دومارحله‌ی زیر را به ترتیب انجام دهند:

### ۵-۱- گواهی امضا در دفتر اسناد رسمی

شخص حقیقی یا نمایندگان صاحب امضای شخص حقوقی باید فرم پیوست شماره‌ی ۱ یا ۲ (وابسته به حقیقی یا حقوقی بودن شخص) را پر کنند و در یکی از دفترخانه‌های اسناد رسمی حاضر شوند و امضای خود ذیل آن فرم را گواهی نمایند.



## ۲-۵- ارسال فرم گواهی امضا شده برای شرکت‌های اپراتور احراز هویت

طبق استاندارد SIP003 شرکت‌های پذیرفته شده به عنوان اپراتور احراز هویت اشخاص حقیقی و حقوقی مورد تأیید بنیاد در سایت بنیاد معرفی می‌شوند. اشخاص متقاضی احراز هویت باید به یکی از این شرکت‌ها یا سایت یا اپلیکیشن آنها مراجعه کنند و ضمن ارائه‌ی گواهی امضای مورد تأیید دفترخانه (در بند ۵-۱) متن فرم گواهی شده را با کلید اختصاصی شماره‌ی حساب سوری خود امضا کنند و امضای خود را در اختیار شرکت مزبور قرار دهند.

## ۶- شرایط احراز هویت

- هر شخص حقیقی یا حقوقی می‌تواند با آدرس‌های سوری مختلف به دفعات احراز هویت نماید.
- هر شخص حقیقی یا حقوقی با هر آدرس سوری تنها یک بار می‌تواند فرآیند احراز هویت را انجام دهد.

## ۷- از دست دادن کلید اختصاصی

اگر یک شخص حقیقی یا حقوقی کلید اختصاصی خود را به هر روشی از دست بدهد، چه از طریق مفقود شدن کلید اختصاصی باشد و چه از راه لو رفتن آن، لازم است که در اولین فرصت ممکن فرآیند زیر را به ترتیب انجام دهد:

### ۱-۷- گواهی امضا در دفاتر اسناد رسمی

شخص حقیقی یا نمایندگان صاحب امضای شخص حقوقی که کلید اختصاصی خود را از دست داده است، باید فرم پیوست شماره‌ی ۳ یا ۴ (وابسته به حقیقی یا حقوقی بودن شخص) را تکمیل کند و شماره‌ی حساب سوری جدیدی را به عنوان جانشین حساب قبلی اعلام کند و با حضور در یکی از دفترخانه‌های اسناد رسمی، امضای خود ذیل آن فرم را گواهی نمایند.



## ۲-۷- ارسال فرم گواهی امضا شده برای شرکت‌های اپراتور احراز هویت

شخص حقیقی یا حقوقی که کلید اختصاصی خود را از دست داده است، باید به یکی از شرکت‌های تابع استاندارد SIP003 یا سایت یا اپلیکیشن آنها مراجعه کند و ضمن ارائه‌ی گواهی امضای مورد تأیید دفترخانه (در بند ۷-۱) متن فرم گواهی شده را با کلید اختصاصی جدید خود امضا کند و امضای خود را در اختیار شرکت مزبور قرار دهد.

بدیهی است پس از انجام این فرآیند شخص حقیقی یا حقوقی نخواهد توانست در هیچ یک از دپ‌های بلاکچین سور با آدرس سوری قبلی احراز هویت کند، ولی مسئولیت وی برای دپ‌هایی که قبلاً در آنها با آدرس قبلی احراز هویت کرده است، همچنان محفوظ است.

## ۸- سوزاندن آدرس سوری

اگر یک شخص حقیقی یا حقوقی نخواهد دیگر از آدرس سوری ثبت‌شده‌ی خود استفاده کند، باید فرآیند زیر را به ترتیب طی کند:

### ۸-۱- گواهی امضا در دفاتر اسناد رسمی

شخص حقیقی یا نمایندگان صاحب امضای شخص حقوقی که متقاضی سوزاندن آدرس سوری خود است، باید فرم پیوست شماره‌ی ۵ یا ۶ (وابسته به حقیقی یا حقوقی بودن شخص) را تکمیل کند و با حضور در یکی از دفترخانه‌های اسناد رسمی، امضای خود ذیل آن فرم را گواهی نمایند.

## ۲-۸- ارسال فرم گواهی امضا شده برای شرکت‌های اپراتور احراز هویت

شخص حقیقی یا حقوقی که متقاضی سوزاندن آدرس سوری خود است، باید به یکی از شرکت‌های تابع استاندارد SIP003 یا سایت یا اپلیکیشن آنها مراجعه کند و ضمن ارائه‌ی گواهی امضای مورد تأیید دفترخانه (در بند ۸-۱) متن فرم گواهی شده را با کلید اختصاصی جدید خود امضا کند و امضای خود را در اختیار شرکت مزبور قرار دهد.

