

پروپوزال ارائه خدمت

امضای دیجیتال فراشناسا



گروه نرم افزاری پارت
Part Software Group



شرکت پردازش اطلاعات مالی
دستیار هوشمند اقتصادی شما



مرکز تحقیقات
هوش مصنوعی پارت

پاییز ۱۴۰۴

فهرست

معرفی پارت.....	۲
مقدمه.....	۳
امضای دیجیتال فراشناسا.....	۴
۱- پشتوانه قانونی امضا.....	۴
۲- انواع سطوح گواهی.....	۵
۳- مدل های ارائه سرویس:.....	۶
۱-۳ نسخه (SDK (Software Development Kit.....	۶
۲-۳ اپلیکیشن (اپلیکیشن صدور گواهی و امضای دیجیتال).....	۷
۴- معرفی محصول.....	۷
۱-۴ فرآیند بارگزاری اسناد توسط سازمان.....	۸
۲-۴ فرآیند صدور گواهی توسط کاربر.....	۱۱
۳-۴ گواهی های من.....	۲۱
۴-۴ جزئیات گواهی.....	۲۲
۵-۴ اطلاعات من.....	۲۲
۵- قابلیت ها و مزیت رقابتی محصول امضا دیجیتال پارت.....	۲۳
۶- اجزای زیرساخت محصول.....	۲۵
۱-۶ مرکز ثبت گواهی (RA).....	۲۵
۲-۶ کیت توسعه نرم افزار مدیریت گواهی (SDK).....	۲۷
۳-۶ اعتبارسنجی امضای اسناد دیجیتال.....	۲۸
۴-۶ مدیریت گواهی های قابل اعتماد.....	۲۹
۵-۶ مرکز صدور مهر زمانی (TSA).....	۳۰
۶-۶ مانیتورینگ و قابلیت اتکا سامانه.....	۳۰

معرفی پارت

مجموعه دانش بنیان پردازش اطلاعات مالی پارت با همراهی جمعی از بهترین متخصصان حوزه مالی، فناوری اطلاعات و هوش مصنوعی کشور و با شعار هوشمندسازی فرآیندهای زندگی در سال ۱۳۹۲ تاسیس شد.

هدف پارت از ارائه خدمت، به کارگیری تکنولوژی‌های روز برای هوشمندسازی زندگی، کسب و کارها و دسترسی هر چه بیشتر افراد جامعه به خدمات الکترونیک است. مجموعه دانش بنیان پارت با بیش از هزار و دویست نفر منابع انسانی در حال حاضر در شهرهای تهران، مشهد و کرمان مشغول به فعالیت است.

مرکز تحقیقات هوش مصنوعی پارت، به عنوان یکی از اصلی‌ترین واحدهای شرکت دانش بنیان پارت، فعالیت خود را از سال ۱۳۹۶ با هدف تبدیل شدن به بزرگ‌ترین و پیشروترین بازیگر هوش مصنوعی در خاورمیانه آغاز کرده است. مشتریان خدمات هوش مصنوعی پارت را طیف وسیع و متنوعی از سازمان‌ها، استارت‌آپ‌ها، برنامه‌نویسان و مراکز تحقیقاتی و دانشگاهی تشکیل می‌دهند.

مقدمه

امروزه با پیشرفت تکنولوژی و امکان دیجیتالی شدن بیش‌تر فرآیندها، نیاز به حضور فیزیکی افراد برای انجام امور مختلف به حداقل رسیده است و چنانچه کسب‌وکاری از این موهبت بهره لازم را ببرد، می‌تواند با کاهش هزینه‌ها گامی بزرگ در راستای افزایش سود و پیشی‌گرفتن آن در عرصه رقابت بردارد. اما با توجه به حساسیت این موضوع، می‌بایست اطمینان لازم از انجام امور توسط خود فرد و مجموعه کسب شود. این مهم در مراجعات حضوری به راحتی قابل تشخیص و شناسایی است، اما چنانچه سازمانی قصد همگام شدن با تکنولوژی و ارائه خدمات به صورت غیرحضوری را داشته باشد، با چالش‌هایی مواجه می‌شود که می‌تواند به طور مستقیم ریسک فرآیندها را افزایش دهد.

علاوه بر این، ظهور فناوری‌های نو و استفاده روزافزون از آن در سازمان‌ها نیز نیاز به دیجیتالی شدن اسناد را امری ناگزیر نموده است. برای دیجیتالی نمودن اسناد سازمانی، نیاز است مهرهای سنتی سازمان‌ها را به صورت یک عنصر دیجیتال درآورده و حضور شخص را نیز حذف کرد که بتوان فرآیندهای مکانیزه را خلق نمود.

امضای دیجیتال فراشناسا

سال‌های زیادی است که امضای دیجیتال به عنوان یک راهکار شناخته شده برای حل چالش انکارناپذیری و تضمین صحت پیام‌ها استفاده می‌شود. در حال حاضر راهکار رایج امضای دیجیتال که در کشور مورد استفاده قرار می‌گیرد، نیازمند خرید یک توکن سخت‌افزاری و مراجعه حضوری به دفاتر اسناد رسمی است. فراشناسا با ارائه این خدمت بر بستر وب و موبایل سادگی و دسترس‌پذیری بیشتری را برای کاربران فراهم کرده است که به موجب آن موفق به صدور حدود ۷,۸۵۰,۰۰۰ گواهی امضای دیجیتال تاکنون شده است.

امضای دیجیتال یک مکانیزم رمزنگاری برای تایید اعتبار و انسجام داده‌های دیجیتال است. رمزنگاری کلید عمومی یا PKC (public-key cryptography) به سیستمی اشاره دارد که از دو جفت کلید استفاده می‌کند: یک کلید عمومی و یک کلید خصوصی. این دو کلید با هم نسبت ریاضی دارند که علاوه بر رمزنگاری داده، در امضاهای دیجیتال نیز کاربرد دارند.

سرویس امضای دیجیتال فراشناسا دارای یک سرویس مرکزی با قابلیت اتکای بالا و توانایی ارائه خدمت امضا برای انواع داده‌های PDF، JSON، XML و باینری می‌باشد. در این نوع امضای دیجیتال اطلاعات کامل و دقیقی برای بررسی دعاوی حقوقی آینده وجود دارد که نیاز داده‌های باینری، ویدئو، تراکنش را نیز با کارایی بالا مرتفع می‌نماید.

۱- پشتوانه قانونی امضا

مزیت برجسته امضای دیجیتال پشتوانه حقوقی آن در کشور است. در ماده ۷ قانون تجارت الکترونیک به این موضوع اشاره شده است:

«هرگاه قانون وجود امضا را لازم بداند، امضای الکترونیکی مکفی است.»

بر این اساس، امضای دیجیتال به تنهایی و بدون نیاز به امضای دستی برای قانون کفایت می‌کند.

