
سرویس‌های صدور گواهینامه

راهنمای بهره‌برداران



واحد مرکز میانی صدور گواهی

نسخه	۱,۱۰
تاریخ	آذر ماه ۱۴۰۱
شناسه	PKI-PRA-API-DG
طبقه بندی	عمومی

فهرست مطالب

۰.....	فهرست مطالب
۲.....	تاریخچه
۲.....	پیوست‌ها
۳.....	پیشگفتار
۳.....	امکانات سرویس
۴.....	تعاریف عمومی
۵.....	چگونه از این سرویس می‌توان استفاده کرد ؟
۶.....	فرآیند صدور گواهی امضای دیجیتال
۸.....	سرویس‌های درگاه
۹.....	سرویس مرکز میانی (CA)
۹.....	GetCAList API
۱۰.....	GetCAProfileInfo API
۱۱.....	IsAvailable API
۱۲.....	سرویس گواهی (Certificate)
۱۲.....	RegisterInfo
۱۴.....	GetTrackingCodeInfo
۱۶.....	IssueCertificateByTrackingCode
۱۷.....	RevokeCertificate
۱۸.....	IsApproved
۱۹.....	RequestApprove
۲۰.....	RecievedCertConfirmation
۲۱.....	سرویس گزارشات (Reporting Service)
۲۱.....	CRLGetAllCert
۲۲.....	GetAllMobileCert
۲۳.....	GetUserCertHistory
۲۴.....	IssuingReport
۲۵.....	GetCredit
۲۶.....	پیوست شماره ۱
۲۷.....	پیوست شماره ۲
۲۸.....	پیوست شماره ۳

تاریخچه

نسخه	تاریخ	تهیه کنندگان	مرور کنندگان	توضیحات
۱,۰	۱۴۰۱/۸/۱۵	واحد مرکز میانی	واحد کنترل کیفیت	تهیه سند
۱,۱	۱۴۰۱/۸/۱۵	واحد مرکز میانی	واحد کنترل کیفیت	اضافه شدن پیوست ها به سند
۱,۲	۱۴۰۱/۸/۱۹	واحد مرکز میانی	واحد کنترل کیفیت	اضافه شدن پیوست ۳
۱,۳	۱۴۰۱/۹/۲۰	واحد مرکز میانی	واحد کنترل کیفیت	بروزرسانی متد getallmobilecert
۱,۴	۱۴۰۱/۱۰/۲۰	واحد مرکز میانی	واحد کنترل کیفیت	افزایش توضیحات برخی بخشها
۱,۵	۱۴۰۱/۱۰/۲۷	واحد مرکز میانی	واحد کنترل کیفیت	اصلاح سرویس IssuingReport
۱,۶	۱۴۰۲/۳/۳	واحد مرکز میانی	واحد کنترل کیفیت	اصلاح سرویس Registration
۱,۷	۱۴۰۲/۳/۱۷	واحد مرکز میانی	واحد کنترل کیفیت	اصلاح متد RequestApprove اضافه شدن فیلد email به Registration
۱,۸	۱۴۰۲/۵/۸	واحد مرکز میانی	واحد کنترل کیفیت	توضیحات تکمیلی در خصوص نحوه ارسال تاریخ
۱,۹	۱۴۰۲/۷/۱۷	واحد مرکز میانس	واحد کنترل کیفیت	تغییر در متد RequestApprove
۱,۱۰	۱۴۰۲/۷/۱۹	واحد مرکز میانس	واحد کنترل کیفیت	اصلاح در توضیح فرآیندها

پیوست ها

شماره	عنوان	نسخه	توضیحات
۱	جدول کد خطا	۱,۰	در این پیوست کدهای خطا برنامه وجود دارد
۲	فرم اخذ کد مشتری	۱,۰	لیست اطلاعاتی که برای دریافت کد مشتری باید ارسال شود
۳	فلوچارت صدور گواهی	۱,۰	نمون فلوچارت صدور گواهی بکار رفته در برنامه mKeyOne

پیشگفتار

استنادپذیری اسناد و عملیات الکترونیک یکی از اساسی‌ترین پایه‌های خدمات الکترونیکی بخصوصی در حوزه‌هایی که مسائل حقوقی در آن وجود دارد می‌باشد.

طبق قوانین جمهوری اسلامی ایران تنها راه اعطای وجاهت حقوقی به یک سند الکترونیکی امضای دیجیتال آن سند است. به منظور امضای دیجیتال هر شخص باید گواهی امضا دریافت کند. در این سند نحوه استفاده از سرویس‌های صدور گواهی شرکت پندار کوشک ایمن به منظور دریافت گواهی امضای دیجیتال ارائه شده است.

