



شرکت فن آوران اعتماد راهبر  
Raahbar Trust Tech.

---

## سرویس‌های RA

---

راهنمای بهره‌برداران



## تاریخچه بازنگری

توضیحات		ورژن	تاریخ
واحد CA	ایجاد سند	۱,۰	۱۴۰۱/۰۸/۰۲
واحد CA	تصحیحات نگراشی	۱,۱	۱۴۰۲/۰۵/۱۵





## فهرست مطالب

۱	پیشگفتار
۱	امکانات سرویس
۲	تعاریف عمومی
۳	چگونه از این سرویس می‌توان استفاده کرد؟
۴	فرآیند صدور گواهی امضای دیجیتال
۶	سرویس‌های درگاه
۷	سرویس مرکز میانی (CA)
۷	Get CALi st API
۸	Get CAProfi l eI nf o API
۹	I sAvai l abl e API
۱۰	سرویس گواهی (Cert i fi cat e)
۱۰	Regi st erI nf o
۱۲	Get Tracki ngCodeI nf o
۱۴	I ssueCert i fi cat eByTracki ngCode
۱۵	RevokeCert i fi cat e
۱۶	I sApproved
۱۷	Request Approve
۱۸	Reci vedCert Conf i rmat i on
۱۹	سرویس گزارشات (Report i ng Servi ce)
۱۹	CRLGet Al l Cert
۲۰	Get Al l Mbi l eCert
۲۱	Get UserCert Hi st ory
۲۲	I ssui ngReport
۲۳	Get Credi t
۲۴	پیوست شماره ۱





پیوست شماره ۲..... ۲۵

پیوست شماره ۳..... ۲۶



## 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 فن‌آوران اعتماد راهبر 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 پیاده سازی
- 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 شرکت فن‌آوران اعتماد راهبر قابلیت های 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 گواهی های 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

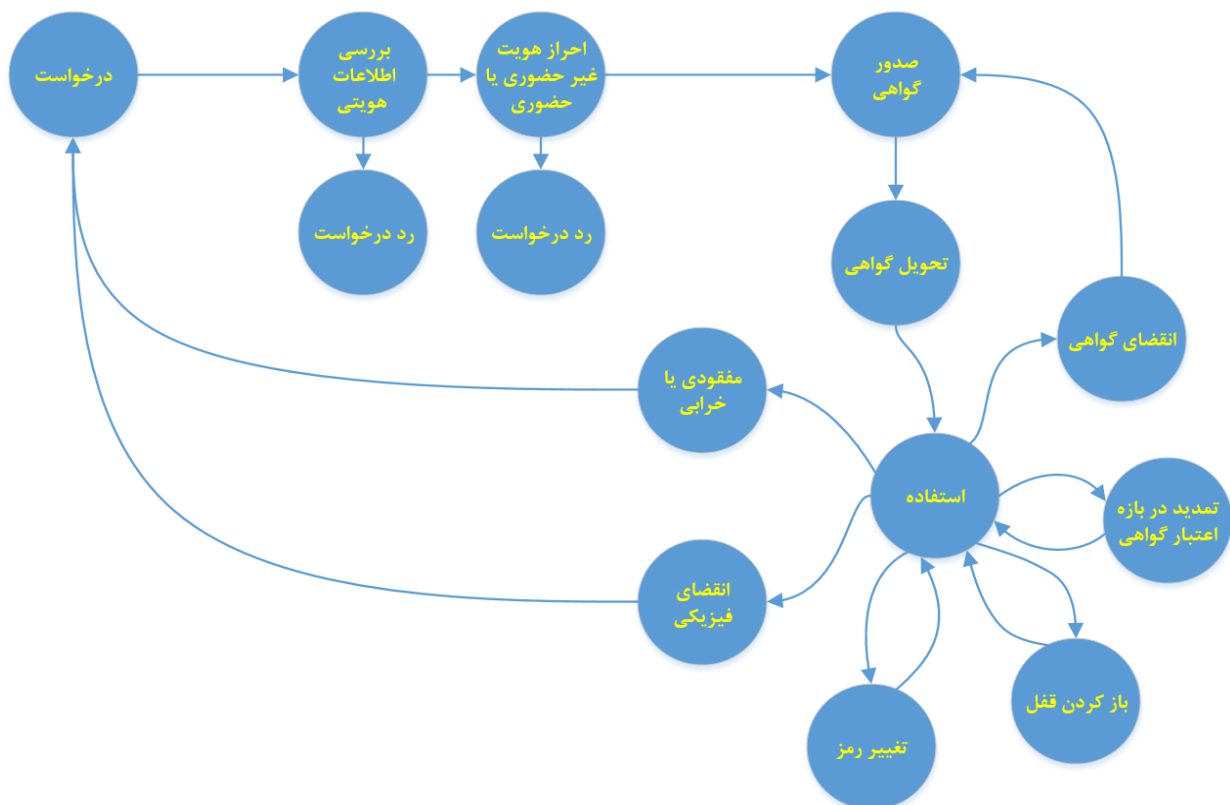
- Customercode : کد مشتری که توسط شرکت به ایشان تخصیص داده می‌شود.
- LisenceNumber : شماره مجوز که توسط شرکت به مشتری تخصیص داده می‌شود.
- caName : نام یا کد مرکز صدور که باید از شرکت دریافت شود.
- profileName : نام پروفایل گواهی که باید از شرکت دریافت شود.
- reportkey : کلید گزارش گیری که باید از شرکت دریافت شود.