کسی که از امضای دیجیتال استفاده می‌کند هویتش احراز شده است، بنابراین پیامی که با امضای دیجیتال امضا شده، به هیچ عنوان قابل انکار نیست و همچنین پیامی که به صورت امضا شده دریافت می‌شود، قطعاً دست نخورده است و از طرف ارسال کننده اصلی می‌باشد.

۲- انواع سطوح گواهی

با استفاده از معیاری به نام سطح اطمینان گواهی الکترونیکی، می‌توان به میزان اطمینانی که میان پیوند اطلاعات مالک گواهی الکترونیکی و کلید عمومی آن وجود دارد، دست یافت. این معیار، نشان‌دهنده میزان امنیت لحاظ شده در فرآیند تولید گواهی و زوج کلید مرتبط با آن و همچنین استفاد از کلید خصوصی متناظر با کلید عمومی مالک گواهی الکترونیکی می‌باشد.

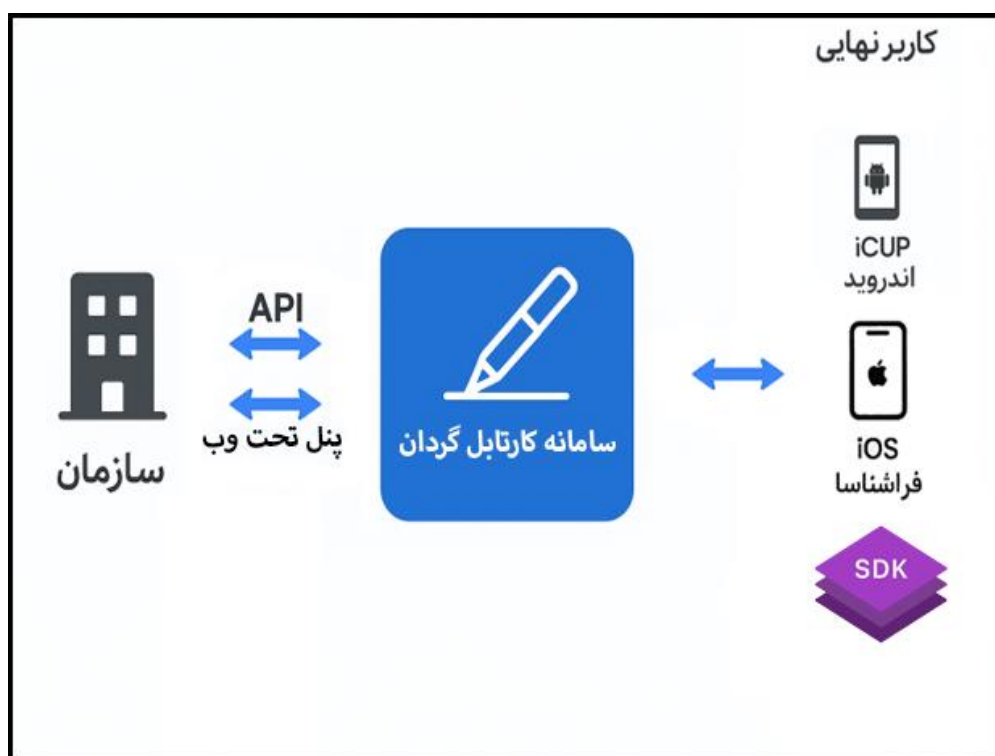
راهکار امضای دیجیتال فراشناسا، به لحاظ فنی، سطح ۱ و ۲ گواهی امضای دیجیتال را

پشتیبانی می‌کند.

شایان ذکر است که اتصال و انجام عملیات مرتبط با صدور گواهی الکترونیکی و امضا دیجیتال فراشناسا، از مراکز صدور گواهی مورد تأیید مرکز ریشه وزارت صمت انجام شده و در حال حاضر مراکز میانی مختلفی با شرکت پارت همکاری می‌کنند.

۳- مدل های ارائه سرویس:

به منظور پاسخ گویی به نیازهای متنوع سازمان ها، توسعه دهندگان و کاربران نهایی، سرویس امضای دیجیتال شرکت پارت در چند مدل مختلف ارائه می شود تا بالاترین سطح انعطاف پذیری، دسترسی و سهولت استفاده را فراهم آورد. این مدل ها شامل نسخه توسعه دهندگان (SDK) و اپلیکیشن موبایل هستند که در ادامه، هر یک از این مدل ها به تفکیک معرفی شده اند.



۱-۳ نسخه (SDK (Software Development Kit

کاربرد: برای شرکت ها یا سامانه هایی که قصد دارند امضا دیجیتال را در محصول خود یکپارچه سازی کنند. لازم به ذکر است که محصول امضا شرکت پارت دارای SDK هر دو پلتفرم اندروید و IOS می باشد.

ویژگی‌ها:

- قابلیت اتصال به سامانه‌های داخلی مشتری (API / SDK)
- انعطاف‌پذیر برای توسعه‌دهندگان
- مناسب برای سامانه‌های بزرگ

۲-۳. اپلیکیشن (اپلیکیشن صدور گواهی و امضای دیجیتال)

اپلیکیشن اندروید (آیکاپ) و IOS فراشناسا توسط شرکت پارت توسعه داده شده‌اند و سرویس امضای دیجیتال روی آن‌ها فعال است.

کاربرد:

- سازمان‌ها از طریق سامانه کارتابل گردان قراردادها را برای کاربران ارسال می‌کنند تا در ICUP امضا شوند.
- کاربر نهایی می‌تواند از طریق اپلیکیشن ICUP گواهی امضا صادر کند.

۴- معرفی محصول

کاربر می‌تواند با ورود به اپلیکیشن‌های توسعه داده شده توسط پارت یا اپلیکیشن توسعه داده شده توسط خود سازمان که راهکار امضای دیجیتال در آن به کار رفته، درخواست صدور گواهی امضای دیجیتال را ثبت نماید. پس از ثبت این درخواست و طی نمودن گام‌های مربوطه (شامل پذیرفتن قوانین و مقررات، وارد کردن اطلاعات هویتی و احراز هویت کاربر با استفاده