از ویژگی‌های اصلی این سرویس می‌تواند به موارد ذیل اشاره کرد:

- ۱- دسترسی به مراکز میانی مختلف جهت صدور گواهی فقط با یک پیاده‌سازی
- ۲- عدم وابستگی به یک مرکز میانی خاص
- ۳- پایداری بالای سرویس
- ۴- سرعت بالای سرویس
- ۵- امکان ارائه سرویس‌های پایه مثل شاهکار و ثبت احوال
- ۶- کسب درآمد از صدور گواهی

امکانات سرویس

در سرویس‌های مرکز صدور گواهی پندار قابلیت‌های زیر وجود دارد:

- ۱- ثبت اطلاعات هویتی متقاضی گواهی
- ۲- صدور گواهی امضای دیجیتال برای متقاضی
- ۳- ابطال گواهی امضای دیجیتال صاحب گواهی
- ۴- دریافت لیست گواهی‌های امضای یک فرد
- ۵- تمدید گواهی امضای دیجیتال یک فرد
- ۶- تشخیص وضعیت مرکز صدور گواهی
- ۷- بررسی وضعیت احراز هویت متقاضی گواهی
- ۸- تایید هویت یک متقاضی گواهی

تعاریف عمومی

Customercode: کد مشتری که توسط شرکت به ایشان تخصیص داده می‌شود.

LisenceNumber: شماره مجوز که توسط شرکت به مشتری تخصیص داده می‌شود.

caName: نام یا کد مرکز صدور که باید از شرکت دریافت شود.

profileName: نام پروفایل گواهی که باید از شرکت دریافت شود.

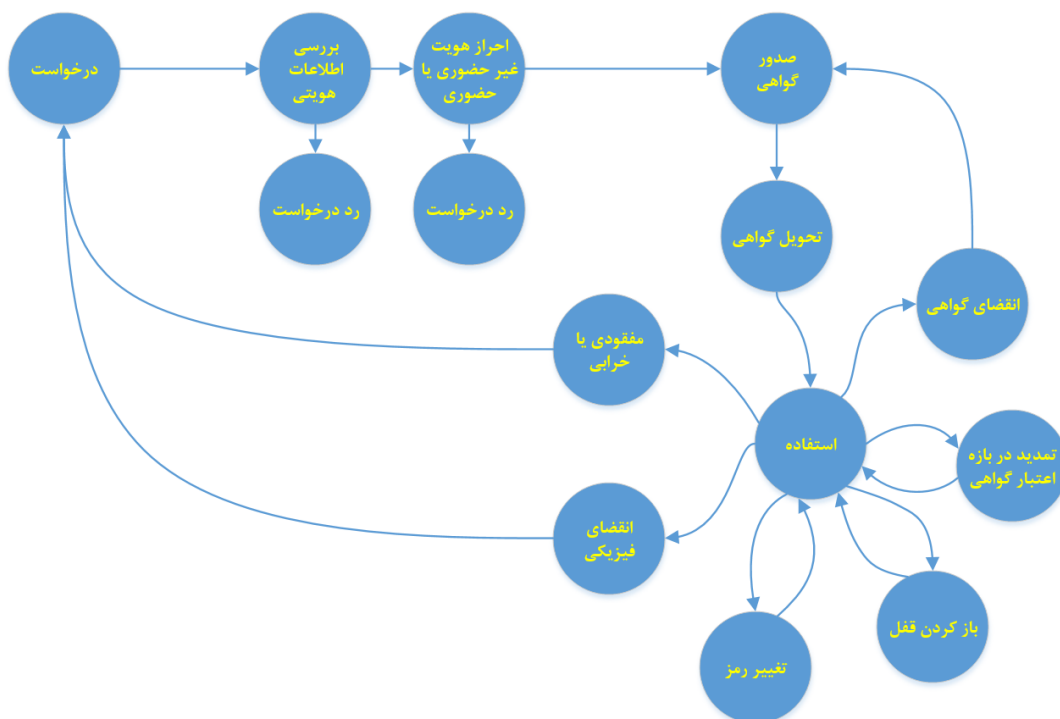
reportkey: کلید گزارش گیری که باید از شرکت دریافت شود.

متقاضی گواهی: فردی که می‌خواهد گواهی امضای دیجیتال دریافت نماید.

