

بسمه تعالی



گروه نرم افزار پارت  
Part Software Group

# مستندات فنی پلتفرم احراز هویت غیرحضوری فراشناسا

تیم فراشناسا  
با همکاری تیم پشتیبانی فنی گروه نرم افزار پارت  
بهار 1400



## فهرست مطالب

2	تعریف اجزای سیستم
2	فراشناسا
2	پذیرنده
2	کاربر
2	نیازمندی های webservice
2	پذیرنده
3	کاربر
3	توصیف فرایند احراز هویت
4	مدل آفلاین
4	مدل آنلاین
5	پنل مدیریت
6	نحوه استفاده از سرویس
6	لیست API های مورد نیاز
6	validateToken
7	authenticateCallback
10	نکات
11	پیوست ها
11	پیوست 1: دیاگرام فرآیند در مدل آفلاین
12	پیوست 2: دیاگرام فرآیند در مدل آنلاین
14	پیوست 3: نمونه تصاویر اجرای سامانه

## اجزای سیستم

### فراشناسا

احراز هویت فرآیندی است که طی آن درستی هویت یک فرد شناسایی و تأیید می‌گردد. امروزه تأیید هویت افراد با استفاده از الگوریتم‌های مبتنی بر چهره فرد، به دلیل عمومیت و در دسترس بودن این عضو از بدن به یکی از زمینه‌های پرطرفدار در حوزه احراز هویت دیجیتال تبدیل شده است. سامانه احراز هویت هوش مصنوعی شرکت پارت که در این سند به نام «فراشناسا» شناخته می‌شوند، سامانه‌ای بیومتریک و مبتنی بر فناوری تشخیص چهره و صوت است که با قابلیت‌های گوناگون خود، امکان احراز هویت الکترونیکی را با امنیت و دقت بالا میسر کرده است. فراشناسا با صدها تجزیه و تحلیل مبتنی بر هوش مصنوعی، الگوریتم‌ها و مقایسه بیومتریک چهره، نسل جدیدی از سرویس احراز هویت دیجیتال را برای بازارها، سرویس‌های مبتنی بر وب و سازمان‌های دولتی و خصوصی طراحی کرده است. رویکرد لایه لایه ما برای تأیید اسناد هویتی، دقت بالا و تجربه موفق عملی در سطح گسترده، باعث شده این محصول شرکت پارت به عنوان یکی از کم خطا ترین و دقیق‌ترین سرویس‌های احراز هویت شناخته شود.

### پذیرنده

برخی از خدماتی که سازمان‌ها ارائه می‌دهند نیاز به احراز هویت کاربران دارد. با توجه به وضعیت کنونی جامعه احراز هویت حضوری کاربران برای سازمان‌ها با چالش‌هایی روبه‌رو است، به همین دلیل ارائه‌ی احراز هویت غیرحضوری به امری الزامی تبدیل شده است. در این سند به سازمان‌هایی که سامانه فراشناسا را به عنوان راه حل احراز هویت غیرحضوری خود انتخاب کرده‌اند؛ پذیرنده گفته می‌شود.

### کاربر

کاربر فردی است که پذیرنده خواستار احراز هویت او است؛ از این رو او را برای انجام مراحل احراز هویت به سامانه فراشناسا منتقل می‌کند.

## نیازمندی‌های webService

### پذیرنده

به منظور دریافت سرویس احراز هویت فراشناسا، لازم است پذیرنده، موارد زیر را آماده و یا ارایه دهد. (جزئیات فنی در ادامه آمده است). وجود محیط‌های توسعه<sup>1</sup> و تست<sup>2</sup> و عملیات<sup>3</sup> الزامی است.

1- امکان ارسال تصویر مرجع کاربر به منظور انجام پردازش‌های احراز (به عنوان مثال تصویر ثبت احوال کاربر)

<sup>1</sup> Develop

<sup>2</sup> Test

<sup>3</sup> Production

- 2- تخصیص شناسه یکتا (در این سند توکن نامیده می‌شود) به کاربر خود به منظور شناسایی شدن در سامانه فرانشاسا
  - 3- آدرس بازگشت<sup>4</sup> به منظور بازگرداندن کاربر به پذیرنده در صورت خطا یا اتمام فرایند احراز
  - 4- دریافت آدرس فرانشاسای اختصاصی خود برای هدایت<sup>5</sup> کاربر با توکن به سامانه.
  - 5- آماده‌سازی دو API (بر مبنای معماری RESTfull API) به منظور استعلام توکن و دریافت تصویر ثبت احوال و اعلام نتیجه احراز هویت کاربر. در صورت وجود محدودیت‌های ارتباطی، لطفا در قرارداد ذکر شود تا IP اختصاص داده شده به پذیرنده جهت انجام تنظیمات اعلام شود.
- یک API با نام " validateToken " که با فراخوانی آن توسط فرانشاسا، توکن کاربر اعتبارسنجی شده و در صورت معتبر بودن، تصویر مرجع کاربر را با فرمت base64 برگردانده شود.
  - یک API با نام " authenticateCallback " که بعد از انجام عملیات احراز هویت توسط سامانه فرانشاسا به منظور ارسال نتیجه احراز هویت به پذیرنده فراخوانی می‌شود.

## کاربر

کاربر با یک توکن خود از سوی پذیرنده به سامانه فرانشاسا به منظور انجام مراحل احراز هویت هدایت می‌شود. سیستم کاربر باید مجهز به دوربین و میکروفن بوده و مراحل احراز را مطابق با راهنمای موجود در سامانه انجام دهد. اگر پذیرنده خواستار استفاده از ویژگی امضا به صورت عکس بوده، کاربر باید قبل از شروع مراحل احراز، امضای خود را بر روی برگه سفیدی در اختیار داشته باشد.

## توصیف فرایند احراز هویت

در این بخش توضیحاتی در مورد فرایند احراز هویت در فرانشاسا آورده شده است. نکته ای که در ابتدا باید به آن اشاره کرد این است که فرایند فرانشاسا براساس نیازهای پذیرنده قابل تنظیم بوده و لازم است این فرایند اختصاصی در متن قرارداد پذیرنده و شرکت پردازش اطلاعات مالی پارت مشخص گردد. به طور کلی مراحل احراز هویتی که کاربر در فرانشاسا باید آن را تکمیل کند عبارت است از:

- بارگذاری یا ترسیم امضا
- گرفتن عکس خویش انداز
- گرفتن ویدئو از خود که در آن کاربر باید یک متنی را خوانده یا حرکات اشاره ای را با دست خود اجرا کند.