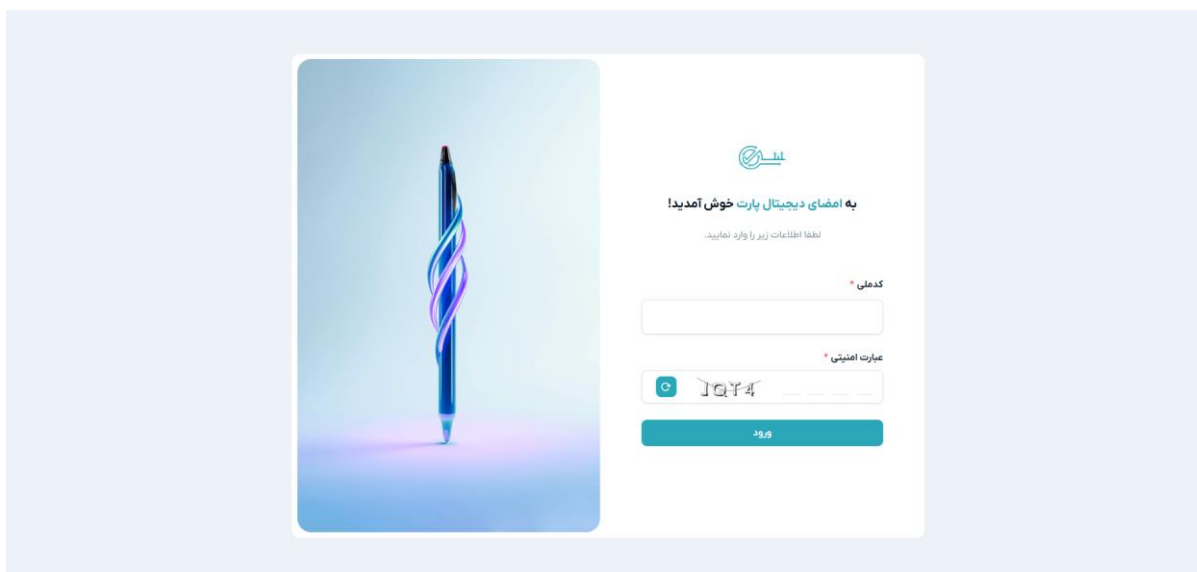
از سامانه احراز هویت تصویری فراشناسا) زوج کلید برای کاربر صادر می‌گردد. این کلید خصوصی، به صورت امن بر روی دستگاه تلفن همراه کاربر ذخیره می‌شود.

در گام بعدی، پس از اخذ گواهی امضای دیجیتال و ثبت این گواهی در مراکز میانی معتبر، کاربر می‌تواند با استفاده از تلفن همراه خود امضای دیجیتالی اسناد را انجام دهد. اسناد به صورت PDF در اختیار کاربر قرار می‌گیرد و کاربر پس از مطالعه سند می‌تواند آن را به صورت دیجیتالی امضا نماید.

در ادامه بخش‌های مختلف مربوط به امضای دیجیتال شامل «فرآیند صدور گواهی»، «گواهی‌های من»، «جزئیات گواهی» و «اطلاعات من» به تفصیل توضیح داده شده است.

۱-۴- فرآیند بارگزاری اسناد توسط سازمان

چنانچه سازمان بخواهد قراردادهای کاربران را بارگزاری نماید می‌تواند یا به صورت خودکار و از طریق API یا با استفاده از پنل تحت وب این عمل را انجام دهد که در ادامه تصاویر مربوط به پنل تحت وب را مشاهده خواهید کرد:



در این مرحله اپراتور سازمان با استفاده از کد ملی و توسط کد OTP وارد پنل مدیریتی خود می‌شود.

لیست درخواست های امضا							
لیست درخواست های امضا							
افزودن سند جهت امضا							
عنوان	درخواست دهنده	آپ	امضا کننده	تاریخ ارسال	مهلت امضا	زمان امضا	وضعیت
تست گزارش	دوم امضا دیجیتال پارت	ایپیکشن آی کاب	[Redacted]	1404/7/22 - 14:29	6 روز 22 ساعت 11 دقیقه	-	در انتظار امضا
توسعه OCSIP امضا	دوم امضا دیجیتال پارت	ایپیکشن آی کاب	[Redacted]	1404/7/22 - 10:09	-	-	منتظمی شده
تست نسخه جدید	دوم امضا دیجیتال پارت	ایپیکشن آی کاب	[Redacted]	1404/7/22 - 09:59	6 روز 17 ساعت 41 دقیقه	1404/7/22 - 10:06	امضا شده
قرارداد	دوم امضا دیجیتال پارت	ایپیکشن آی کاب	[Redacted]	1404/7/16 - 11:31	19 ساعت 12 دقیقه	1404/7/16 - 11:32	امضا شده
قرارداد تست و تحویل سیستم	دوم امضا دیجیتال پارت	ایپیکشن فرانشاساین	[Redacted]	1404/7/16 - 11:14	18 ساعت 56 دقیقه	1404/7/16 - 11:16	امضا شده
قرارداد همکاری در فروش	دوم امضا دیجیتال پارت	ایپیکشن فرانشاساین	[Redacted]	1404/7/16 - 11:13	18 ساعت 55 دقیقه	1404/7/16 - 11:16	امضا شده
قرارداد انجام کار به صورت پیمانکاری	دوم امضا دیجیتال پارت	ایپیکشن فرانشاساین	[Redacted]	1404/7/16 - 11:12	18 ساعت 54 دقیقه	1404/7/16 - 15:49	امضا شده
قرارداد عدم افشای اطلاعات	دوم امضا دیجیتال پارت	ایپیکشن فرانشاساین	[Redacted]	1404/7/16 - 11:07	18 ساعت 49 دقیقه	1404/7/16 - 15:52	امضا شده
قرارداد همکاری در فروش	دوم امضا دیجیتال پارت	ایپیکشن فرانشاساین	[Redacted]	1404/7/16 - 10:30	19 ساعت 19 دقیقه	1404/7/16 - 10:31	امضا شده

سازمان می‌تواند اطلاعات اسناد مختلف اعم از تاریخ ارسال، شخص امضا کننده، مهلت انقضا، زمان امضا و وضعیت سند را مشاهده نموده و همچنین فایل امضا را دانلود نماید.

✕
افزودن امضاکننده

کد ملی *

افزودن طرح تصویر امضا با اختیاری:

ⓘ لطفا اندازه پاکس محل امضا را مشخص نموده و سپس مکان آن را با جابه‌جایی روی تصویر مشخص نمایید.



