

پُلاریس سامانه مدیریت کلید Crypto KMS

تهیهکننده: استارتاپ پُلاریس

نسخه مستند: ۱/۱

تاریخ مستند: ۱۴۰۲/۰۹/۰۸

تاریخچه نگارش

تاريخ ويرايش	تغييرات ويرايش	ويرايش
1604/09/01	ایجاد سند	1/0
1404/09/04	بروزرسانی سرویسها	1/1

فهرست مطالب

1a	۱ - مقدم
ف مستند	۲ - اهدا
ِد کلی	
١X-Ap	
ب کلید	
استخراج کلید	
ویسهای مدیریت کلید	۴ – سرو
ى كليد جديد	ساخد
ن کلید براساس کلید خصوصی	افزودر
ن کلید براساس MNEMONICS	افزودر
کلید	
ق کلید	
راج کلید	
ویسهای شبکههای مبتنی بر اتریوم	۵ – سرو
توسط کلید	امضا
ت اطلاعات عمومی کلید٧	دریاف
ویسهای شبکههای مبتنی بر UTXO	۶ – سرو
توسط کلید	امضا
ت اطلاعات عمومی کلید	د، ياف



۱ - مقدمه

مجموعـه سـرویسهای Blockchain as a Service پلاریـس تـلاش مـیکنـد تـا زمـان توسـعه محصـول را بـرای مشـتریان خـود در حـوزه بلاکچـین را کـاهش داده و نیـاز و وابسـتگی آنهـا را بـه دانـش فنـی مـرتبط بـا بلاکچـین بـه حـداقل میـزان ممکـن برسـاند. بـدین ترتیـب کسـبوکارهای نوپـا و نیـز سـازمان یافتـه مـیتواننـد در سـریعترین زمـان ممکـن بـا اسـتفاده از سـرویسهـای مبتنـی بـر وب پلاریـس محصـولات خـود را توسـعه و گسترش دهند.

۲ - اهداف مستند

ایـن مسـتند در راسـتای معرفی سـرویسهای مـدیریت کلیـد مبتنـی بـر بلاکچـین (Crypto) میباشــد. بــر اســاس طراحــی ســامانههای پلاریــس، سـرویسهای BaaS پلاریــس میتواننـد کلیـدهای خـود را در بـیش از یـک محــل ذخیــره کنند.

در ایــن راســتا، ســرویسهای KMS بــه صــورت مســتقل از Wallet ارائــه شــده اســت و قابلیـت ایـن را دارد کـه بـه صـورت اختصاصـی بـرای مشـتریان نصـب شـده و یــا اینکـه بـه صورت مشترک و از سرویس مدیریت کلید cloud پلاریس استفاده نماید.

۳ - موارد کلی

X-Api-Key •

مقـدار api-key یـک رشـته تولیـد اسـت کـه جهـت احـراز هویـت و تنظـیم دسترسـی بـه سرویسها استفاده میشود.

• برچسب کلید

در بعضی از عملیات کاربر میتواند یک برچسب (Label) بـرای خـود مشـخص کنـد. در آینده ایـن برچسب جهـت تحلیـل دادههـا توسـط کـاربر در داشـبورد میتوانـد مـورد اسـتفاده قرار گیرد.





• امكان استخراج كليد

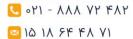
در هنگام ثبت اطلاعـات کلیـد و یـا تولیـد کلیـد در سـامانه، کـاربر میتوانـد بـا مقـدار دهـی بـه فیلـد Exportable=true مشـخص کنـد کـه در آینـده امکـان اسـتخراج اطلاعـات کلیـد وجـود خواهد داشت.

۴ - سرویسهای مدیریت کلید

• ساخت کلید جدید

این سرویس یک کلید کاملاً جدید تولید می کند و شناسه یکتای آن را باز میگرداند.

Generate Key				
<server-url>/api/keys/generate</server-url>				
	Method	POST		
	Header	Content-Type	application/json	
Request	ricadei	X-API-Key	Authorization Token	
	Body	<pre>{ "label": "<s "exportable'="" pre="" }<=""></s></pre>	string>", ': " <boolean>"</boolean>	
Daggara	keyld			شناسه یکتای کلید
Response	Example	{ "keyId": " <u }</u 	uuid>"	





• افزودن کلید براساس کلید خصوصی

این سرویس یک کلید را بر اساس کلید خصوصی در سیستم ثبت میکند.