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

مشتری: شخص حقوقی طرف قرارداد شرکت فن‌آوران اعتماد راهبر که از سروی‌های 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 می‌توان استفاده کرد ؟

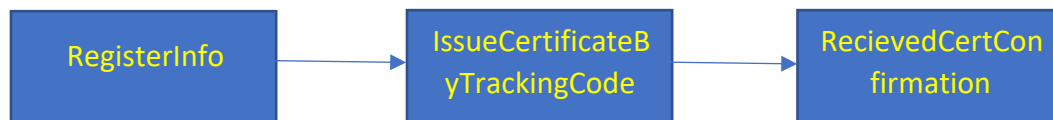
برای استفاده از سرویس‌های صدور گواهی شرکت فن‌آوران اعتماد راهبر باید مراحل زیر طی شود:

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



## 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



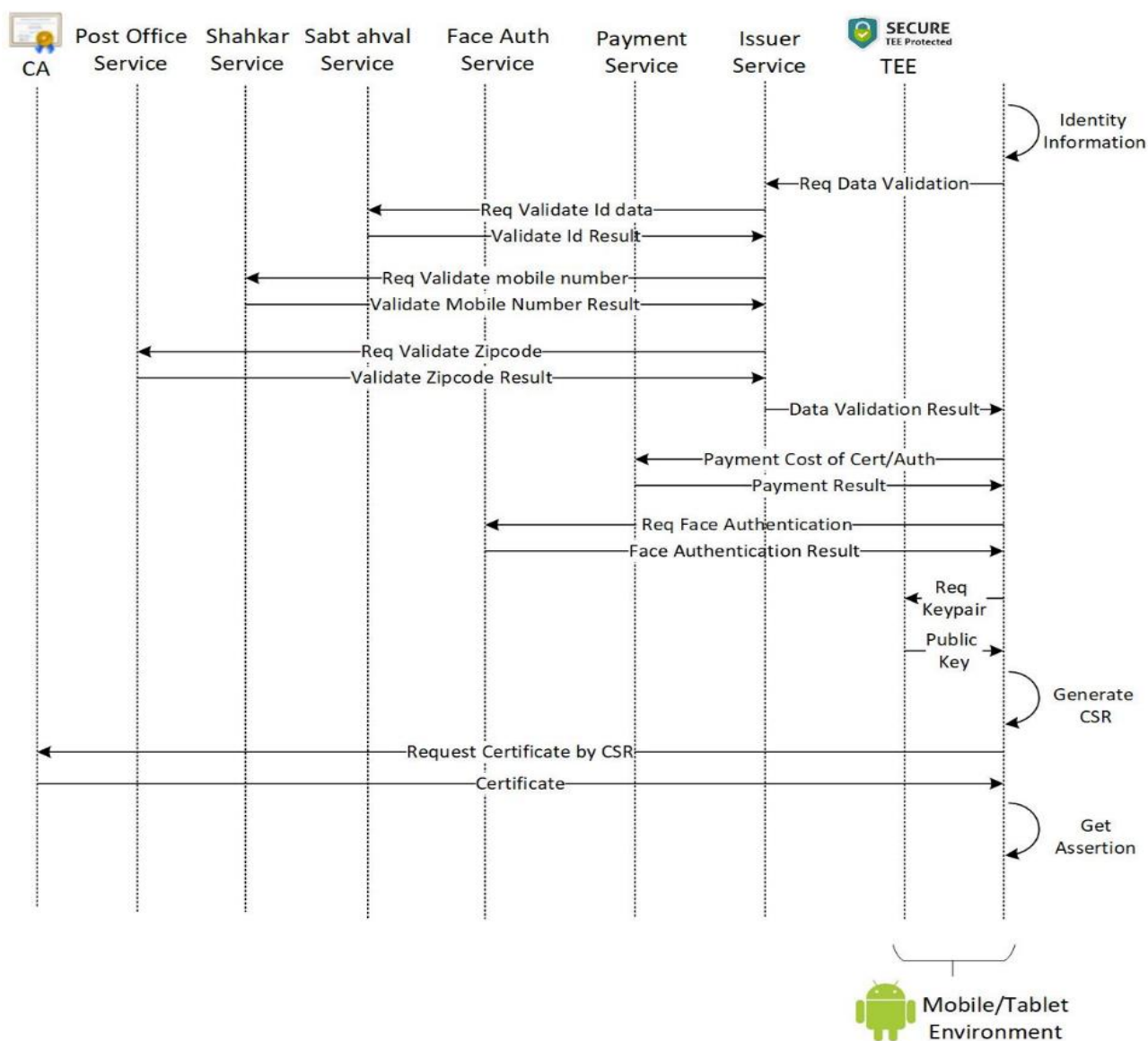
همانگونه که در نمودار فوق مشخص است، کلیات فرآیند دریافت گواهی امضای دیجیتال چنین است:





- ۱- ثبت اطلاعات هویتی متقاضی گواهی امضای دیجیتال و دریافت کد رهگیری
- ۲- ارسال CSR و دریافت گواهینامه
- ۳- تایید دریافت گواهینامه توسط مشتری

## نمودار توالی صدور گواهینامه الکترونیک غیر حضوری Issue Certificate Sequence Diagram





## سرویس‌های درگاه

سند پیش رو مربوط به سرویس‌های درگاه RA شرکت فن‌آوران اعتماد راهبر نگارش ۱,۳ می‌باشد. جهت دریافت نگارش سرویس فعال می‌تواند از آدرس زیر استفاده کرد:




<https://api.raahbartrust.ir/api/GetVersion>

کلید متدها از طریق آدرس زیر در دسترس می‌باشند:








[https://api.raahbartrust.ir/api/{api\\_name}](https://api.raahbartrust.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- کلید متدها بر پایه تراکنش (Transact i on Base) بوده و جلسه‌ای (Sessi on) 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 کلید مسولیت آن بعهده 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:

GetCAList API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	<a href="#">UTF8</a>
Parameters	customercode
Response	
Status Code	۲۰۰ Success / ۴۰۱ Unauthorized
	<pre>{   "IsSuccess": true,   "CAList": [],   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>





## GetCAProfileInfo API

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

GetCAProfileInfo API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	<a href="#">UTF8</a>
Parameters	caName
Response	
Status Code	۲۰۰ Success / ۴۰۱ Unauthorized
	<pre>{   "IsSuccess": true,   "Profile": [ {     "SubjectDNConfig": "",     "ProfileName": "",     "Price":,     "FaceAuth": true/false,     "InputType": "manually/card/mobile",     "Approval": false/true,     "ProductId":,     "Description": ""   }],   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>





## IsAvailable API

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

IsAvai l abl e API	
Request	
Method	Get
Body Content-Type	application/json
Encoding	<a href="#">UTF8</a>
Parameters	caName
Response	
Status Code	۲۰۰ Success / ۴۰۱ Unauthorized
	<pre>{   "IsAvailable": true/false,   "Description": "",   "ErrorCode": ۰,   "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 می‌شود. در این متد با توجه به تنظیمات مربوط به مشتری ممکن است سرویس‌های 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": "", ("۰۱" for test)   "customer code": "CustomerCode-Li senceNumber",   "profileName": "",   "signature": ""   (Base64(Sign_RSAWithSHA)(UnicodeByte(customer code+"-   "+National Code))))   "personData":   {     "Name": "نام فارسی",     "LastName": "نام خانوادگی فارسی",     "EnName": "نام انگلیسی",     "EnLastName": "نام خانوادگی انگلیسی",     "National Code": "کد ملی",     "IsMan": true, "زن false",     "Postal Code": "کدپستی",     "Telephone": "شماره همراه",     "IsForeign": false,     "BirthCertificateID": "شماره شناسنامه",     "BirthDate": "تاریخ تولد به میلادی",     "City": "شهر",     "ProvinceName": "استان"   } }</pre>