بدیهی است پس از انجام این فرآیند شخص حقیقی یا حقوقی نخواهد توانست در هیچ یک از



دپ‌های بلاکچین سور با آن آدرس سوری احراز هویت کند، ولی مسئولیت وی برای دپ‌هایی که قبلاً در آنها احراز هویت کرده است، همچنان محفوظ است.

## ۹- فرآیند ذخیره‌سازی اطلاعات احراز هویت

شرکت‌های اپراتور احراز هویت تابع استاندارد SIP003 موظفند اطلاعات اشخاص حقیقی و حقوقی احراز هویت‌شده را در یک قرارداد هوشمند محرمانه که توسط «بنیاد سور» ایجاد گردیده است و دسترسی لازم آن برای شرکت اپراتور احراز هویت ایجاد شده است، ثبت کنند. شرکت‌های اپراتور احراز هویت طبق تعرفه‌ای که خود تعیین می‌کنند، هزینه‌ی انجام این عملیات را از مقاضیان دریافت می‌کنند. برنامه‌ی قرارداد هوشمند مربوط به این عملیات نیز روی گیت‌هاب «بنیاد سور» قرار دارد.

## ۱۰- استفاده از خدمات احراز هویت توسط دپ‌ها

فرآیند پرس‌وجوی دپ‌های متقاضی احراز هویت از قرارداد هوشمند احراز هویت در استاندارد SIP002 تشریح شده است.

## ۱۱- فرآیند توسعه

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 استاندارد حاضر توسعه داده شود.

## ۱۲- مرجع‌ها

- استاندارد آدرس اتریومی و روش تست اعتبار آن:

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



شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

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

SIP002

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

SIP003

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

## پیوست ۱ فرم گواهی امضای ثبت مشخصات اشخاص حقیقی

کد ملی:

نام:

نام خانوادگی:

نام پدر:

جنسیت:

تاریخ تولد:

شماره‌ی موبایل:

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

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

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

۳- مسئولیت صحت اطلاعات فوق را بر عهده می‌گیرم.

۴- مسئولیت امضای تمامی مواردی را که با این کلید اختصاصی در اپلیکیشن‌های مختلف  
صورت می‌گیرد، بر عهده می‌گیرم.

۵- متعهد می‌شوم در صورت مفقودی کلید اختصاصی یا لو رفتن آن سریعاً فرآیند «از دست  
دادن کلید اختصاصی» که توسط بنیاد سور اعلام شده است، انجام دهم.



شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

## پیوست ۲

### فرم گواهی امضای ثبت مشخصات اشخاص حقوقی

شناسه‌ی ملی:

نام شخصیت حقوقی:

نوع شخصیت حقوقی:

شماره‌ی ثبت:

تاریخ ثبت:

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- مسئولیت صحت اطلاعات فوق را بر عهده می‌گیرم/می‌گیریم.

۴- مسئولیت امضای تمامی مواردی را که با این کلید اختصاصی در اپلیکیشن‌های مختلف

صورت می‌گیرد، بر عهده می‌گیرم/می‌گیریم.

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

- ۵- متعهد می‌شوم/می‌شویم در صورت مفقودی کلید اختصاصی یا لو رفتن آن سریعاً فرآیند «از دست دادن کلید اختصاصی» که توسط بنیاد سور اعلام شده است، انجام دهم/دهیم.
- ۶- متعهد می‌شوم/می‌شویم در پایان مدت مأموریت خود در این شخصیت حقوقی به هیچ وجه هیچ سند یا تراکنشی در هیچ یک از اپلیکیشن‌ها با این کلید اختصاصی امضا نکنم/نکنیم و سریعاً فرآیند «سوزاندن کلید اختصاصی» را که توسط «بنیاد سور» اعلام شده است، انجام دهم/دهیم.



### پیوست ۳

#### فرم گواهی امضای از دست دادن کلید اختصاصی 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 کلید اختصاصی اینجانب مربوط به حساب شبکه‌ی بلاکچین سور به  
شماره‌ی ..... مفقود شده/در اختیار افراد دیگر قرار  
گرفته/..... .

۲- متعهد می‌شوم که از این پس با این کلید اختصاصی به هیچ وجه هیچ سندی یا تراکنشی را  
در سیستم احراز هویت بلاکچین سور امضا نکنم.

۳- اعلام می‌کنم که مسئولیت تمام تراکنش‌ها و سندهای امضا شده با این کلید اختصاصی قبل  
از این تاریخ را می‌پذیرم، ولی مسئولیت امضاهای بعدی با اینجانب نمی‌باشد.

۴- متعهد می‌شوم از این پس به جای کلید اختصاصی قبلی، از کلید اختصاصی مربوط به  
حساب شبکه‌ی بلاکچین سور به شماره‌ی ..... برای احراز  
هویت استاندارد شبکه استفاده کنم و اعلام می‌کنم که کلید اختصاصی مربوط به این  
شماره‌ی حساب در اختیار اینجانب و فقط در اختیار اینجانب است.