ترتیب و یا تعداد مراحل احراز هویت فرانشاسا توسط پذیرنده قابل تنظیم است. پیش از توضیح فرایند، لازم است به انواع احراز هویت در فرانشاسا اشاره کرد. فرانشاسا از حیث پاسخگویی به کاربر به دو نوع آفلاین و آنلاین تقسیم می‌شود. پذیرنده می‌تواند آنلاین و آفلاین بودن سامانه را مشخص کند.

<sup>4</sup> آدرس بازگشت یا (Return URL)، آدرسی است که از سوی پذیرنده تعیین می‌شود تا کاربر پس از اتمام فرایند احراز هویت به آن آدرس هدایت شود.

<sup>5</sup> Redirect

## مدل آفلاین

نوع آفلاین، آن دسته از احراز هویت‌هایی را شامل می‌شود که کاربر تمامی مراحل احراز هویت را یکی پس از دیگری انجام می‌دهد، سپس پرونده او توسط سرویس‌های هوش پردازش شده و بعد از مدتی نتیجه‌ی احراز هویت به پذیرنده ارسال می‌شود. هر پرونده شامل اطلاعات ارسال شده کاربر به علاوه‌ی درصد پردازش‌های سرویس‌های هوش است. همچنین پذیرنده می‌تواند مشخص کند نتیجه سرویس‌های هوش را قبول کند یا درخواست بررسی پرونده‌ها از سوی عامل انسانی را هم داشته باشد. در این حالت، پرونده‌ها که شامل تمامی محتوای خواسته شده از سوی سازمان برای احراز هویت و نتیجه‌ی سرویس‌های هوش می‌باشد؛ توسط اپراتور نیز مورد بررسی قرار می‌گیرد. اگر اپراتور در تایید یا رد پرونده‌ای شک داشته باشد، پرونده توسط اپراتور ناظر مجدد مورد بررسی قرار می‌گیرد و در نهایت نتیجه نهایی به پذیرنده ارسال می‌شود.

## مدل آنلاین

در نوع آنلاین، صحت داده‌های ارسال شده توسط کاربر، در همان مرحله از مراحل احراز هویت بررسی می‌شود. در هر مرحله، در صورت تصدیق داده‌های ارسالی با داده‌های مرجع کاربر توسط سرویس‌های فراشناسا، کاربر به مرحله بعد احراز هویت خود منتقل می‌شود؛ در غیراین صورت، کاربر تا تعداد محدودی امکان تلاش مجدد برای بارگذاری داده‌های صحیح از خود را دارد. در این نوع می‌توان گفت رسیدن کاربر به مرحله‌ی آخر احراز هویت، به منزله‌ی نتیجه‌ی مثبت احراز هویت اوست. تعداد تلاش‌های کاربر برای بارگذاری داده‌های معتبر و مناسب از خود، توسط پذیرنده قابل تنظیم است.

فرآیند از پذیرنده شروع می‌شود. به این صورت که کاربر پس از تکمیل مراحل در سایت پذیرنده، به منظور احراز هویت با توکنی یکتا به سایت فراشناسا هدایت می‌شود. فراشناسا توکن را به سرویس استعلام توکن پذیرنده ارسال و صحت آن را درخواست می‌کند. پذیرنده در صورت تصدیق توکن، تصویر مرجع کاربر را به همراه سایر اطلاعات<sup>6</sup> به عنوان نتیجه برمی‌گرداند.

کاربر ابتدا امضای خود را بارگذاری و یا ترسیم می‌کند. پس از آن، عکس خویش اندازی از خود گرفته و بارگذاری می‌کند. سپس تست تصادفی‌ای که از سمت سرویس‌های هوش فراشناسا تایید شده است، ارائه می‌شود و کاربر باید از انجام تست خود ویدئو بگیرد. تست‌ها از دو نوع حرکتی و صوتی هستند. در تست صوتی، کاربر باید متنی که برای او نمایش داده شده است را به صورت رسا بخواند و در تست حرکتی، کاربر باید حرکات اشاره‌ای که در صفحه مشاهده می‌کند را با دست خود اجرا کند. کاربر می‌تواند یکی از تست‌ها را انتخاب و انجام دهد.

حال اگر نوع سرویس درخواست شده آنلاین باشد در هر مرحله از کار سرویس هوش مربوط به آن بخش صدا زده می‌شود و نتیجه بررسی و به کاربر نشان داده می‌شود. اگر نتیجه مثبت باشد کاربر به مرحله‌ی بعد می‌رود در غیر این صورت برای تعداد دفعات مشخصی می‌تواند آن مرحله را تکرار کند. اگر سرویس درخواست شده از نوع آفلاین باشد اطلاعات همه‌ی مراحل در پایگاه داده‌ای ذخیره شده و سرویس‌های هوش اطلاعات را بررسی می‌کنند و نتیجه را به پذیرنده ابلاغ می‌کند.

<sup>6</sup> در صورت نیاز پذیرنده می‌تواند علاوه بر تصویر مرجع کاربر، اطلاعات دیگری مانند کدملی، تاریخ تولد، جنسیت و ... کاربر را هم به عنوان نتیجه استعلام توکن برگرداند.

## پنل مدیریت

پنل تحت عنوان بک آفیس<sup>7</sup> طراحی شده است که نتیجه‌ی پرونده‌ها توسط پذیرنده در آن قابل بررسی می‌باشد. پذیرنده می‌تواند محتوای هر پرونده و وضعیت آن را به ازای هر کاربر مشاهده کند. اگر پرونده‌ای رد شده باشد دلیل رد شدن آن نیز در پنل قابل مشاهده است.

دیگرام کلی فرایند، در دو حالت آفلاین و آنلاین در پیوست‌های شماره ۱ و ۲ آمده است. همچنین نمایی از وبسایت فرانشاسا در پیوست شماره ۳ آمده است.

---

<sup>7</sup> Backoffice

## نحوه استفاده از سرویس

به منظور دریافت وب سرویس فراشناسا، لازم است پذیرنده، کاربر را به آدرس فراشناسایی که دریافت کرده همراه با داده‌هایی مانند توکن کاربر، آدرس بازگشت کاربر<sup>8</sup> و ... هدایت کند. در این سند این آدرس redirectURL نامیده شده است.