	}
Response	
Status Code	۲۰۰ Success
۲۰۰ 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"   }",   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>





## GetTrackingCodeInfo

این متد اطلاعات هویتی متقاضی گواهی را بر می‌گرداند:

Get TrackingCodeInfo API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{   "national Code": "کد ملی",   "trackingCode": "کد رهگیری",   "customerCode": "CustomerCode-Li senceNumber ",   "sign":     "(Base64(Sign_RSAAWithSHA1(Unicode(national Code+trackingCode))))"</pre>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	<pre>{   "Result Code": true,   "Description": "{ \"Name\": \"\",     \"Last Name\": \"\",     \"EnName\": \"\",     \"EnLast Name\": \"\",     \"National Code\": \"\",     \"BirthCertificateID\": \"\",     \"FatherName\": \"\",     \"EnFatherName\": null,     \"IssueCardDate\": null,     \"Organization\": null,     \"EnOrganization\": null,     \"OrganizationUnit\": null,     \"EnOrganizationUnit\": null,     \"AgencySM\": null,</pre>





```
\ "Affliati on\ ":nul l ,
\ "EnAffli ati on\ ":nul l ,
\ "IssuerI denti fication\ ":nul l ,
\ "Val i di tyDurati on\ ":nul l ,
\ "Bi rthDate\ ":\"\",
\ "IsMan\ ":\"\",
\ "Ci ty\ ":\"\",
\ "EnCi ty\ ":nul l ,
\ "Cust omi ze\ ":\"\",
\ "Cust omi ze۲\ ":nul l ,
\ "Cust omi ze۳\ ":nul l ,
\ "Cust omi ze۴\ ":nul l ,
\ "GUI D\ ":nul l ,
\ "EndEnt i tyProfi le\ ":nul l ,
\ "Expi rati onEngl i shDate\ ":nul l ,
\ "IsForei gn\ ":fal se,
\ "Count ry\ ":nul l ,
\ "Address\ ":\"\",
\ "Post al Code\ ":\"\",
\ "Tel ephone\ ":\"\",
\ "Provi nceName\ ":\"\",
\ "Provi nceId\ ":} ",
  "Message": "Success"
}
```

\* در نسخه جاری مقدار versi on برای الگوها همیشه ۱,۰ است.



## IssueCertificateByTrackingCode

این متد جهت صدور گواهی برای متقاضی گواهی مبتنی بر کد رهگیری می‌باشد:

API IssueCertificateByTrackingCode	
<b>Request</b>	
<b>Method</b>	Post
<b>Body Content-Type</b>	application/json
<b>Encoding</b>	UTF8
<b>Body</b>	<pre>{   "caName": "",   "profileName": "",   "trackingCode": "",   (base64(csr)) "csr": "",   "paymentId": "",   "signature": "" (Base64(Sign_RSAWithSHA1(csr)))   "customercode": "CustomerCode-LisenceNumber " }</pre>
<b>Response</b>	
<b>Status Code</b>	۲۰۰ Success
<b>۲۰۰ Schema</b>	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": ۰,   "ErrorMessage": "" }</pre>



## RevokeCertificate

این متد جهت ابطال گواهی می باشد:

RevokeCertificate API	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF <sup>۸</sup>
Body	<pre>{   "certificate" : "", (base64(certificat))   "signature" : "",   (Base64(Sign_RSAWithSHA1(certificat)))   "customercode": " CustomerCode-LisenceNumber   ",   "revokeCertReason" : ۲ }</pre>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	<pre>{   "IsSuccess" = true/false,   "Description" = revokeDescription,   "ErrorCode": ۰,   "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	UTF^
Body	{ "trackingCode": "" }
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	{ "ResultCode": false/true, "Description": "", "Message": "Success/Unsuccess" }



## 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_RSAShA1(Unicode(nationalCode   + trackingCode + approver))))"</pre>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	<pre>{   "ResultCode": false/true,   "Description": "",   "Message": "Success/Unsuccess",   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>