آپلود عکس امضا با اختیاری: ☐

بستن
افزودن

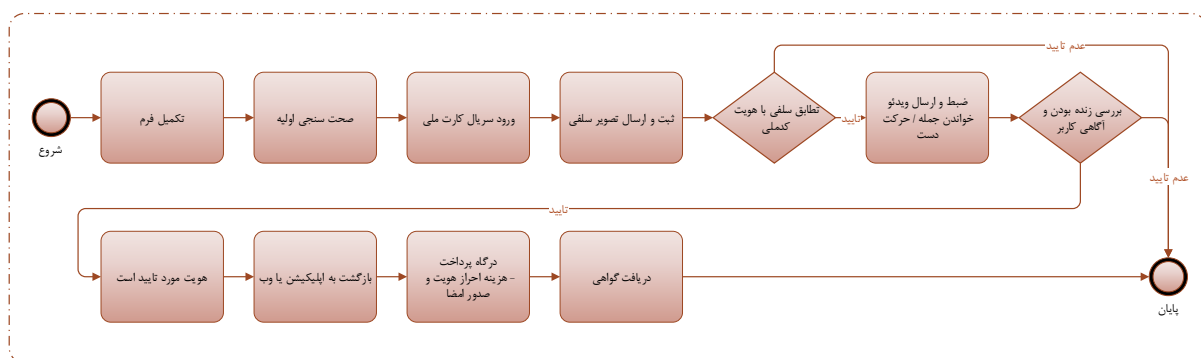
پس از فشردن گزینه افزودن امضا کننده صفحه‌ای باز خواهد شد که در آن می‌توانید محل امضا را مشخص کنید و کد ملی امضا کننده را وارد کنید. تصویر امضا در PDF صرفاً نمایشی است؛ اعتبار واقعی امضا مربوط به داده‌های رمزنگاری‌شده‌ی درج‌شده در ساختار دیجیتال فایل است.

۲-۴- فرآیند صدور گواهی توسط کاربر

حال چنانچه کاربر بخواهد برای خود گواهی صادر نماید و از آن جهت امضا زدن فایل‌های PDF استفاده کند نیاز دارد گام‌های زیر را سپری کند.

در ادامه فرآیند سفر مشتری صدور گواهی، بصورت شماتیک آمده است که گام‌های آن به تفصیل توضیح داده شده است.

شکل ۱. فرآیند سفر مشتری صدور گواهی



۱- اولین مرحله مطالعه قوانین و مقررات مربوط به صدور گواهی و پذیرفتن شرایط آن است. پس از آن، کاربر می‌بایست فرم مربوطه را از طریق وارد کردن اطلاعات کاربر (شماره همراه، کد ملی، تاریخ تولد و کد پستی) به طور دقیق کامل نماید.

→ صدور گواهی امضا

۴

۳

۲

۱

دریافت گواهی
پرداخت وجه
احراز هویت
تکمیل فرم

فرم زیر را جهت صدور گواهی امضا تکمیل کنید.

شماره موبایل
کد ملی
تاریخ تولد
کد پستی

تایید اطلاعات

→ صدور گواهی امضا

هشدار های صدور گواهی امضا

توجه داشته باشید که با حذف اپلیکیشن از روی گوشی همراه شما، گواهی امضای دیجیتال شما پاک خواهد شد.

تلفن همراه شما باید حداقل از یک روش اعتبار سنجی بر خوردار باشد. (اثر انگشت، الگو، رمز عبور و ..)

کاربر گرامی در صورت حذف یا تعویض رمز یا الگو امنیتی گوشی خود، امضای دیجیتال شما غیرقابل استفاده می گردد.

هزینه احراز هویت غیر حضوری و صدور گواهی امضای دیجیتال ۲۰۰ تومان می باشد.

شما می توانید در طول مدت اعتبار گواهی امضای دیجیتال، بدون نیاز به پرداخت وجه، از امضای صادر شده استفاده کنید.

☐ شرایط فوق را با دقت مطالعه و تایید میکنم .

شروع فرآیند

پس از وارد کردن اطلاعات، کاربر وارد صفحه کد تایید می شود.

۲- در گام بعدی نیاز به احراز هویت الکترونیکی می باشد که ابتدا باید سریال پشت کارت ملی وارد شود.

→ صدور گواهی امضا

۴
۳
۲
۱

دریافت گواهی پرداخت وجه احراز هویت تکمیل فرم

سریال پشت کارت ملی خود را وارد کنید.

سریال کارت ملی

در صورت عدم دریافت کارت ملی جدید، لطفاً کد رهگیری رسید را وارد کنید.

برای انجام مراحل احراز هویت دکمه "شروع احراز هویت" را بفشارید.

هشدارهای احراز هویت:

- رعایت شئونات اسلامی
- ضبط ویدئو / عکس از شخص متقاضی
- پرداخت وجه بابت کارمزد احراز هویت

انصراف

شروع احراز هویت

کد تایید

کد پیامک شده به را وارد کنید.

۰۱:۴۸

تایید

→ ویرایش اطلاعات

۱-۲- جهت احراز هویت ابتدا کاربر باید نمونه امضا خود را با یکی از روش‌های زیر (گرفتن تصویر یا ترسیم امضا) ثبت و تأیید کند.

نمونه امضا

گرفتن تصویر امضا

ترسیم امضا

در این مرحله شما باید امضای خود را در کادر سفید بکشید. در تلفن همراه، با لمس صفحه گوشی هوشمند و در رایانه بوسیله ماوس امضا خود را بکشید.