مشتری: شخص حقوقی طرف قرارداد شرکت پندار کوشک ایمن که از سرویس‌های برای صدور گواهی به متقاضی استفاده می‌کند.

چرخه حیات گواهی :

چرخه حیات گواهی بر روی توکن یا کارت هوشمند یا برنامه موبایل Certificate Live Cycle



چگونه از این سرویس می توان استفاده کرد ؟

برای استفاده از سرویس های صدور گواهی شرکت پندار کوشک ایمن باید مراحل زیر طی شود:

انجام دهنده	اقدام	
طرفین	امضای تفاهمنامه همکاری	۱
پندار کوشک ایمن	ارائه مستندات سرویس	۲
پندار کوشک ایمن	ایجاد کد مشتری و تخصیص دسترسی به سرویس مطابق با اطلاعات پیوست ۲	۳
مشتری	پیاده سازی سرویس در سامانه مشتری	۴
مشتری	استفاده از سرویس و کسب درآمد از آن	۵
پندار کوشک ایمن	پشتیبانی	۶

فرآیند صدور گواهی امضای دیجیتال

برای صدور گواهی امضای دیجیتال مطابق توالی زیر باید ابتدا اطلاعات متقاضی گواهی دریافت و سه متد زیر از سرویس اجرا شود



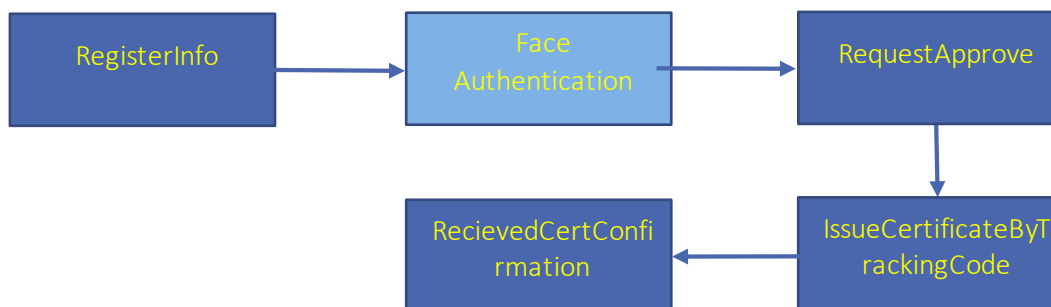
همانگونه که در نمودار فوق مشخص است، کلیات فرآیند دریافت گواهی امضای دیجیتال چنین است:

۱- ثبت اطلاعات هویتی متقاضی گواهی امضای دیجیتال و دریافت کد رهگیری

۲- ارسال CSR و دریافت گواهینامه

۳- تایید دریافت گواهینامه توسط مشتری

در فرآیند صدور غیر حضوری باید مراحل زیر طی شود:

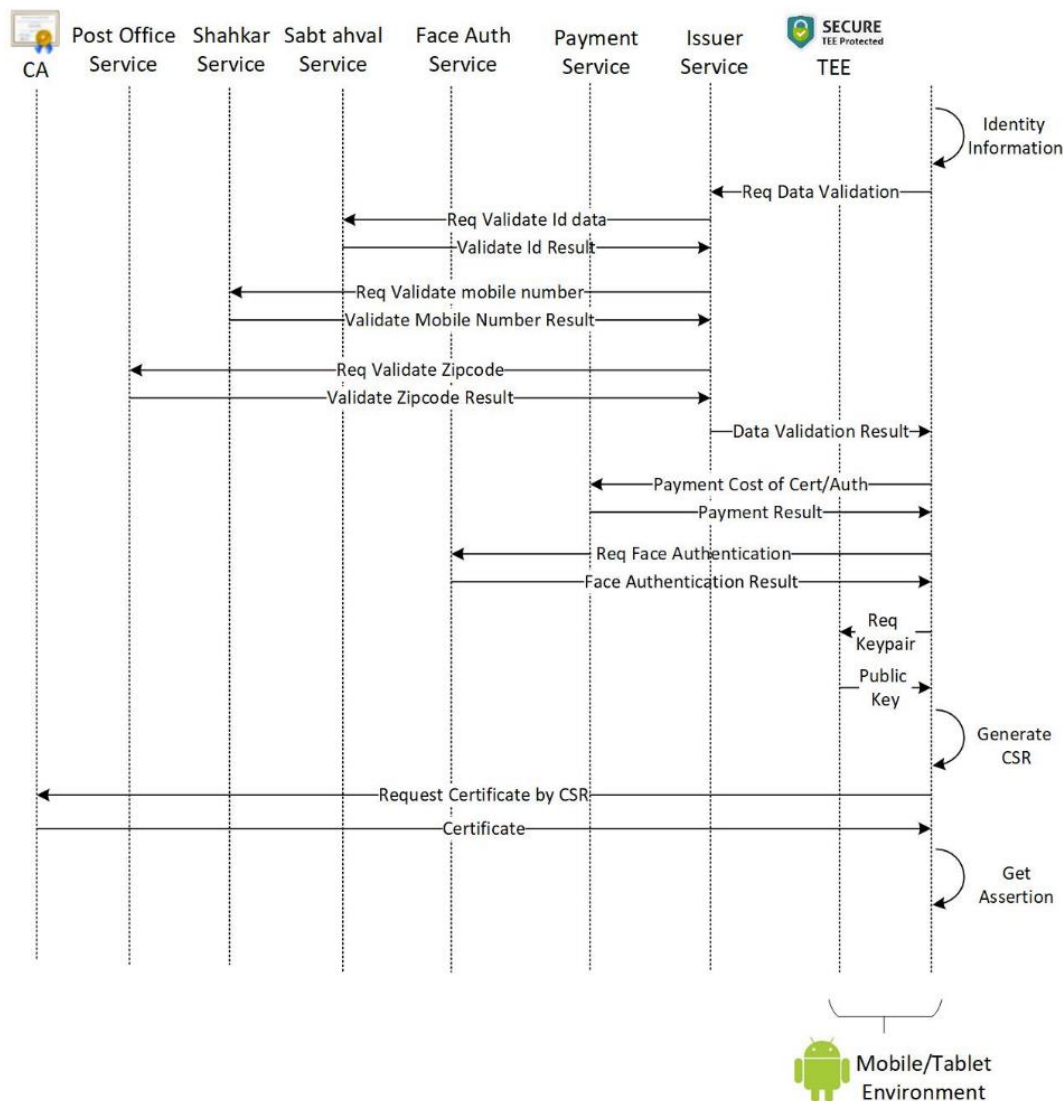


به منظور احراز هویت چهره از هر سرویس مورد تایید مرکز دولتی ریشه می‌تواند استفاده کرد.

چنانچه جهت احراز هویت غیر حضوری از سرویس‌های شرکت پندار کوشک ایمن یا شرکت‌های طرف قرارداد آن استفاده شود در متد RequestApprove باید orderId حتما درج گردد.

در ادامه، نمودار توالی صدور گواهی ارائه شده است. این نمودار صرفاً پیشنهاد بود و ارائه دهنده سرویس می‌تواند به هر نحوی که صلاح می‌داند با رعایت قوانین مرکز دولتی ریشه به مشتریان خود سرویس ارائه نماید.

نمودار توالی صدور گواهینامه الکترونیک غیر حضوری Issue Certificate Sequence Diagram



سرویس‌های درگاه

سند پیش رو مربوط به سرویس‌های درگاه RA شرکت پندار کوشک ایمن می‌باشد. جهت دریافت نگارش سرویس فعال می‌تواند از آدرس زیر استفاده کرد:

<https://api.pki.co.ir/api/GetVersion>

کلیه متدها از طریق آدرس زیر در دسترس می‌باشند:

https://api.pki.co.ir/api/{api_name}

جهت اخذ گواهی امضای دیجیتال و مدیریت چرخه حیات گواهی متدهای زیر در سرویس این شرکت وجود دارد:

CA

- ✚ [GetCAList](#)
- ✚ [GetCAProfileInfo](#)
- ✚ [IsAvailable](#)

Certificate

- ✚ [RegisterInfo](#)
- ✚ [GetTrackingCodeInfo](#)
- ✚ [IssueCertificateByTrackingCode](#)
- ✚ [RevokeCertificate](#)
- ✚ [IsApproved](#)
- ✚ [RequestApprove](#)
- ✚ [RecievedCertConfirmation](#)

Report

- ✚ [GetAllCert](#)
- ✚ [GetAllMobileCert](#)
- ✚ [GetUserCertHistory](#)
- ✚ [IssuingReport](#)
- ✚ [GetCredit](#)

نکات امنیتی :

- ۱- دسترسی به سرویس مبتنی بر امضای اختصاصی RSA Sign هر مشتری انجام شده و فاقد Username, Password است.
- ۲- کلیه متدها بر پایه تراکنش (Transaction Base) بوده و جلسه‌ای (Session) جهت انجام درخواست ایجاد نمی‌شود.
- ۳- برای هر تراکنش نیاز به تصدیق هویت متقاضی از طریق امضای اختصاصی وی (RSA Sign) در آن تراکنش است.
- ۴- هر تراکنش انجام شده با امضای مشتری بعنوان سند انکارناپذیر درخواست انجام آن تراکنش از سوی مشتری تلقی شده و سندیت حقوقی دارد و کلیه مسولیت آن بعهدہ مشتری می‌باشد.