## RecievedCertConfirmation

پس از اینکه گواهی با موفقیت صادر شد با کمک این متد می توان 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	
<b>Request</b>	
<b>Method</b>	Post
<b>Body Content-Type</b>	application/json
<b>Encoding</b>	UTF8
<b>Body</b>	<pre>{   "certificate": "",   "signature" :   "(Base64(Sign_RSAShWithSHA1(Unicode(certficate))))",   "customercode": " CustomerCode-LisenceNumber ",   "trackingCode" : "" }</pre>
<b>Response</b>	
<b>Status Code</b>	۲۰۰ Success
<b>۲۰۰ Schema</b>	Boolean
	<pre>{   "IsSuccess" = true/false,   "Description" = " " ,   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>



## سرویس گزارشات (Reporting Service)

این سرویس دارای چهار API است:

### CRLGetAllCert

با کمک این متد کلیه گواهی های فعال یک فرد در مراکز میانی طرف قرارداد شرکت فن‌آوران اعتماد راهبر لیست می شود:

API Get All Cert	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	SerialNumber=شماره ملی شخص حقیقی یا شناسه ملی شخص حقوقی
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	لیست گواهی های فرد



## GetAllMobileCert

با کمک این متد کلیه گواهی های فعال یک فرد که گواهی آن از سرویس صدور گواهی شرکت فن‌آوران اعتماد راهبر دریافت شده لیست می شود:

API GetAllMobileCert	
Request	
Method	Get
Body Content-Type	application/json
Encoding	UTF8
Parameters	<p>NationalCode= کد ملی فرد (اختیاری)</p> <p>TrackingCode= کد رهگیری گواهی (اختیاری)</p> <p>CAName= نام مرکز صدور گواهینامه (اختیاری)</p> <p>CustomerCode= کد مشتری (اختیاری)</p> <p>درج کد ملی یا شماره رهگیری یکی از آنها اجباری می باشد و اولویت با کد رهگیری است</p> <p>در صورت درج نام مرکز صدور فقط گواهی های آن مرکز نمایش داده می شود</p> <p>در صورت درج ک مشتری فقط گواهی های آن مشتری نمایش داده می شود</p>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	لیست گواهی های فرد





## GetUserCertHistory

با کمک این متد کلیه گواهی‌های فعال یک فرد که گواهی آن از سرویس صدور گواهی شرکت فن‌آوران اعتماد راهبر 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_RSAWithSHA \ (Unicode(SerialNumber+rnd)))) ,   "rnd": "" یک رشته اتفاقی }</pre>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
	<pre>{   "IsSuccess": true/false,   "CertList": [     {       "Id": "",       "TrackingCode": "",       "Status": "Registered/Issued/Revoked",       "Issuer": "",       "Certificate": "",       "RegisterDate": "",       "IssueDate": "",       "RevokeDate": ""     }   ],   "ErrorCode": ۰,   "ErrorMessage": "" }</pre>



## IssuingReport

این متد جهت دریافت گزارش آمار گواهی های ثبت شده، صادر شده و یا باطل شده می‌باشد:

API IssuingReport	
Request	
Method	Post
Body Content-Type	application/json
Encoding	UTF8
Body	<pre>{   "reportkey": "",   "customercode": "CustomerCode",   "startdate": "yyyy/mm/dd",   "enddate": "yyyy/mm/dd",   "type": "PerCA/PerCA&amp;Status/detail" }</pre>
Response	
Status Code	۲۰۰ Success
۲۰۰ Schema	Boolean
گزارش گواهی های صادر شده به تفکیک مرکز صدور	



## GetCredit

این متد جهت دریافت گزارش آمار گواهی های ثبت شده، صادر شده و یا باطل شده می باشد:

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	۲۰۰ Success
۲۰۰ Schema	Boolean
	<pre>{   "IsSuccess": true,   "Credit": "۰",   "Description":"","",   "ErrorCode": ۰,   "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
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 درخواست گواهینامه مجاز به امضای این نامه نمی باشد
۱۱۰۶	امضای نامه درخواست گواهینامه نامعتبر است
۱۱۰۷	گواهی امضا کننده نامه درخواست باطل شده است
۱۱۰۸	گواهی امضا کننده نامه درخواست ناشناخته است
۱۱۰۹	در اعتبارسنجی گواهی امضا کننده نامه درخواست 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 قبلاً 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