لازم به ذکر است که مقدار chaincodeHex یک مقدار اختیاری است و جهت اشتقاق کلید است و جهت اشتقاق کلید است که نیازی به آن ندارید کلید استفاده میگردد و در صورتی که نیازی به آن ندارید می توانید مقدار آن را null ارسال کنید. جهت دریافت اطلاعات بیشتر لطفاً به مستندات BEP-۰۰۳۲۴ مراجعه بفرمایید.

Import-Priv	Import-Privatekey			
<server-url< th=""><th>-/api/keys/import-privatekey</th><th></th><th></th></server-url<>	-/api/keys/import-privatekey			
	Method	POST		
	Header	Content-Type	application/json	
Request		X-API-Key	Authorization Token	
	Body	"chainCodeHe": " <s< td=""><th>dex": "<string>", ex": "<string>", string>", ': "<boolean>"</boolean></string></string></th></s<>	dex": " <string>", ex": "<string>", string>", ': "<boolean>"</boolean></string></string>	
Respons	keyld		کلید یکتا	
е	Example	{ "keyId": "< }	uuid>"	

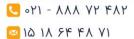
• افزودن کلید براساس Mnemonics

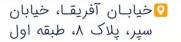
ایـن سـرویس یـک کلیـد خصوصـی بـر اسـاس mnemonic ارسـال شـده در سـامانه ثبـت میکند.

\ Key Deriviation

^{*} https://github.com/bitcoin/bips/blob/master/bip-۰۰٣٢.mediawiki









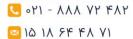
Import-Privatekey				
<server-url>/api/keys/import-mnemonics</server-url>				
	Method	POST		
	Header Request	Content-Type	application/json	
Request		X-API-Key	Authorization Token	
	Body	<pre>{ "mnemonics": "<string>", "label": "<string>", "exportable": "<boolean>" }</boolean></string></string></pre>		
Dooponoo	keyld		کلید یکتا	
Response	Example	{ "keyId": " <u td="" }<=""><td>uuid>"</td></u>	uuid>"	

• حذف كليد

با ایـن سـرویس کـاربر میتوانـد بـا ارائـه شناسـه کلیـد (تولیـد شـده در سـرویسهای فـوق) اقـدام بـه حـذف کلیـدی کـه از آن کلیـد دیگـری مشـتق شـده باشـد، مشـکلی بـه وجـود نخواهـد آمـد و در واقـع تنهـا کـاربر اسـت کـه ارتبـاط بـین کلیدها را میداند.

Delete Key				
<server-url>/api/keys/delete</server-url>				
	Method	POST		
Request	Request Header	Content-Type	application/json	
Request		X-API-Key	Authorization Token	
	Body	{ "keyId": " }</th <th>string>",</th>	string>",	
Response	keyld		کلید یکتا	
Example frarvy-ersf-facy-a-sd-ceyaxqysdbay-y		°Y-a∙۶d-ceY۵۸۹Y۶db۵Y•Y		







• اشتقاق كليد

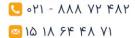
ایــن ســرویس امکــان انشــقاق کلیــد (Key Deriviation) بــر اســاس اســتاندارد BEP-۰۰۳۲ را بــه کــاربر میدهــد. لازم بــه ذکــر اســت کــه کلیــد جدیــد تولیــد شــده نیــز امکــان اشــتقاق را خواهد داشت.

Derive Key			
<server-url>/api/keys/derive</server-url>			
	Method	POST	
	Header	Content-Type	application/json
Request		X-API-Key	Authorization Token
	Body	<pre>{ "parentId": "<uuid>", "label": "<string>", "exportable": "<boolean>" }</boolean></string></uuid></pre>	
Dooponoo	keyld		کلید یکتا
Response	Example	{ "keyId": " <br }	uuid>"

• استخراج کلید

با کمک ایان سرویس میتوانید مقدار کلید خصوصی، chain code و سایر اطلاعات کلید را دریافت نمایید. در صورتی که در زمان تولید کلید، آن را exportable معرفی نکرده باشید، امکان export آن وجود نخواهد داشت.





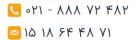


Export Key					
<server-url>/api/keys/export-key</server-url>					
	Method	GET			
Request	Header	Content-Type	application/json		
Request	i leauei	X-API-Key	Authorization Token		
	Query Params	"keyId": " <uuid>"</uuid>			
	privatekeyHex		کلید خصوصی در مبنای شانزده		
	chainCodeHex		کد مخصوص به صورت hex		
	timestamp		زمان دریافت کلید برچسب کلید		
Response	Response label		برچسب کلید		
	Example	<pre>{ "privatekeyHex": "<string>", "timestamp": "<datetime>", "chainCodeHex": "<string>", "label": "<string>" }</string></string></datetime></string></pre>			

۵ - سرویسهای شبکههای مبتنی بر اتریوم

• امضا توسط كليد

این سرویس hash یک تراکنش را بر اساس کلید مشخص شده امضا میکند.