ادامه

شماره تماس سامانه فرانشاسا: ۰۲۱۷۲۴۴۳۳۰۰

کلیه حقوق سامانه احراز هویت فرانشاسا متعلق به شرکت پردازش اطلاعات مالی پارت است

ترسیم امضا

پاک کردن

تایید و ارسال

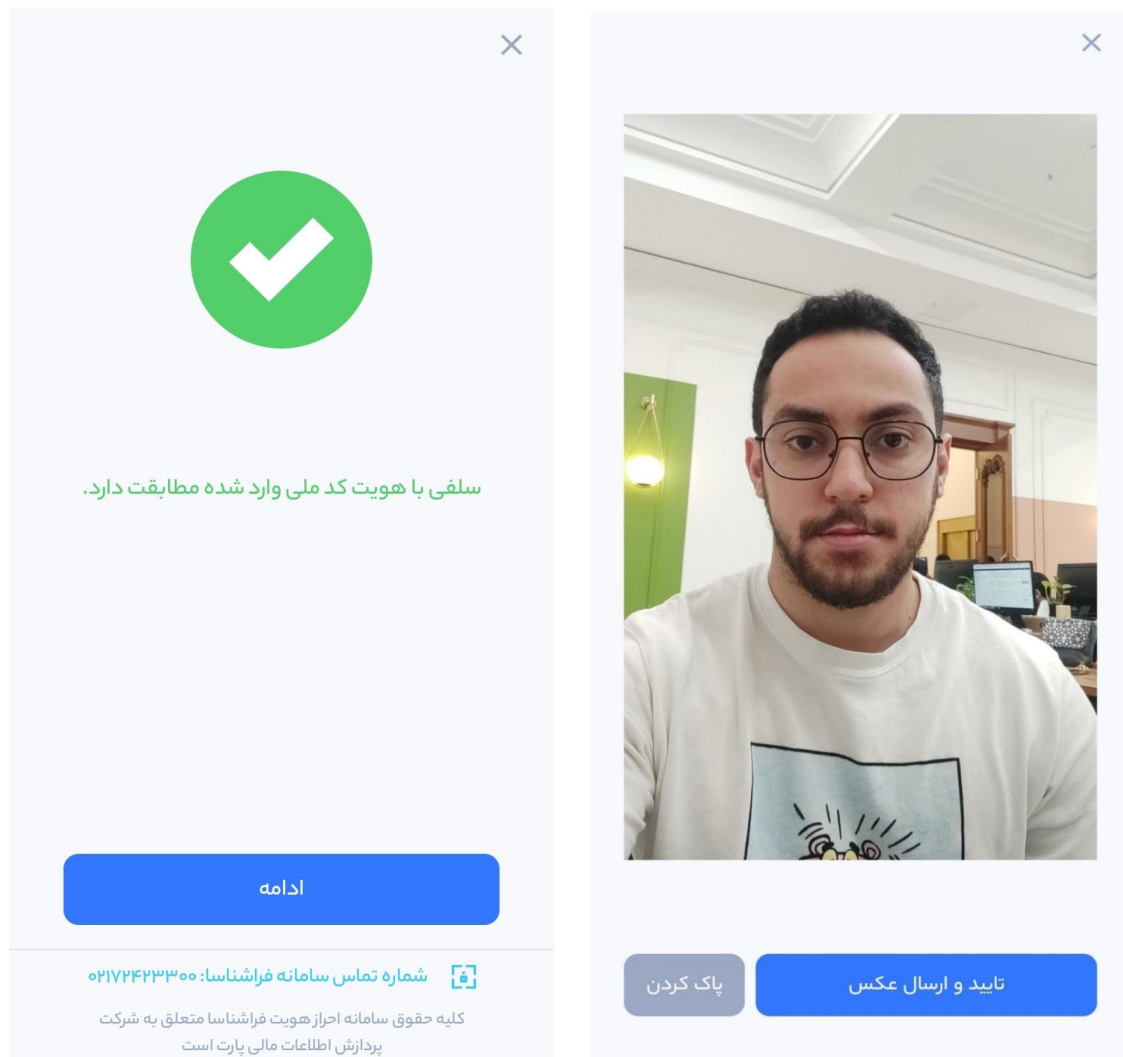
شماره تماس سامانه فرانشاسا: ۰۲۱۷۲۴۴۳۳۰۰

کلیه حقوق سامانه احراز هویت فرانشاسا متعلق به شرکت پردازش اطلاعات مالی پارت است

۲-۲- در گام بعدی، پس از اینکه نمونه امضا تایید شد کاربر باید مطابق تصاویر زیر پیش برود.



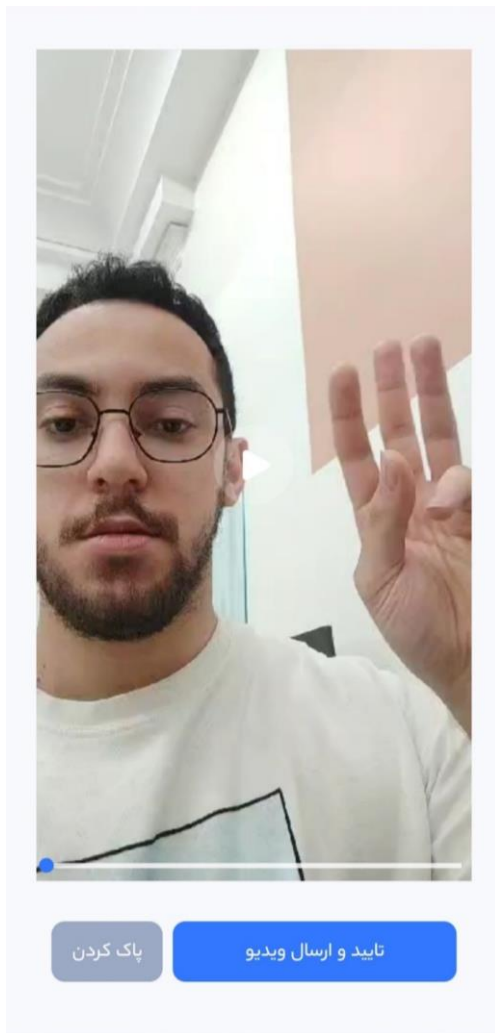
پس از تنظیمات لازم برای گرفتن تصویر سلفی، کاربر می‌بایست عکس سلفی مورد نظر را تایید و ارسال نماید.



۳-۲- در این مرحله، جهت بررسی زنده بودن تصویر و اطمینان از آگاهی کاربر از اقدام در حال انجام، کاربر می‌بایست مطابق تصاویر زیر، ویدئویی از خود ضبط و ارسال نماید.

پس از تنظیمات لازم برای گرفتن ویدئو، کاربر می‌بایست ویدئوی مورد نظر را تایید و ارسال نماید.





۳- پس از این که احراز هویت با موفقیت به پایان رسید، کاربر وارد مرحله پرداخت می‌شود.
در این مرحله کاربر با زدن دکمه پرداخت وارد صفحه پرداخت در مرورگر شده و می‌تواند پرداخت را انجام دهد.

صادر امضا

۴

۳

۲

۱

نمایش گواهی

پرداخت وجه

احراز هویت

تکمیل فرم

احراز هویت شما با موفقیت انجام شد.
جهت انتقال به درگاه پرداخت اینترنتی، دکمه پرداخت را بزنید.

بانک سامان

بانک ملت

بانک صادرات

بانک پارسیان

پرداخت

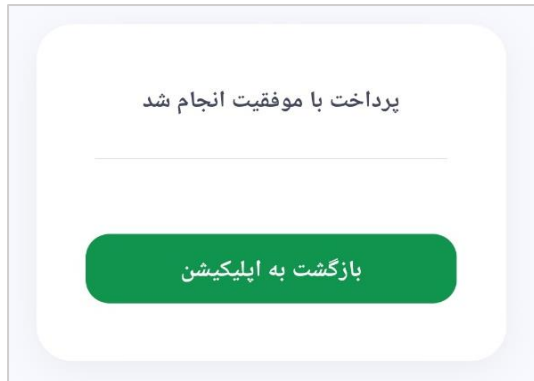
هویت شما مورد تایید قرار گرفت.