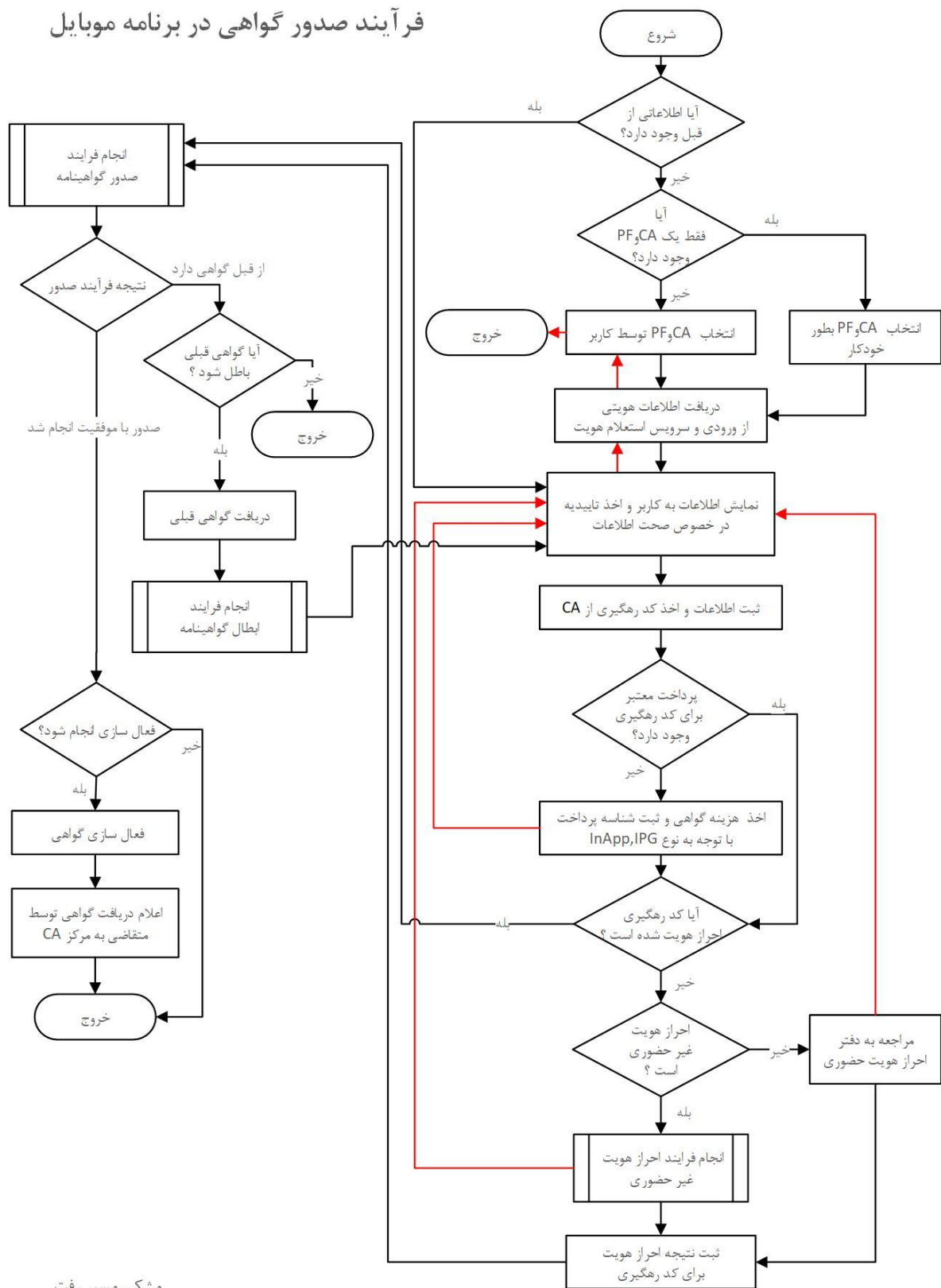
## پیوست شماره ۲

اطلاعات مورد نیاز جهت تعریف کد مشتری به شرح زیر می باشد. این اطلاعات به همراه کلید عمومی مشتری باید به آدرس ایمیل [cto@aaahbartrust.com](mailto:cto@aaahbartrust.com) 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 مدیرعامل
- ۹- تلفن همراه مدیرعامل
- ۱۰- کلید عمومی با طول کلید ۱۰۲۴ الگوریتم RSA اختصاصی شرکت

### پیوست شماره ۳

#### فرآیند صدور گواهی در برنامه موبایل



مشکی مسیر رفت  
قرمز مسیر برگشت