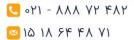


Signs Transaction Hash				
<server-url>/ap</server-url>	i/evm/sign/hash			
	Method	POST		
	Header	Content-Type	application/json	
Request	neduei	X-API-Key	Authorization Token	
	Body	<pre>{ "keyId": "< "hashHex": ' "chainId": ' }</pre>	" <string>",</string>	
	keyld			کلید یکتا
	hashHex			مقدار هش به صورت hex
Response	chainId	د یکتای شبکه		کد یکتای شبکه
	Example	{ "r_Hex": " <string>", "s_Hex": "<string>", "v_Hex": "<string>", "signature": "<string>" }</string></string></string></string>		

• دریافت اطلاعات عمومی کلید

ایـن سـرویس اطلاعـات کلیـد و آدرس تولیـد شـده بـر اسـاس اسـتانداردهای شـبکههای مبتنی بر اتریوم را مشخص میکند.







Returns public information			
<server-url>/api/evm/get-public-info</server-url>			
Method		GET	
Request	Header	Content-Type	application/json
	neauei	X-API-Key	Authorization Token
	keyld	کد یکتای کلید	
	publicKeyHex	کلید عمومی	
Response	publicAddress	آدرس اتریمی	
	Example	<pre>{ "keyId": "<uuid>", "publicKeyHex": "<string>", "publicAddress": "<string>" }</string></string></uuid></pre>	

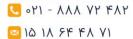
۶ - **سرویسهای شبکههای مبتنی بر UTXO**

در ایـن بخـش سـرویسهای شـبکه هـای مبتنـی بــر سـاختار UTXO ً ماننــد بیــت کــوین توضیح داده خواهند شد.

• امضا توسط كليد

ایسن سسرویس یسک تسراکنش را رمسز میکنسد. لازم بسه ذکسر اسست کسه مقسدار hexadecimal در واقع داده json تسراکنش اسست کسه بسه صبورت transactionDataHex کند شده است. ایس سرویس تبلاش میکنند کنه ورودی های تبراکنش را توسط کلیندهای ارائیه شده امضا نمایند. بندیهی است کنه در صورت عندم ارائیه تمامی کلیندها، تبراکنش تولید شده در خروجی، به طور کامل رمز نشده باشد.

ایـن موضـوع بـه کـاربر امکـان ارائـه سـرویس رمزنگـاری یـک تـراکنش توسـط چنـدین نفـر را میدهد به این صـورت کـه هـر یـک از کـاربران اطلاعـات تـراکنش را بـه صـورت جداگانـه رمـز میکند و نتیجه را در اختیار نفر بعد قرار میدهد.



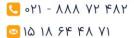


Signs a UXTO (like bitcoin) transaction				
<server-url> /api/utxo/sign-tx</server-url>				
	Method			
	Header	Content-Type	application/json	
Request	neauei	X-API-Key	Authorization Token	
Request	Body	<pre>{ "keyIds": ["<uuid>", "<uuid>"], "transaction "network": ' }</uuid></uuid></pre>	<mark>nDataHex":</mark> " <string>", "MainNet"</string>	
Response	Hash string	داده تراکنش UTXO که به صورت hex کد شده است.		
	Example	<string></string>		

• دریافت اطلاعات عمومی کلید

ایـن سـرویس اطلاعـات کلیـد و آدرس تولیـد شـده بـر اسـاس اسـتانداردهای شـبکههای مبتنی بـر UTXO ماننـد بیتکـوین را مشـخص میکنـد. بـا توجـه بـه اینکـه آدرس تولیـد شـده ممکـن اسـت کـه بـر اسـاس نـوع شـبکه (mainnet و یـا testnet و ...) متفـاوت باشـد، کـاربر میبایست نوع شبکه خود را مشخص نماید.







Returns public information (public key and address based on utxo networks)

<server-url> /api/utxo/get-public-info

	Method	GET	
Request	Header	Content-Type	application/json
	ricadei	X-API-Key	Authorization Token
	Query	Keyld	کد یکتای کلید
		ChainType	نوع شبکه
	keyld		کد یکتای کلید
	publicKeyHex		کلید عمومی
Response	publicAddress	آدرس در شبکه	
	Example		uuid>", ex": " <string>", ess": "<string>"</string></string>