پایان

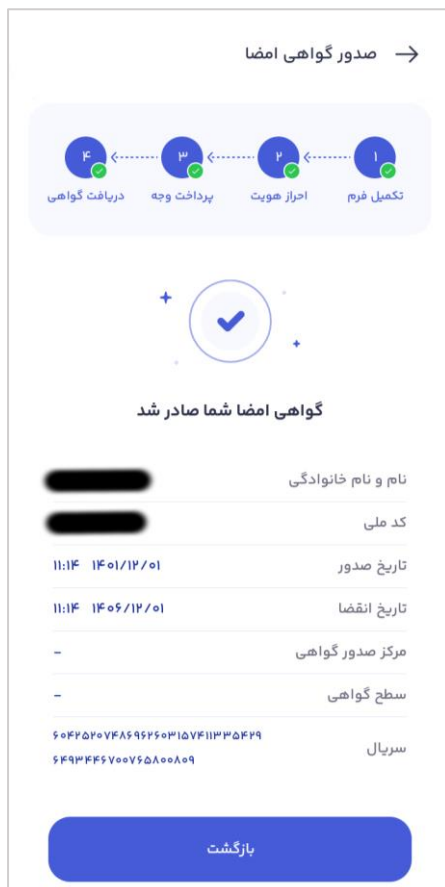
شماره تماس سامانه فرانشاسا: ۰۲۱۷۲۴۲۳۳۰۰

کلیه حقوق سامانه احراز هویت فرانشاسا متعلق به شرکت پردازش اطلاعات مالی پارت است

چنانچه پرداخت موفقیت آمیز باشد صفحه‌ی مقابل، ظاهر می‌گردد که برای بازگشت کاربر به اپلیکیشن می‌باشد.



۴- چنانچه تمامی گام‌های صدور گواهی به درستی انجام پذیرد، فرآیند صدور گواهی امضا با موفقیت همراه بوده و کاربر به صفحه زیر منتقل می‌شود.



در صورتی که عملیات ناموفق باشد تا مدت زمان مشخصی کاربر این امکان را دارد که با استفاده از دکمه تلاش مجدد برای صدور گواهی درخواست دهد، در غیر اینصورت مراحل را باید از ابتدا انجام دهد.

۳-۴- گواهی های من

زمانی که کاربر وارد صفحه «گواهی های من» می شود، می تواند در تب «گواهی های معتبر» گواهی صادر شده و فعال خود، در تب «سایر گواهی ها» لیست همه گواهی هایی که قبلاً صادر شده و به هر دلیلی برچسب ابطال شده، منقضی شده و غیرقابل دسترس (به دلیل پاک کردن دیتا SDK از روی گوشی، فعال بودن گواهی در گوشی دیگر و...) را مشاهده نماید. همچنین می تواند با انتخاب کردن گواهی مورد نظر از جزئیات آن مطلع گردد.

→ گواهی های من

گواهی های معتبر

سایر گواهی ها

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

دوشنبه ۱۷ بهمن ۱۴۰۱ ۱۲:۳۵

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

دوشنبه ۱۷ بهمن ۱۴۰۱ ۱۰:۴۲

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

دوشنبه ۱۷ بهمن ۱۴۰۱ ۱۰:۱۶

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

یکشنبه ۲ بهمن ۱۴۰۱ ۱۲:۵۵

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

یکشنبه ۲ بهمن ۱۴۰۱ ۱۲:۴۸

ابطال شده

گواهی برنز مرکز میانی پارت

صادر شده از اپلیکیشن پارت
تاریخ ابطال:

یکشنبه ۲ بهمن ۱۴۰۱ ۱۰:۵۹

عدم وجود گواهی

گواهی معتبری برای این دستگاه موجود نیست

درخواست صدور گواهی

کاربر گرامی!

توجه فرمایید که گواهی های دیگری که در قسمت "سایر گواهی ها" موجودند، غیرقابل استفاده برای این دستگاه هستند و میباید برای صدور مجدد گواهی اقدام نمایید.

چنانچه برای صدور گواهی نیاز به ابطال دیگر گواهی ها داشتید از قسمت "سایر گواهی ها" گواهی مورد نظر را انتخاب نموده و سپس اقدام به ابطال آن نمایید.

۴-۴- جزئیات گواهی

در این صفحه کاربر می‌تواند اطلاعات گواهی خود را با توجه به مرکز صدور گواهی (CA) و اپلیکیشن میزبان مشاهده نماید.

در صورت منقضی شدن یا ابطال گواهی تاریخ آن نیز قابل مشاهده است.

→ مدیریت گواهی امضا

گواهی برنز مرکز میانی پارت

وضعیت: **ابطال شده**

نام و نام خانوادگی: [مasks]

کد ملی: [masks]

تاریخ صدور: دوشنبه ۱۷ بهمن ۱۴۰۱ ۱۲:۳۴

تاریخ ابطال: یکشنبه ۱۷ بهمن ۱۴۰۶ ۱۲:۳۴

مرکز صدور گواهی: مرکز میانی پارت

سطح گواهی: برنز

سریال: ۵۶۹۵۴۷۱۵۲۹۱۴۸۸۵۳۹۹۳۲۴۱۴۹۸۷۶۹۲۹
۴۵۰۵۷۷۱۹۸۳۹۴۹۱۷۸۷۷

⚠ این گواهی از طریق اپلیکیشن پارت صادر شده است، و صرفاً برای آن قابل استفاده است.

۴-۵- اطلاعات من

در صفحه «اطلاعات من» کاربر می‌تواند اطلاعات شخصی خود را مشاهده یا ویرایش کند. در صورتی که ابتدا مرحله صدور گواهی را طی کرده باشد اطلاعاتی که قبلاً وارد کرده است به طور پیش فرض نمایش داده می‌شود. در غیر اینصورت وقتی وارد این صفحه می‌شود بعد از وارد کردن اطلاعات و زدن دکمه «ذخیره» به صفحه کد تایید منتقل شده و با وارد کردن کدی که به شماره موبایل کاربر ارسال شده و زدن دکمه تایید به همین صفحه باز می‌گردد و اطلاعات ذخیره می‌شود.

→ اطلاعات من

شماره موبایل: ۰۹۱۲ [masks]

کد ملی: ۰۸ [masks]

تاریخ تولد: ۱۳۷۷ [masks]

کد پستی: ۶۹ [masks]

ذخیره

۵- قابلیت‌ها و مزیت رقابتی محصول امضا دیجیتال پارت

محصول امضای دیجیتال مجموعه پارت با تکیه بر قابلیت‌هایی که دارد موفق شده است حدود نیمی از گواهی‌های سطح کشور را صادر نماید، در ادامه به برخی از این قابلیت‌ها اشاره شده است:

- ✓ پشتیبانی از چندین CA : شرکت پارت امکان برقراری ارتباط و همکاری فنی با چندین مرجع صدور گواهی (Certification Authority - CA) را فراهم نموده است.
- ✓ پایداری و انعطاف‌پذیری: در صورت بروز اختلال یا قطعی در سرویس یکی از CA ها، سامانه به‌صورت خودکار به مرجع دیگر سوئیچ می‌کند تا فرآیند صدور و امضای دیجیتال بدون وقفه ادامه یابد. این معماری چندمرجعی، موجب افزایش پایداری، دسترس‌پذیری و سرعت ارائه خدمات امضای دیجیتال می‌گردد.
- ✓ تیم امنیت و مانیتورینگ تخصصی: زیرساخت‌های محصول امضای دیجیتال شرکت پارت توسط تیم تخصصی امنیت به‌صورت ۲۴ ساعته و در تمامی روزهای هفته (۲۴×۷) پایش و پشتیبانی می‌شود. هدف از این پایش مستمر، اطمینان از امنیت داده‌ها، حفظ دسترس‌پذیری سرویس، و پیشگیری از تهدیدات و حملات سایبری است. همچنین سامانه امضای دیجیتال پارت از پشتیبانی فنی ۲۴×۷ برخوردار است تا در صورت بروز هرگونه اختلال، خدمات بدون تأخیر بازیابی گردد.
- ✓ قابلیت امضای گروهی به صورت سری و موازی
- ✓ راهکارهای متنوع ارائه خدمت با توجه به نیاز سازمان‌ها