نمونه کامل آدرس:

```
{{farashenase_baseUrl}}/#/?token={{token}}&returnUrl={{returnURL}}
```

- farashenase\_baseUrl: آدرس فراشناسای پذیرنده
- token: توکن (شناسه یکتا) کاربر
- returnUrl: آدرس بازگشت به پذیرنده

## لیست API‌های مورد نیاز

### validateToken

#### معرفی

این API، باید توکن دریافت شده را اعتبارسنجی کند؛ در صورت معتبر بودن توکن باید تصویر مرجع کاربر با فرمت base64 و اطلاعاتی همچون جنسیت، کد ملی و شماره موبایل برگرداند. وجود فیلد تصویر الزامیست.

متد: POST

آدرس:

```
{{baseUrl}}/validateToken
```

ورودی‌ها

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	token	اجباری / رشته	توکن کاربر که رشته‌ای حداقل 3 کاراکتری و شامل کاراکترهای مجاز در URL می‌باشد.

خروجی در حالت صحیح

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	base64Image	اجباری / رشته	یک تصویر با فرمت base64
2	nationalCode	اختیاری / رشته	کد ملی کاربر به صورت رشته‌ای 10 کاراکتری.
3	gender	اختیاری / رشته	جنسیت کاربر که فقط دو رشته‌ی female و male باشد.
	phone	اختیاری / رشته	شماره موبایل کاربر به صورت رشته‌ای 11 کاراکتری

<sup>8</sup> returnUrl

```
{
  "result": {
    "base64Image": "",
    "nationalCode": "",
    "phone": "",
    "gender": ""
  }
}
```

خروجی در حالت خطا

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	errorMessage	اجباری / رشته	در صورتی که به هر دلیلی اجرای سرویس با خطا مواجه شود، متن خطا در پارامتر errorMessage مقداردهی شود.
	errorCode	اجباری / رشته	در صورتی که به هر دلیلی اجرای سرویس با خطا مواجه شود، کدخطا در پارامتر errorCode مقداردهی شود.

```
{
  "errorMessage": "",
  "errorCode": ""
}
```

توجه! اگر نیازی به استفاده از نام کاربری و گذرواژه باشد، این فیلدها در بخش "header" درخواست قرار گیرد.

## authenticateCallback

معرفی

این API نتیجهی احراز هویت را به پذیرنده اطلاع می‌دهد.

متد: POST

آدرس:

```
{{baseUrl}}/authenticateCallback
```



ورودی‌ها

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	status	اجباری / رشته	نتیجه احراز کاربر. رشته‌ای که فقط سه مقدار "reject"، "accept" و یا "timeout" را می‌پذیرد. reject: عدم تایید هویت accept: تایید هویت timeout: عدم تکمیل مراحل احراز توسط کاربر یا منقضی شدن توکن
2	token	اجباری / رشته	توکن کاربر
3	errorCodes	اجباری / رشته	رشته‌ای از اعداد که با "؛" از هم جدا شده‌اند. در صورت اینکه هویت کاربر تایید نشود، این پارامتر مقدار خواهد داشت؛ در غیر این صورت این پارامتر ارسال نخواهد شد.

ورودی در حالت تایید هویت

```
{
  "status": "accept"
  "token":""
}
```

ورودی در حالت رد هویت

```
{
  "status": reject
  "token":""
  "errorCodes": "11,12"
}
```

خروجی

خروجی در حالت صحیح

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	status	اجباری / رشته	مقدار success به عنوان تایید دریافت داده

```
{
  "result": {
```

```
"status": "success"
}
}
```

خروجی در حالت خطا

ردیف	پارامتر	نوع ورودی	شرح پارامتر
1	errorMessage	اجباری / رشته	در صورتی که به هر دلیلی اجرای سرویس با خطا مواجه شود یا نتیجه ارسال برای توکن مغایرت داشته باشد، متن خطا در پارامتر errorMessage مقداردهی شود.
	errorCode	اجباری / رشته	در صورتی که به هر دلیلی اجرای سرویس با خطا مواجه شود یا نتیجه ارسال برای توکن مغایرت داشته باشد، کدخطا در پارامتر errorCode مقداردهی شود.

```
{
"errorMessage": "",
"errorCode": ""
}
```

توجه! اگر نیازی به استفاده از نام کاربری و گذرواژه باشد، این فیلدها در بخش "header" درخواست قرار گیرد.

کدهای خطا، قراردادی بین پارت و پذیرنده است. این قرارداد به صورت زیر است.

کدخطا	شرح
11	عدم تطابق عکس خویش انداز با عکس مرجع
12	عدم تطابق خویش انداز با ویدئو
13	مشکل داشتن ویدئوی ضبط شده
14	نخواندن توضیحات ویدئو
15	رعایت نشدن شرایط عکس خویش انداز
16	عدم احراز هویت در خویش انداز
17	عدم دریافت ویدئو
18	عدم احراز هویت در ویدئو
19	اجرای نادرست ژست های حرکتی