سرویس مرکز میانی (CA)

این سرویس دارای سه API است:

GetCAList API

این متد جهت دریافت لیست مراکز میانی است که در اختیار یک مشتری می‌باشد.

ورودی این متد کد مشتری است و خروجی آن لیست مراکز میانی است که مشتری به آن دسترسی دارد.

GetCAList API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	Customercode="کد مشتری"
Response	
Status Code	200 Success / 401 Unauthorized
	{ "IsSuccess": true, "CAList": [], "ErrorCode": 0, "ErrorMessage": "" }

GetCAProfileInfo API

این متد لیست پروفایل‌های مجاز به استفاده یک مشتری را در یک مرکز صدور گواهی را در اختیار می‌گذارد.

ورودی این متد کد مشتری و نام مرکز میانی است که از متد GetCAList بدست آمده می‌باشد و خروجی آن لیست پروفایل‌هایی است که مشتری به آن دسترسی دارد.

GetCAProfileInfo API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	Customercode="کد مشتری" caName="نام مرکز صدور"
Response	
Status Code	200 Success / 401 Unauthorized
	<pre>{ "IsSuccess": true, "Profile": [{ "SubjectDNConfig": "", "ProfileName": "", "Price":, "FaceAuth": true/false, "InputType": "manually/card/mobile", "Approval": false/true, "ProductId":, "Description": "" }], "ErrorCode": 0, "ErrorMessage": "" }</pre>

IsAvailable API

این متد مشخص می‌کند یک مرکز صدور هم اکنون فعال است یا خیر

IsAvailable API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	<u>UTF8</u>
Parameters	caName= نام مرکز میانی
Response	
Status Code	200 Success / 401 Unauthorized
	<pre>{ "IsAvailable": true/false, "Description": "", "ErrorCode": 0, "ErrorMessage": "" }</pre>

سرویس گواهی (Certificate)

این سرویس دارای هفت API است:

RegisterInfo

برای دریافت گواهی باید ابتدا اطلاعات هویتی متقاضی گواهی را در مرکز ثبت و کد رهگیری دریافت کنید. برای این منظور از متد زیر استفاده می شود. در این متد با توجه به تنظیمات مربوط به مشتری ممکن است سرویس های احراز هویت ثبت احوال، شاهکار و کدپستی کنترل شود یا خیر.

Register API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "caName": "", ("01" for test) "customercode": "CustomerCode-LisenceNumber", "profileName": "", "signature": "" (Base64(Sign_RSAWithSHA1(UnicodeByte(customercode+"-"+NationalCode)))) "personData": { "NationalCode": "کد ملی", "Name": "نام فارسی", "LastName": "نام خانوادگی فارسی", "EnName": "نام انگلیسی", "EnLastName": "نام خانوادگی انگلیسی", "FatherName": "نام پدر", "IsMan": true, مرد false زن "PostalCode": "کدپستی", "Telephone": "شماره همراه", "IsForeign": false, "BirthCertificateID": "شماره شناسنامه", "BirthDate": "yyyy/mm/dd", تاریخ تولد به میلادی یا شمسی, "City": "شهر", "ProvinceName": "استان", "TokenType": "USERGENERATED/P12", "password": "فقط در نوع P12 الزامی است", "AgencySN": "شناسه شهاب/شماره نظام پزشکی/شماره پرستاری", "Email": "اختیاری" } }</pre>

	}
	}
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre> { IsSuccess = true/false, TrackingCode = کد رهگیری, Description = "{ "FirstName": "نام فارسی", "LastName": "نام خانوادگی فارسی", "EnFirstName": "نام انگلیسی", "EnLastName": "نام خانوادگی انگلیسی", "City": "شهر", "ProvinceName": "استان", "ProvinceId": "کد استان", "FatherName": "نام پدر", "AgencySN": "مقدار ورودی", "CSR": "در صورت وجود", "Certificate": "در صورت وجود" }", "ErrorCode": 0, "ErrorMessage": "" }</pre>

توجه داشته باشید :