✓ تنها SDK امضا در سطح کشور با قابلیت صدور گواهی از اکثر مراکز میانی صدور گواهی
امضا

✓ دارا بودن امکان ابطال گواهی توسط کاربر با استفاده از CRR و احراز هویت مبتنی بر
سرویس‌های حاکمیتی

✓ دارای قابلیت بررسی مشخصات متقاضی صدور گواهی از طریق سرویس‌های حاکمیتی
✓ دارای قابلیت‌های هوش مصنوعی در احراز هویت؛ امکان تشخیص چهره، امکان تطبیق
چهره، بررسی زنده بودن و بررسی آگاهی کاربر

✓ امکان نمایش لیست گواهی‌های صادر شده کاربر از طریق تمامی اپلیکیشن‌های متصل
به هاب صدور گواهی امضای پارت

✓ دارای انعطاف‌پذیری مناسب جهت شخصی‌سازی رابط کاربری SDK

✓ امکان امضای اسناد PDF با استاندارد PAdES از طریق توابع در اختیار اپلیکیشن
میزبان

✓ امکان امضای XAdES از طریق توابع در اختیار اپلیکیشن میزبان

✓ دارای قابلیت ذخیره سازی کلید در eSE و اجرای فرآیند امضا در TEE جهت فراهم کردن
انکار ناپذیری امضا

✓ دارای مهر زمانی اسناد از طریق TSA

۶- اجزای زیرساخت محصول

همان‌طور که پیش‌تر در بخش مقدمه نیز به آن اشاره نمودیم، وجود مولفه‌هایی در زیرساخت محصول امضای دیجیتال فراشناسا این اطمینان را جهت تایید مهم‌ترین ویژگی‌های آن از جمله انکارناپذیری، ایمن بودن و قابل اعتماد بودن حاصل می‌نماید. این مولفه‌ها جهت اطمینان از ویژگی‌های اصلی محصول عوامل زیر را به دقت بررسی می‌نماید؛

- اطمینان از هویت شخص متقاضی امضا در زمان صدور گواهی
- اطمینان از زمان امضای سند
- اطمینان از صحت و اعتبار گواهی در زمان تایید

در ادامه به بررسی دقیق‌تر این مولفه‌های زیرساختی شامل مرکز ثبت گواهی، کیت توسعه نرم‌افزار مدیریت گواهی، سرویس اعتبارسنجی گواهی‌های دیجیتال، سرویس مدیریت گواهی‌های قابل اعتماد، سرویس مرکز صدور مهر زمانی و مانیتورینگ و قابلیت اتکا سامانه پرداخته شده است.

۶-۱- مرکز ثبت گواهی (RA)

یک مرجع ثبت (RA)، جزء حیاتی زیرساخت کلید عمومی (PKI) است که نقش مهمی در فرآیند صدور گواهی ایفا می‌کند. دلیل اصلی توسعه RA این است که اطمینان حاصل شود که صدور گواهی‌های دیجیتال به صورت ایمن، قابل اعتماد و انکارناپذیر انجام می‌شود. تاییدیه‌های زیر به کمک این توسعه انجام می‌پذیرد؛

- تأیید هویت متقاضیان گواهی؛ برای این مهم احراز هویت کاربر از طریق هوش مصنوعی به فرآیندهای یک RA اضافه گردیده است که این احراز هویت از طریق سامانه‌های موجود انجام می‌شود. علاوه بر این اطلاعات ارائه شده توسط کاربر از طریق سامانه‌های حاکمیتی سنجیده می‌شود.
- اطمینان از واقعی بودن درخواست صدور گواهی
- اطمینان از مالکیت کلید خصوصی توسط کاربر
- اطمینان از ذخیره سازی امن و قابل اعتماد بودن کلید کاربر
- حفظ حریم خصوصی کاربران
- مدیریت ابطال گواهی کاربران

یکی دیگر از عوامل مهم در توسعه RA نیاز به مقیاس‌پذیری است. از آنجایی که کاربران و دستگاه‌های بیشتری به گواهی‌های دیجیتال نیاز دارند، RA باید بتواند این رشد را تطبیق دهد و حجم فزاینده درخواست‌های گواهی را مدیریت نماید. این امر مستلزم یک زیرساخت مناسب است که قادر به مدیریت فرآیندها و رویه‌های کارآمد جهت صدور گواهی باشد که در محصول امضای دیجیتال فراشناسا محقق گردیده است.

در نهایت، داشتن یک برنامه اضطراری در صورت خرابی و یا نقص زیرساخت‌های RA حائز اهمیت است که شامل سیستم‌ها و فرآیندهای پشتیبانی و همچنین رویه‌های واکنش به حادثه جهت اطمینان از ادامه فرآیند صدور گواهی در صورت ایجاد وقفه، می‌باشد.

با توجه به اینکه هر گواهی باید از نظر CA برای هر شخص یکتا باشد، امکان ارائه خدمات به کاربران مختلف در اپلیکیشن‌های مختلف تنها از طریق یک مرکز صدور گواهی امکان‌پذیر

نمی‌باشد. برای فائق آمدن بر این مشکل شرکت پارت اقدام به راه اندازی RA نموده است که به عنوان یک هاب بتواند با تمامی مراکز صدور گواهی معتبر موجود در کشور هماهنگ شده و در صورت لزوم امکان صدور گواهی برای کاربر را از طریق مراکز مختلف فراهم نماید. به علت تفاوت در نحوه پیاده‌سازی ارتباط با مراکز مختلف و لزوم برقراری این ارتباط به صورت انکارناپذیر (احراز هویت مبتنی بر چالش) هیچ یک از ابزارهای متن‌باز موجود، توان مدیریت چنین درخواست‌هایی را نداشته و لازم است معماری خاصی برای یک RA توسعه یابد به صورتی که از خطوط قرمز استاندارد‌های این حوزه عبور نکند و علاوه بر این تطبیق لازم را با زیرساخت‌های کشور در این حوزه داشته باشد که تمامی این موارد در محصول امضای دیجیتال فراشناسا پیاده‌سازی شده است.