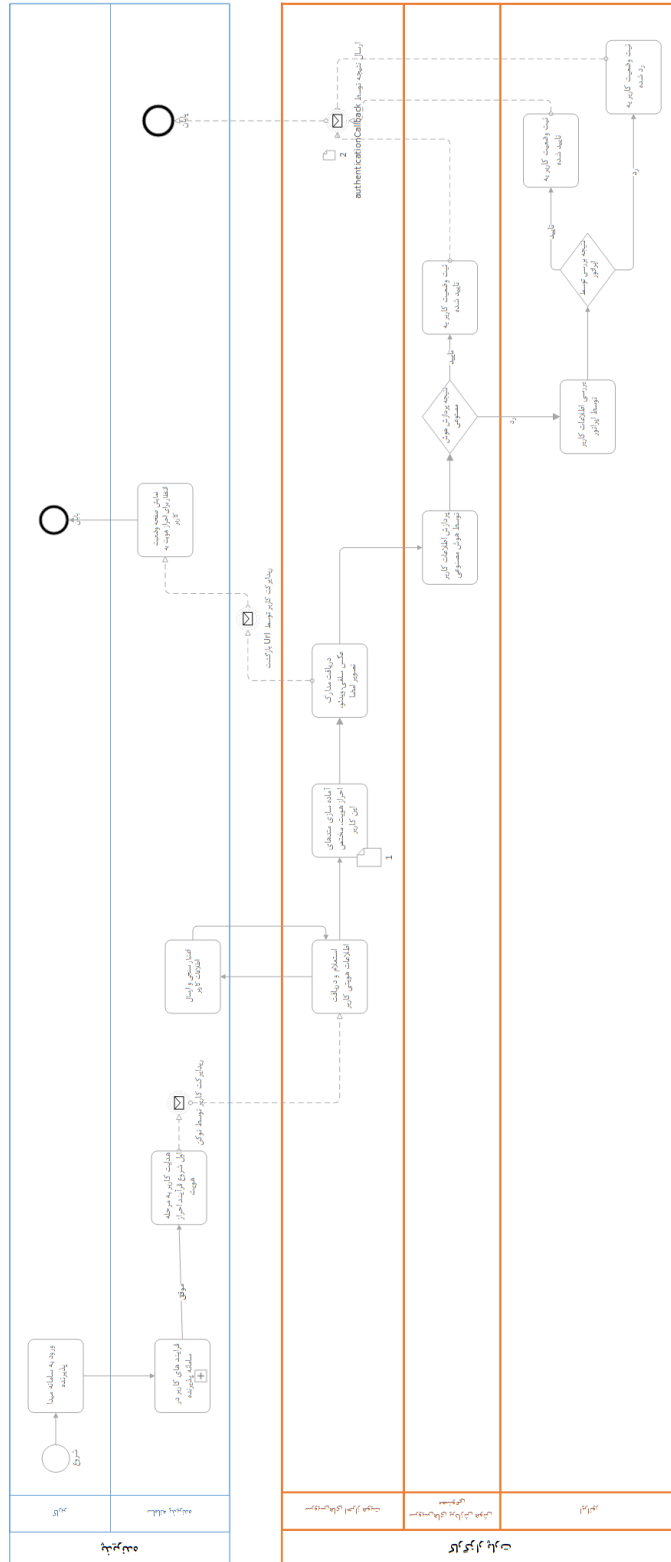
## نکات

حداکثر زمان فرایند طی توافق با پذیرنده مشخص می شود. توکنی که کاربر با آن به سامانه فراشناسا منتقل می شود به همان اندازه معتبر بوده و پس از انقضا، کاربر (در صورت فعال بودن در فراشناسا) به آدرس بازگشت پذیرنده هدایت می شود و وضعیت آن توکن به مقدار "timeout" به پذیرنده اعلام می شود.

در صورت هدایت مجدد کاربر به فراشناسا به دلایلی مانند (احراز نشدن هویت یا منقضی شدن توکن کاربر)، توکن جدیدی برای کاربر تولید شود. در غیر این صورت این مورد حتما باید در قرارداد ذکر شود.