- ۱- درج کدپستی و نام شهر و استان فقط در مرکز میانی دولتی عام اجباری است و در سایر مراکز میانی در این موارد اختیاری می باشد.
- ۲- کد رهگیری (TrackingCode) به ازای هر SubjectDN یکتا می باشد. یعنی برای یک فرد با اطلاعات ثابت همیشه کد رهگیری ثابت ارائه می شود. این موضوع در مرکز میانی دولتی عام استثنا است.
- ۳- می توانید در صورت تمایل سرویس خود را به گونه ای درخواست دهید که نام و نام خانوادگی به فارسی و لاتین توسط سرویس به شما داده شود و نیاز به درج این اطلاعات در ورودی نباشد. برای اینکار باید با واحد فروش شرکت هماهنگ کنید. در این حالت هزینه استعلام هویت نیز به هزینه گواهی اضافه می شود اما نیازی به اخذ اطلاعات هویتی فرد متقاضی گواهی نمی باشد و از صحت آن مطمئن خواهید بود.
- ۴- در صورتی که برای فرد متقاضی، گواهی فعال وجود داشته باشد در خروجی certificate و csr مقدار دهی می شود. چنانچه کلید خصوصی متناظر با این گواهی یا csr را دارید دیگر نیازی به انجام مرحله صدور گواهی نیست و از همین گواهی می توانید استفاده کنید و برای آن هزینه ای هم دریافت نمی شد. اما چنانچه کلید خصوص معادل گواهینامه را در اختیار ندارید باید حتما گواهی فعال فعلی را باطل کرده و مجدد فرآیند درخواست گواهی را از ابتدا انجام دهید.

GetTrackingCodeInfo

این متد اطلاعات هویتی متقاضی گواهی را بر می‌گرداند:

GetTrackingCodeInfo API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "nationalCode": "کد ملی", "trackingCode": "کد رهگیری", "customercode": " CustomerCode-LisenceNumber ", "sign": "(Base64(Sign_RSAWithSHA1(Unicode(nationalCode+trackingCode))))" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "ResultCode": true, "Description": "{ \"Name\": \"\", \"LastName\": \"\", \"EnName\": \"\", \"EnLastName\": \"\", \"NationalCode\": \"\", \"BirthCertificateID\": \"\", \"FatherName\": \"\", \"EnFatherName\": null, \"IssueCardDate\": null, \"Organization\": null, \"EnOrganization\": null, \"OrganizationUnit\": null, \"EnOrganizationUnit\": null, \"AgencySN\": null, \"Affiliation\": null, \"EnAffiliation\": null, \"IssuerIdentification\": null, \"ValidityDuration\": null, \"BirthDate\": \"\", \"IsMan\": \"\", \"City\": \"\", \"EnCity\": null, \"Customize1\": \"\", \"Customize2\": null, \"Customize3\": null, \"Customize4\": null, \"GUID\": null,</pre>

```
\EndEntityProfile\":null,  
\ExpirationEnglishDate\":null,  
\IsForeign\":false,  
\Country\":null,  
\Address\":\"\",  
\PostalCode\":\"\",  
\Telephone\":\"\",  
\ProvinceName\":\"\",  
\ProvinceId\":},  
  \"Message\": \"Success\"  
}
```

* در نسخه جاری مقدار version برای الگوها همیشه ۱,۰ است.

IssueCertificateByTrackingCode

این متد جهت صدور گواهی برای متقاضی گواهی مبتنی بر کدرهگیری می باشد:

IssueCertificateByTrackingCode API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "caName": "", "profileName": "", "trackingCode": "", "csr": "", (base64(csr)) "paymentId": "", "signature": "", (Base64(Sign_RSAWithSHA1(csr))) "customercode": " CustomerCode-LisenceNumber ", "password": " فقط در نوع P12 الزامی است " }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ IsSuccess = true/false, Certificate = Base64(Certificate), PaymentStatus = Payment Status, Description = Error Description, CN = Certificate CN, IssuerName = Certificate Issuer, ValidFrom = Certificate NotBefore, ValidTo = Certificate .NotAfter, "ErrorCode": 0, "ErrorMessage": "" }</pre>

توجه : در نوع گواهی P12 مقدار csr باید حتما "none" باشد.