۲-۶- کیت توسعه نرم‌افزار مدیریت گواهی (SDK)

در گذشته صدور گواهی امضا تنها در توکن‌های سخت افزاری امکان پذیر بود. این الزام، کاربر را ناچار به مراجعه حضوری به دفاتر اسناد رسمی و همچنین صرف هزینه برای تهیه توکن می‌نمود. فرایند صدور سنتی گواهی از طریق دفاتر اسناد رسمی، بزرگترین مانع برای افزایش ضریب نفوذ خدمات دولت الکترونیک در کشور بوده است.

راهکارهای این حوزه مبتنی بر احراز دو عامل است؛ عامل اول وجود سخت افزار حامل کلید و عامل دوم آگاهی کاربر جهت استفاده از کلید است. به منظور مرتفع نمودن سطح استانداردهای موجود از Trusted Execution Environment (TEE) و Embedded Secure Element (ESE) و گره زدن آن با عنصر امنیتی گوشی تلفن همراه کاربر، می‌بایست

استخراج و بازیابی کلید را غیر ممکن ساخته و همچنین استفاده از آن بدون اطلاع کاربر حتی برای توسعه دهنده و مدیر سیستم ناممکن باشد. از آنجایی که کلید کاربر به گوشی همراه او (به عنوان سخت افزار) گره خورده است، این SDK به همراه RA باید نقش جایگزین دفاتر اسناد رسمی را ایفا کرده و از طرف دیگر، ابزارهای لازم برای استفاده از کلید و رمزنگاری داده‌ها را فراهم کند.

۳-۶- اعتبارسنجی امضای اسناد دیجیتال

هدف از طراحی و تولید این سرویس حصول اطمینان از بکارگیری صحیح استانداردها و مولفه‌های سطح اطمینان در کلیه اسناد و تراکنش‌های موجود در زیست بوم محصول است. این سرویس با بررسی اعتبار گواهی‌های دیجیتال اشخاص، سرویس‌های همکار و سازمان‌ها از منظر اعتبار زمانی، کاربردی و مرکز صدور گواهی این اطمینان را ایجاد می‌کند که استفاده از گواهی در یک مسئله خاص مورد تایید باشد.

همچنین وجود مولفه‌های سطح اطمینان بر مبنای استاندارد AdES که توسط ETSI ارائه شده است، مورد ارزیابی قرار می‌گیرد. در خصوص بررسی اطمینان از انواع امضاهای دیجیتال تحقیقات گسترده‌ای در حوزه امضای فایل‌های PDF، XML، JSON و کلیه داده‌های باینری به صورت جداگانه انجام شده است. پس از مطالعه و تطبیق استانداردهای کارگروه مهندسی اینترنت (IETF) و موسسه استانداردهای مخابرات اروپا (ETSI) به یک جمع بندی درخصوص مولفه‌های تاثیرگذار در هر نوع امضا رسیده، که در هرکدام از این انواع امضا علاوه بر الگوریتم رمزنگاری و الگوریتم‌های درهم‌ساز فایل (Hash Algorithms)، مولفه‌های خاص‌تری جهت

انتساب انکارناپذیری امضا به شخص امضا کننده، زمان امضا فایل، نوع داده امضا شده نیز وجود دارد.

سرویس امضای دیجیتال شرکت پارت، تمام مؤلفه‌های مربوط به جامعیت سند و انکارناپذیری امضا را بررسی می‌کند. پس از بررسی، نتیجه در یکی از سه حالت زیر ارائه می‌شود:

- **قابل اعتماد:** امضا معتبر است، گواهی دیجیتال معتبر و فایل بدون تغییر است.
- **غیر قابل اعتماد:** امضا نامعتبر است؛ به عنوان مثال گواهی منقضی شده یا فایل تغییر یافته است.
- **غیر قابل تشخیص:** اطلاعات کافی برای تصمیم‌گیری وجود ندارد؛ سیستم نمی‌تواند با قطعیت اعتبار امضا را تعیین کند.

این خروجی، پایه و مبنای تصمیم‌گیری‌های بعدی در کل سامانه می‌باشد و به اطمینان از صحت تراکنش‌ها و اسناد دیجیتال کمک می‌کند.

۴-۶- مدیریت گواهی‌های قابل اعتماد

با توجه به تعدد مراکز صدور گواهی و امکان صدور گواهی توسط مراکز غیر رسمی و یا مراکز غیر قابل اعتماد، نیاز به بررسی اعتبار مراکز صدور گواهی‌های مورد استفاده در کل سامانه و همچنین تفاوت مراکز صدور مورد اعتماد در سیستم‌ها، زیرسیستم‌ها و محیط‌های مختلف، نسبت به یک سرویس مرکزی جهت مدیریت وجود دارد.

پس از تعیین ویژگی‌های مورد نیاز این سرویس و مشخص نمودن مولفه‌های اصلی آن از جمله ساختار لیست گواهی‌های قابل اعتماد (که به صورت یک XML ارائه می‌شود)، استفاده از

XAdES برای امضای فایل (جهت انکارناپذیری و حفظ امنیت)، تاریخ انقضا لیست و ایجاد فایل به صورت دوره ای، سرویس مورد نظر با موفقیت پیاده سازی شده است.

۵-۶- مرکز صدور مهر زمانی (TSA)

با توجه به اهمیت زمان امضا و تاثیر آن در نتیجه‌ی صحت‌سنجی فایل امضا شده، نیاز به یک سرویس جهت صدور مهر زمانی معتبر وجود دارد. با توجه به اینکه مهر زمانی برای یک امضا، مولفه‌ای کلیدی می‌باشد و همچنین با توجه به اینکه سرویس‌های موجود کیفیت لازم و توانایی ارائه این سرویس به صورت پایدار را ندارد، نیاز به این سرویس به صورت خصوصی با قابلیت اطمینان بالا مورد نیاز واقع شده است.

این سرویس توسط کارگروه مهندسی اینترنت (IETF) در RFC به شماره ۳۱۶۱ مستند شده است که بر اساس مستندات TSP موجود در همین استاندارد پیاده‌سازی شده است. طبق این مستند مهر زمانی باید مولفه‌هایی در خصوص انکارناپذیری مرکز صدور خود و داده‌های برای آن درخواست شده است، داشته باشد. این مهر زمانی ساختار ویژه‌ای دارد که کلیه اطلاعات مورد نیاز در زمان بررسی دعاوی حقوقی را ارائه می‌دهد.

۶-۶- مانیتورینگ و قابلیت اتکا سامانه

جهت مانیتورینگ و اطمینان از صحت عملکرد سرویس‌های موجود از تکنولوژی‌ها و ابزارهای قابل اندازه‌گیری و معتبر این حوزه استفاده می‌شود که در صورت بروز هرگونه مشکل در سیستم‌ها سریعاً مطلع شده و با کمک لاگ‌های موجود فوراً مشکل را برطرف نماید.