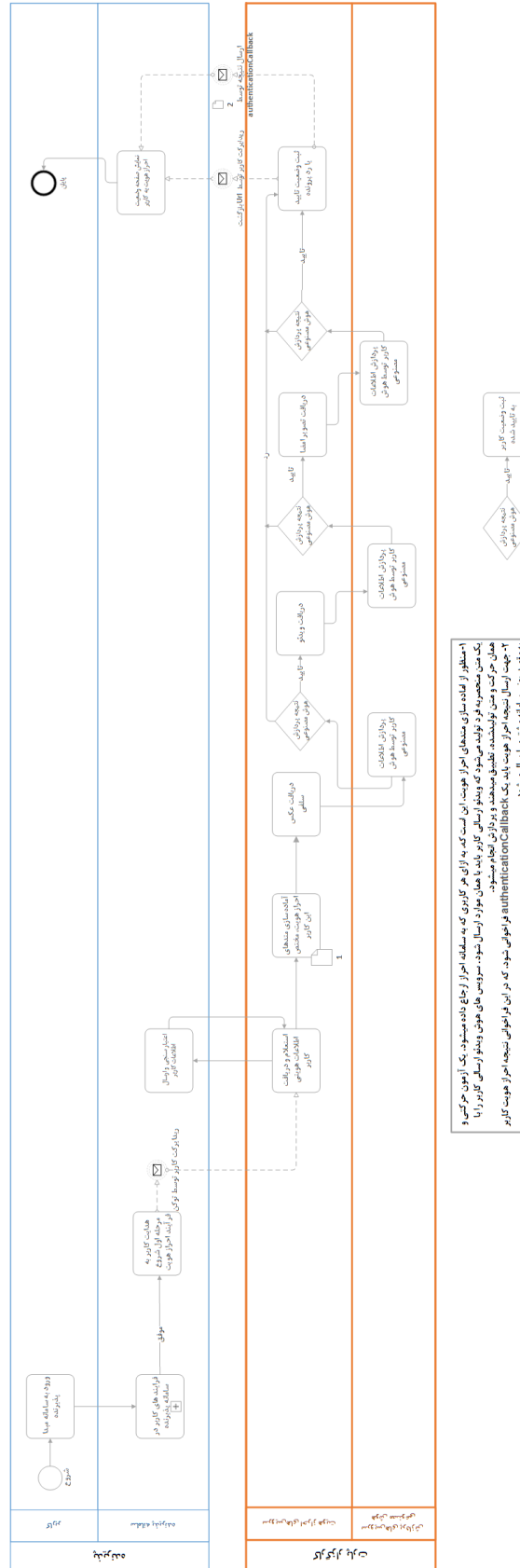
## پیوست‌ها

### پیوست 1: دیاگرام فرآیند در مدل آفلاین



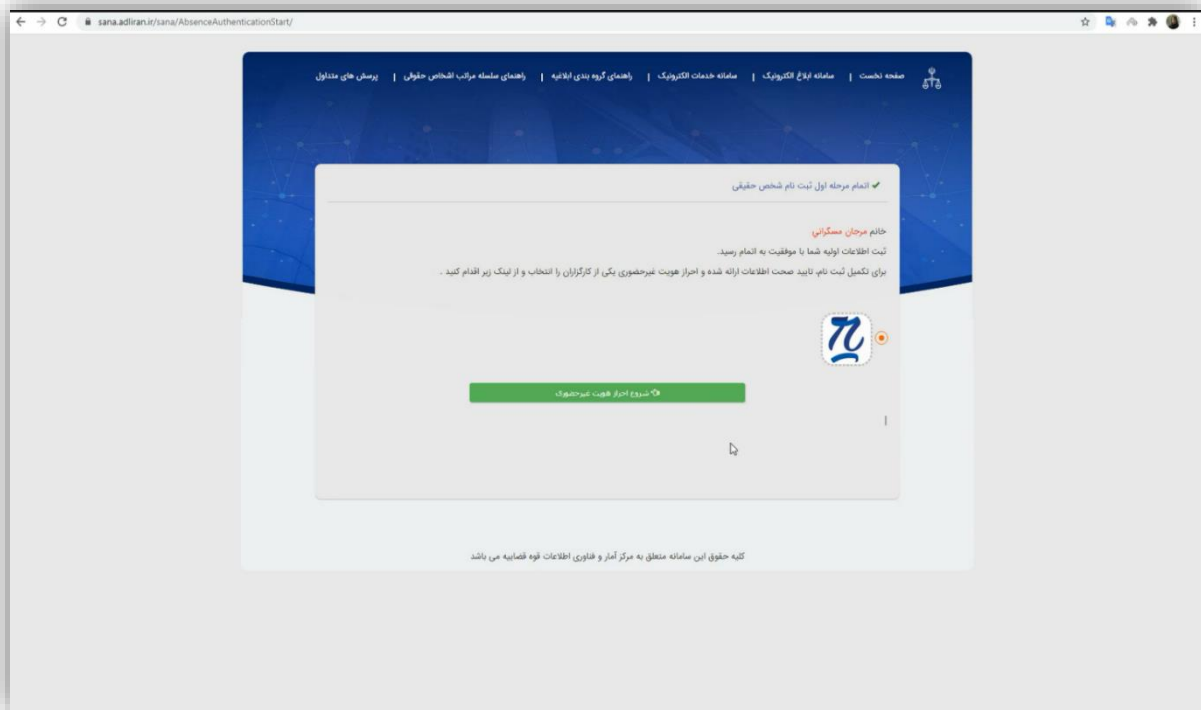
۱- منظور از داده سازی متدهای احراز هویت این است که به ازای هر کاربری که به سامانه احراز هویت داده میشود یک آزمون حرکتی و یک متن مشخصه تولید می‌شود که به عنوان کارایی کاربر به حساب می‌آید. هر کاربری که به سامانه احراز هویت داده میشود یک آزمون حرکتی و یک متن تولید شده. عملی می‌شود و پردازش انجام میشود.  
۲- جهت ارسال نتیجه احراز هویت باید یک authenticationCallback فراخوانی شود که در این فراخوانی نتیجه احراز هویت کاربر به مقصد می‌رسد.

## پیوست 2: دیاگرام فرآیند در مدل آنلاین

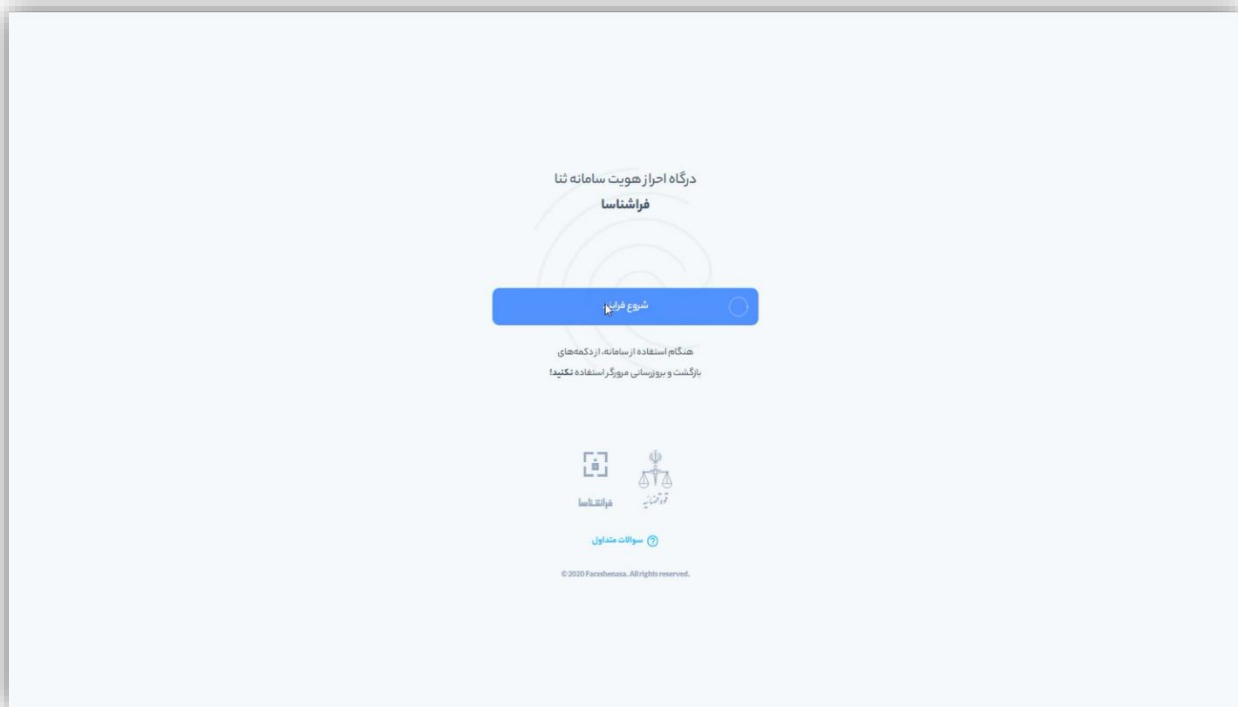


دستورالعمل فرآیند احراز هویت: در صورتی که کاربر در حال احراز هویت است، سیستم به بررسی وضعیت کاربر می‌پردازد. اگر کاربر در حال احراز هویت است، سیستم به ارسال پیامک تایید می‌پردازد. اگر کاربر در حال احراز هویت نیست، سیستم به نمایش پیام خطا می‌پردازد. اگر کاربر در حال احراز هویت است و پیامک تایید را دریافت کرده است، سیستم به بررسی کد تایید می‌پردازد. اگر کد تایید صحیح است، سیستم به احراز هویت کاربر می‌پردازد. اگر کد تایید نادرست است، سیستم به نمایش پیام خطا می‌پردازد. اگر کاربر در حال احراز هویت است و پیامک تایید را دریافت کرده است و کد تایید صحیح است، سیستم به احراز هویت کاربر می‌پردازد. اگر کاربر در حال احراز هویت است و پیامک تایید را دریافت کرده است و کد تایید نادرست است، سیستم به نمایش پیام خطا می‌پردازد.