RevokeCertificate

این متد جهت ابطال گواهی می باشد:

RevokeCertificate API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "certificate": "", (base64(certificate)) "signature": "", (Base64(Sign_RSABWithSHA1(certificate))) "customercode": " CustomerCode-LisenceNumber ", "revokeCertReason": 2 }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "IsSuccess" = true/false, "Description" = revokeDescription, "ErrorCode": 0, "ErrorMessage": "" }</pre>

IsApproved

با کمک این متد می‌توان تشخیص داد آیا اطلاعات هویت یک متقاضی گواهی که نیاز به احراز هویت حضوری دارد تایید شده است یا خیر:

IsApproved API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "trackingCode":"" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "ResultCode": false/true, "Description": "", "Message": "Success/Unsuccess" }</pre>

RequestApprove

چنانچه فردی متقاضی دریافت گواهی است که نیاز به احراز هویت حضوری دارد با کمک این متد مرکز احراز هویت حضوری هویت فرد را در سامانه تایید می نماید

RequestApprove API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "nationalCode": "کد ملی", "trackingCode": "کد رهگیری", "customercode": " CustomerCode-LisenceNumber ", "approver": "نام تایید کننده اطلاعات", "sign": "Base64(Sign_RSAWithSHA1(Unicode(nationalCode+ trackingCode + approver)))", "approverSign": "Base64(Sing_CMSEDetach(Unicode(nationalCode+ trackingCode + approver))), "orderId": "شناسه احراز هویت" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "ResultCode": false/true, "Description": "", "Message": "Success/Unsuccess", "ErrorCode": 0, "ErrorMessage": "" }</pre>

توجه :

- ۱- فیلد approverSign در احراز هویت حضوری الزامی است. در این حالت فردی احراز را انجام می دهد باید اطلاعات را طبق روش فوق امضا و ارسال نماید. در احراز هویت غیرحضوری این فیلد خالی باید باشد.
- ۲- فیلد orderId اختیاری می باشد و فقط در صورت استفاده از مکانیزم احراز هویت شرکت پندار کوشک ایمن درج این فیلد الزامی است.

RecievedCertConfirmation

پس از اینکه گواهی با موفقیت صادر شد با کمک این متد می‌توان به مرکز صدور اعلام کرد که گواهی توسط متقاضی دریافت شده است. اجرای این متد الزامی نیست اما در تایید نهایی اطلاعات بسیار مفید خواهد بود.

RecievedCertConfirmation API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "certificate": "", "signature": "(Base64(Sign_RSAWithSHA1(Unicode(certificate))))", "customercode": " CustomerCode-LisenceNumber ", "trackingCode": "" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "IsSuccess" = true/false, "Description" = "" , "ErrorCode": 0, "ErrorMessage": "" }</pre>

سرویس گزارشات (Reporting Service)

این سرویس دارای چهار API است:

GetAllCert

با کمک این متد کلیه گواهی‌های فعال یک فرد در مراکز میانی طرف قرارداد پندار کوشک ایمن لیست می‌شود:

GetAllCert API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	SerialNumber= شماره ملی شخص حقیقی یا شناسه ملی شخص حقوقی
Response	
Status Code	200 Success
200 Schema	Boolean
	لیست گواهی‌های فرد

از آنجا که این متد اطلاعات را از مراکز میانی مختلف دریافت می‌کند، ممکن است سرعت پاسخ‌دهی پایینی داشته باشد.

GetAllMobileCert

با کمک این متد کلیه گواهی‌های فعال یک فرد که گواهی آن از سرویس صدور گواهی شرکت پندار کوشک ایمن دریافت شده لیست می‌شود:

GetAllMobileCert API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	NationalCode= (اختیاری) کد ملی فرد TrackingCode= (اختیاری) کد رهگیری گواهی CAName= (اختیاری) نام مرکز صدور گواهینامه CustomerCode= (اختیاری) کد مشتری درج کد ملی یا شماره رهگیری یکی از آنها اجباری می‌باشد و اولویت با کد رهگیری است در صورت درج نام مرکز صدور فقط گواهی‌های آن مرکز نمایش داده می‌شود در صورت درج ک مشتری فقط گواهی‌های آن مشتری نمایش داده می‌شود
Response	
Status Code	200 Success
200 Schema	Boolean
	لیست گواهی‌های فرد

GetUserCertHistory

با کمک این متد کلیه گواهی‌های فعال یک فرد که گواهی آن از سرویس صدور گواهی شرکت پندار کوشک ایمن دریافت شده لیست می‌شود:

GetUserCertHistory API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "SerialNumber": "", "customercode": "CustomerCode-LisenceNumber ", "signature": "" (Base64(Sign_RSAWithSHA1(Unicode(SerialNumber+rnd))), "rnd": "" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "IsSuccess": true/false, "CertList": [{ "Id": "", "TrackingCode": "", "Status": "Registered/Issued/Revoked", "Issuer": "", "Certificate": "", "RegisterDate": "", "IssueDate": "", "RevokeDate": "" }], "ErrorCode": 0, "ErrorMessage": "" }</pre>