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

۶- مسئولیت امضای تمامی مواردی را که با این کلید اختصاصی جدید در اپلیکیشن‌های  
مختلف صورت می‌گیرد، بر عهده می‌گیرم.

۷- متعهد می‌شوم در صورت مفقودی کلید اختصاصی جدید یا لو رفتن آن سریعاً فرآیند «از  
دست دادن کلید اختصاصی» که توسط بنیاد سور اعلام شده است، انجام دهم.



## پیوست ۴

### فرم گواهی امضای از دست دادن کلید اختصاصی 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 کلید اختصاصی اینجانب/اینجانبان مربوط به حساب شبکه‌ی  
بلاکچین سور به شماره‌ی ..... مفقود شده/در اختیار افراد  
دیگر قرار گرفته/..... .

۲- متعهد می‌شوم/می‌شویم که از این پس با این کلید اختصاصی به هیچ وجه هیچ سندی یا  
تراکنشی را در سیستم احراز هویت بلاکچین سور امضا نکنم/نکنیم.

۳- اعلام می‌کنم/می‌کنیم که مسئولیت تمام تراکنش‌ها و سندهای امضا شده با این کلید  
اختصاصی قبل از این تاریخ را می‌پذیرم/می‌پذیریم، ولی مسئولیت امضاهای بعدی با  
اینجانب/اینجانبان نمی‌باشد.

۴- متعهد می‌شوم/می‌شویم که از این پس به جای کلید اختصاصی قبلی، از کلید اختصاصی  
مربوط به حساب شبکه‌ی بلاکچین سور به شماره‌ی ..... برای  
احراز هویت استاندارد شبکه استفاده کنم/کنیم و اعلام می‌کنم/می‌کنیم که کلید اختصاصی  
مربوط به این شماره‌ی حساب در اختیار اینجانب/اینجانبان و فقط در اختیار  
اینجانب/اینجانبان است.

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

- ۵- متعهد می‌شوم/می‌شویم در حفظ کلید اختصاصی شماره‌ی حساب جدید فوق نهایت تدبیر و کوشش خود را به کار گیرم/گیریم و آن را در اختیار احدی قرار ندهم/ندهیم.
- ۶- مسئولیت امضای تمامی مواردی را که با این کلید اختصاصی جدید در اپلیکیشن‌های مختلف صورت می‌گیرد، بر عهده می‌گیرم/می‌گیریم.
- ۷- متعهد می‌شوم/می‌شویم در صورت مفقودی کلید اختصاصی جدید یا لو رفتن آن سریعاً فرآیند «از دست دادن کلید اختصاصی» که توسط بنیاد سور اعلام شده است، انجام دهم/دهیم.
- ۸- متعهد می‌شوم/می‌شویم در پایان مدت مأموریت خود در این شخصیت حقوقی به هیچ وجه هیچ سند یا تراکنشی در هیچ یک از اپلیکیشن‌ها با این کلید اختصاصی جدید امضا نکنم/نکنیم و سریعاً فرآیند «سوزاندن کلید اختصاصی» را که توسط «بنیاد سور» اعلام شده است، انجام دهم/دهیم.

شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

## پیوست ۵

### فرم گواهی امضای سوزاندن کلید اختصاصی 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 کلید اختصاصی اینجانب مربوط به حساب شبکه‌ای بلاکچین سور به  
شماره‌ی ..... از این پس دارای اعتبار نمی‌باشد.
- ۲- متعهد می‌شوم که از این پس با این کلید اختصاصی به هیچ وجه هیچ سندی یا تراکنشی را  
در سیستم احراز هویت بلاکچین سور امضا نکنم.
- ۳- اعلام می‌کنم که مسئولیت تمام تراکنش‌ها و سندهای امضا شده با این کلید اختصاصی قبل  
از این تاریخ را می‌پذیرم، ولی مسئولیت امضاهای بعدی با اینجانب نمی‌باشد.



شماره: SIP001-1  
تاریخ: ۱۴۰۰/۰۷/۰۶



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

## پیوست ۶

### فرم گواهی امضای سوزاندن کلید اختصاصی 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:

۹- اعلام می‌کنم/می‌کنیم که کلید اختصاصی اینجانب/اینجانبان مربوط به حساب شبکه‌ی  
بلاکچین سور به شماره‌ی ..... به دلیل خاتمه‌ی مدت  
مأموریت/..... دارای اعتبار نمی‌باشد.

۱۰- متعهد می‌شوم/می‌شویم که از این پس با این کلید اختصاصی به هیچ وجه هیچ سندی یا  
تراکنشی را در سیستم احراز هویت بلاکچین سور امضا نکنم/نکنیم.

۱۱- اعلام می‌کنم/می‌کنیم که مسئولیت تمام تراکنش‌ها و سندهای امضا شده با این کلید  
اختصاصی قبل از این تاریخ را می‌پذیرم/می‌پذیریم، ولی مسئولیت امضاهای بعدی با  
اینجانب/اینجانبان نمی‌باشد.