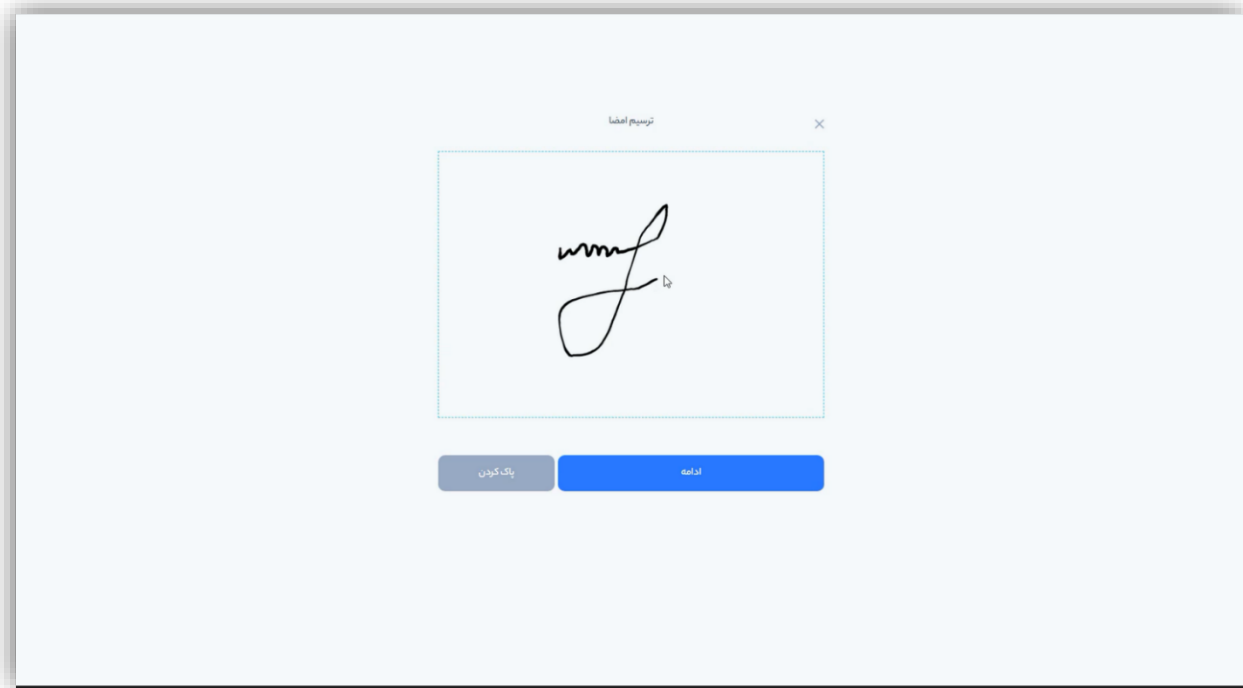
### پیوست 3: نمونه تصاویر اجرای سامانه



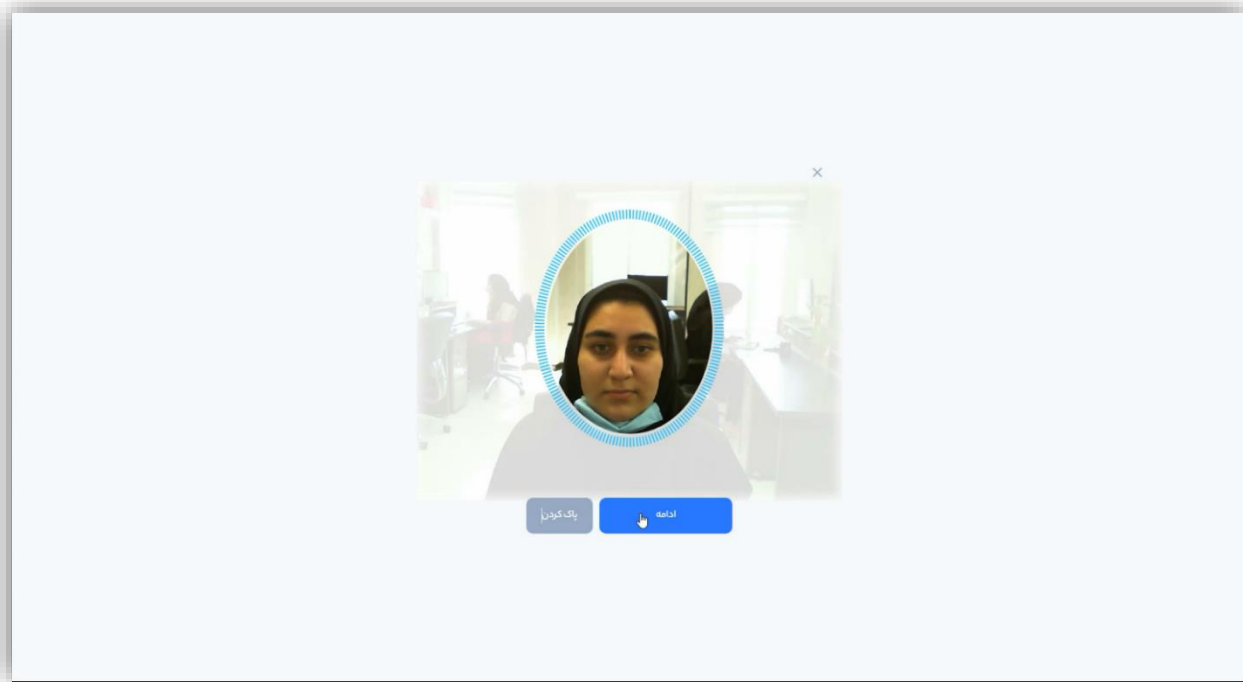
تصویر شماره 1: صفحه احراز هویت پذیرنده



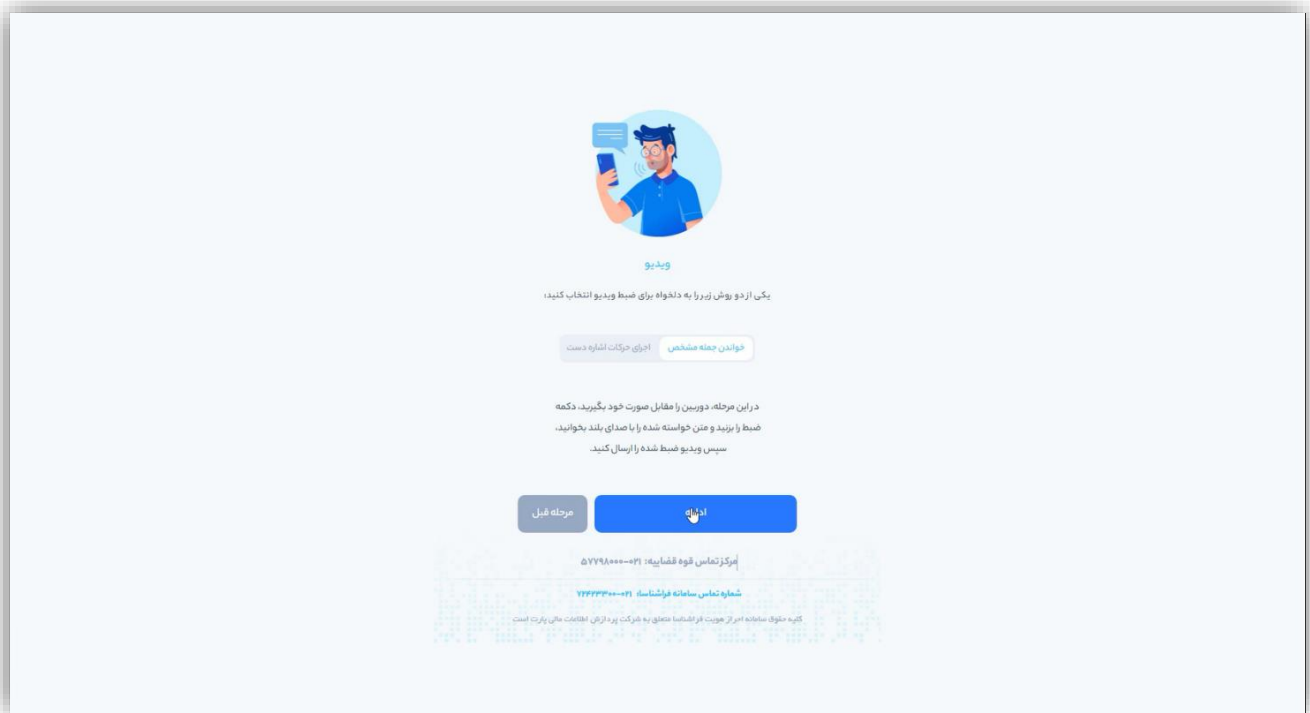
تصویر شماره 2: صفحه آغاز احراز هویت در فرانشاسا