IssuingReport

این متد جهت دریافت گزارش آمار گواهی‌های ثبت‌شده، صادر شده و یا باطل شده می‌باشد:

IssuingReport API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "reportkey":""," کد گزارش گیری منحصر به هر مشتری", "customercode":"CustomerCode", "startdate":"yyyy/mm/dd", "enddate":"yyyy/mm/dd", "type":"PerCA/PerCA&Status/detail", "id":"ردیف گواهی" }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	گزارش گواهی‌های صادر شده به تفکیک مرکز صدور در حالت detail به دلیل پاسخدهی سریع سرویس فقط ۱۰۰ مورد بر می‌گردد و برای دریافت اطلاعات بیشتر سرویس باید با id آخر مرحله قبل مجدد فراخوانی شود

GetCredit

این متد جهت دریافت گزارش آمار گواهی‌های ثبت‌شده، صادر شده و یا باطل شده می‌باشد:

GetCredit API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{ "reportkey":""," کد گزارش گیری منحصر به هر مشتری , "customercode":"CustomerCode", }</pre>
Response	
Status Code	200 Success
200 Schema	Boolean
	<pre>{ "IsSuccess": true, "Credit": "0", "Description": "", "ErrorCode": 0, "ErrorMessage": "" }</pre>

پیوست شماره ۱

کد خطا	شرح خطا
۰	اجرای موفق
۱	خطا در اجرای برنامه
۲	عملیات ناموفق
۳	عدم پشتیبانی از دستور
۱۰۰۱	شما با این اطلاعات گواهینامه فعال دارید برای دریافت گواهی ابتدا باید آن را باطل کنید
۱۰۰۲	خطای ناشناخته در مرحله بروزرسانی اطلاعات
۱۰۰۳	نام وارد شده با کد ملی انطباق ندارد
۱۰۰۴	نام خانوادگی وارد شده با کد ملی انطباق ندارد
۱۰۰۵	مرکز میانی نماد قطع است
۱۱۰۰	مرکز صدور یا پروفایل انتخاب شده نامعتبر است
۱۱۰۱	مرکز صدور گواهینامه نامعتبر است
۱۱۰۲	شما به این مرکز صدور دسترسی ندارید
۱۱۰۳	درج کد ملی الزامی است
۱۱۰۴	درج شماره تلفن همراه الزامی است
۱۱۰۵	امضا کننده نامه در خواست گواهینامه مجاز به امضای این نامه نمی باشد
۱۱۰۶	امضای نامه در خواست گواهینامه نامعتبر است
۱۱۰۷	گواهی امضا کننده نامه در خواست باطل شده است
۱۱۰۸	گواهی امضا کننده نامه در خواست ناشناخته است
۱۱۰۹	در اعتبارسنجی گواهی امضا کننده نامه در خواست خطا رخ داد
۱۱۱۰	کد رهگیری احراز هویت نشده است
۱۱۱۱	"کد رهگیری نامعتبر است
۱۱۱۲	گواهی برای ابطال یافت نشد
۱۱۱۳	این گواهی توسط شما صادر نشده و حق ابطال آن را ندارید
۱۱۱۴	این گواهی قبلا باطل شده است
۱۲۰۰	امضای بسته نامعتبر است
۱۲۰۱	کد پرداخت نامعتبر است
۱۲۰۲	مبلغ پرداختی با هزینه گواهی انطباق ندارد
۱۲۰۳	کد مشتری نامعتبر است

پیوست شماره ۲

اطلاعات مورد نیاز جهت تعریف کد مشتری به شرح زیر می باشد. این اطلاعات به همراه کلید عمومی مشتری باید به آدرس ایمیل sales@pki.co.ir با عنوان "درخواست ایجاد کد مشتری در سرویس صدور گواهی" ارسال شود.

- ۱- نام شرکت
- ۲- شناسه ملی شرکت
- ۳- کدپستی و آدرس شرکت
- ۴- آدرس سایت شرکت
- ۵- آدرس ایمیل شرکت
- ۶- تلفن شرکت
- ۷- نام و نام خانوادگی مدیرعامل
- ۸- شماره ملی مدیر عامل
- ۹- تلفن همراه مدیرعامل
- ۱۰- کلید عمومی با طول کلید ۱۰۲۴ الگوریتم RSA اختصاصی شرکت

پیوست شماره ۳

فرآیند صدور گواهی در برنامه موبایل