تصویر شماره 3: ترسیم امضا توسط کاربر



تصویر شماره 4: ارسال عکس سلفی توسط کاربر

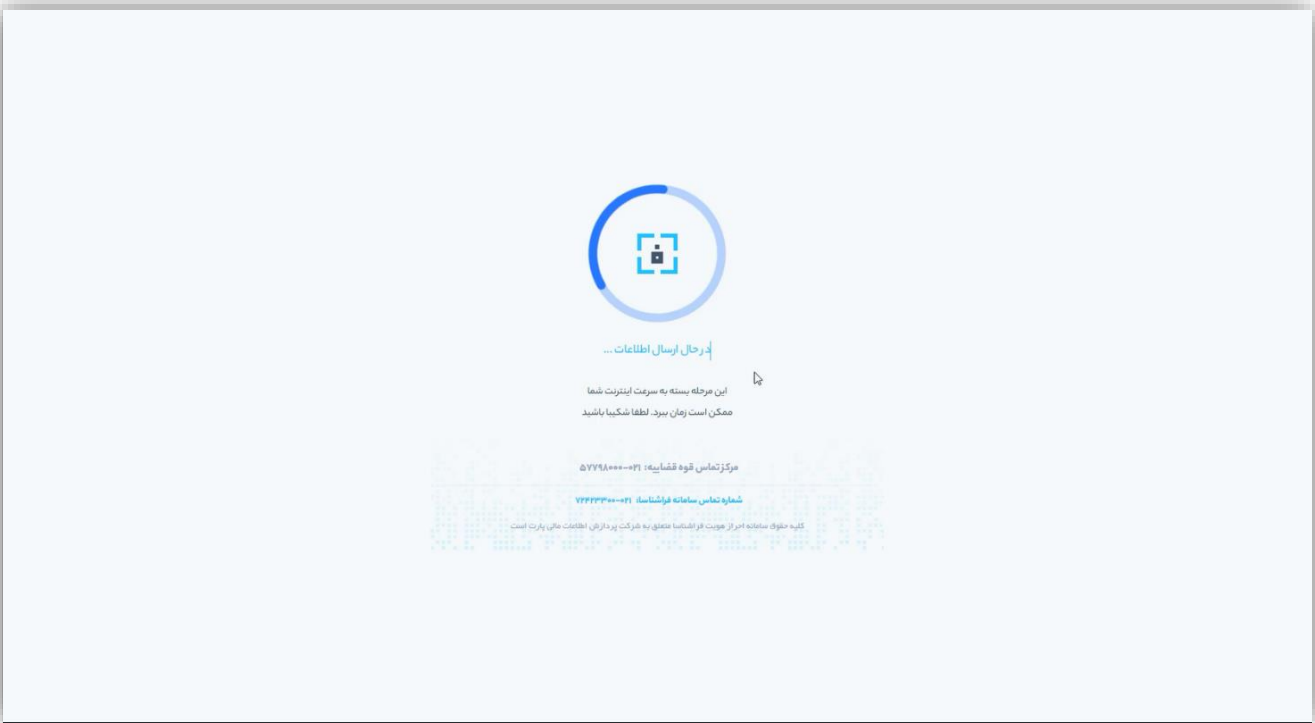


تصویر شماره 5: انتخاب نحوه انجام فرمان صوتی/حرکتی توسط کاربر

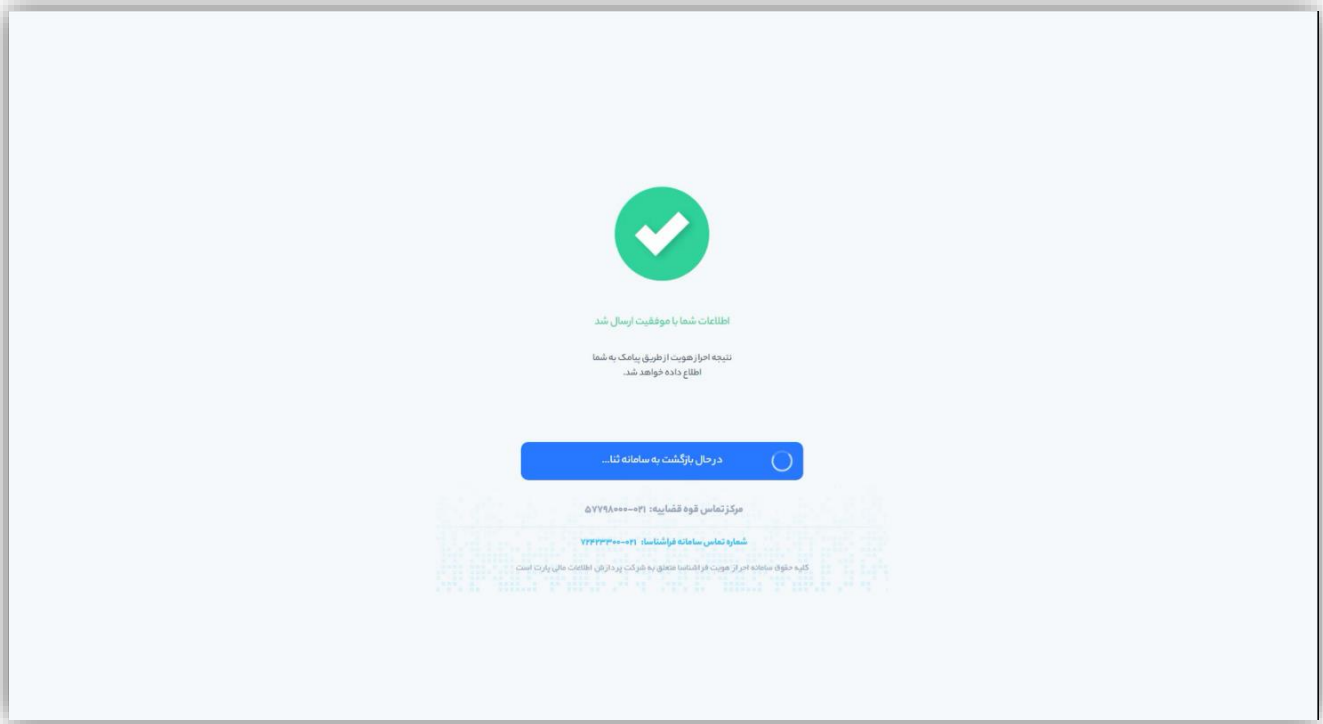


تصویر شماره 6: ضبط فیلم حاوی فرمان

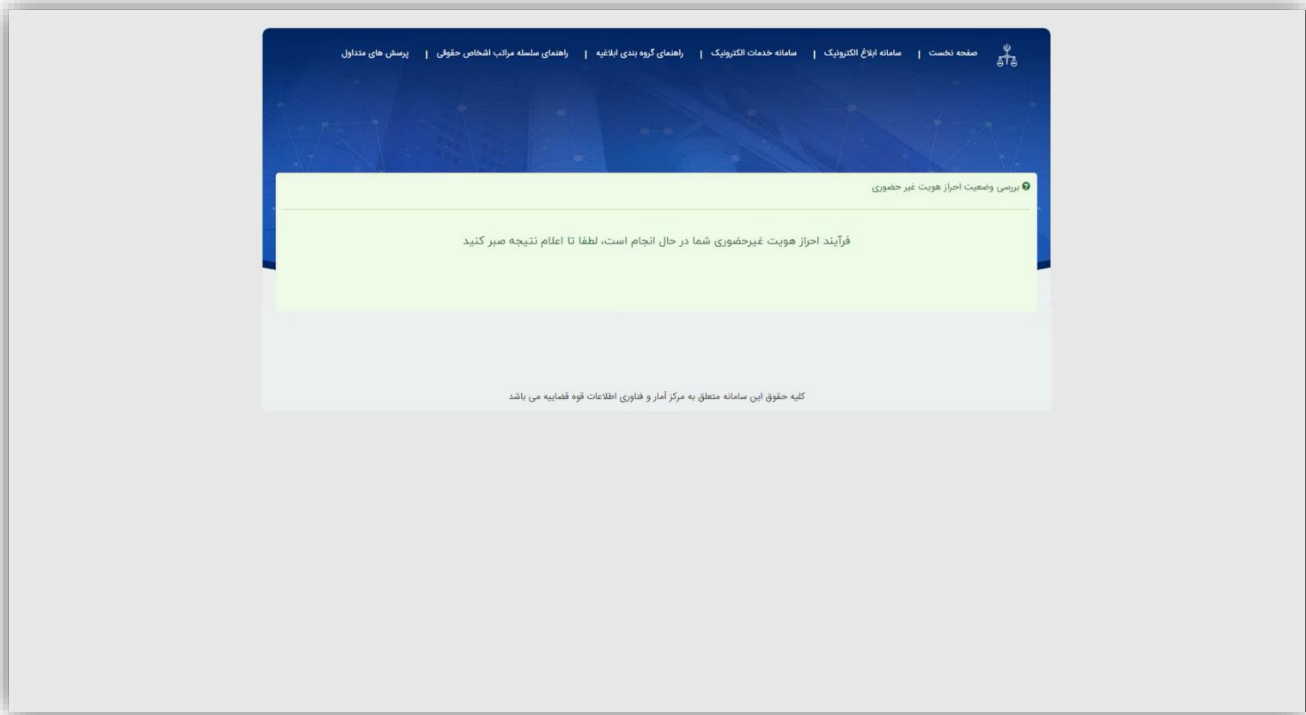




تصویر شماره 7: ارسال اطلاعات کاربر به فرانشاسا



تصویر شماره 8: پایان موفقیت آمیز ارسال اطلاعات در فرانشاسا



تصویر شماره 9: هدایت کاربر به سایت پذیرنده