راهنمای کاربری برنامه مهر و موم



تهیه شده در:

شرکت پندار کوشک ایمن

زیرساخت کلید عمومی و امنیت اطلاعات

نسخه :	۱/۱
تاریخ :	بهار ۱۴۰۰
شناسه :	PKI-SignAndSealUserGuide-v1.1
طبقه‌بندی :	عمومی

تفاهم نامه عدم افشاء

این مستند توسط شرکت پندار کوشک ایمن و با توجه به محصول مهر و موم (SAS) تهیه شده است و تمامی حقوق آن متعلق به شرکت پندار کوشک ایمن می باشد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

تاریخچه گزارش

نسخه	تاریخ	تهیه کننده/گان	مرورکننده/گان	توضیحات
۱/۰	۱۳۹۹/۰۴/۲۲	کارشناس پروژه		تهیه نسخه اولیه سند
۱/۱	۱۴۰۰/۰۱/۱۷	کارشناس پروژه		به روزرسانی سند مطابق با آخرین نسخه محصول

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

فهرست

فهرست ۳
۱ مقدمه ۴
۲ مفاهیم پایه ۵
۲,۱ رمزنگاری نامتقارن ۵
۲,۲ گواهینامه دیجیتال ۶
۳ نصب برنامه مهر و موم ۷
۴ استفاده از برنامه مهر و موم ۱۰
۴,۱ امضای دیجیتال ۱۰
۴,۲ بررسی امضا ۱۷
۴,۳ رمزنگاری فایل ۲۴
۴,۴ رمزگشایی فایل ۳۴
۵ امضا و رمزنگاری ۳۷
۶ رمزنگاری و امضا ۴۰
۷ رمزگشایی و بررسی امضا ۴۲
۸ نکات پایانی ۴۴
۹ پیوست الف ۴۵
۱۰ پیوست ب ۴۸
۱۱ پیوست پ ۴۹

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۱ مقدمه

مهر و موم محصولی از شرکت پندار کوشک ایمن است که با هدف سندیت بخشی به اسناد و فایل های مختلف و حفظ محرمانگی اطلاعات در دنیای دیجیتال، پیاده سازی شده است.

این برنامه مبتنی بر ویندوز می باشد و بر مبنای الگوریتم رمزنگاری نامتقارن پیاده سازی شده و شامل ۴ بخش امضای دیجیتال، بررسی امضا، رمزنگاری و رمزگشایی است که نسخه رایگان آن تنها امکان امضای دیجیتال و بررسی امضا را ارایه می دهد و برای دسترسی امکان رمزنگاری و رمزگشایی باید از نسخه لایسنس دار برنامه استفاده شود.

در ابتدای این مستند آموزشی یکسری مفاهیم پایه در ارتباط با روش رمزنگاری نامتقارن و گواهینامه دیجیتال جهت درک بهتر عملکرد برنامه مهر و موم شرح داده می شود و در ادامه نیز نحوه نصب و استفاده از بخش های مختلف برنامه جهت تحقق بخشیدن به اهداف ذکر شده بیان می شود.

از آن جایی که برخی از فایل ها دارای ماهیت حقوقی می باشند و نیاز است پیش از رمز نمودن آن ها صحت محتویات فایل توسط افراد مربوطه مورد تایید قرار گیرد مانند اسناد مالی و اداری و یا قرارداد ها و تفاهم نامه ها که

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۲ مفاهیم پایه

۲,۱ رمزنگاری نامتقارن

در روش رمزنگاری نامتقارن از یک زوج کلید عمومی و خصوصی به منظور رمزنگاری و رمزگشایی اطلاعات استفاده می شود که کلید عمومی می تواند به صورت گسترده منتشر شود و در اختیار عموم قرار گیرد ولی کلید خصوصی تنها دراختیار مالک آن قرار دارد. در این روش هر پیامی که توسط کلید خصوصی امضا شود تنها با استفاده از کلید عمومی متناظر با آن صحت سنجی می شود و هر پیامی که با استفاده از کلید عمومی رمز شود تنها از طریق کلید خصوصی متناظر با آن رمزگشایی می شود و مالکیت این زوج کلید به واسطه گواهینامه دیجیتالی که توسط مراکز صدور گواهی برای متقاضیان، صادر شده است ثابت می شود.

در فرآیند امضای دیجیتال به منظور سندیت بخشی به اسناد و فایل های موردنظر از **کلید خصوصی** شخص امضاکننده برای امضا استفاده می شود تا هنگام صحت سنجی امضا بتوان هویت امضا کننده را تصدیق نمود چرا که این فایل تنها با استفاده از کلید عمومی متناظر با کلید خصوصی که برای امضا استفاده شده است قابل صحت سنجی می باشد و این کلید خصوصی نیز تنها در اختیار مالک آن قرار دارد بنابراین در این روش فرد امضا کننده قادر به انکار امضا نمی باشد.
در عملیات امضای دیجیتال برای اطمینان از صحت محتویات فایل، از فرآیند چکیده سازی[۱] استفاده می شود. در این فرآیند داده ورودی به یک مقدار ثابت منحصر به فرد در خروجی تبدیل می شود و در نهایت این مقدار ثابت که به آن چکیده نیز گفته می شود توسط کلید خصوصی امضاکننده، امضا می شود. بنابراین هنگام بررسی صحت فایل امضا شده، چکیده فایل اصلی مجدد محاسبه می شود و با چکیده امضا شده تطبیق داده می شود. که مطابقت داشتن این دو مقدار به آن معنی است که فایل امضا شده پس از امضا دچار تحریف و دستخوردگی نشده است و قابل استناد می باشد.

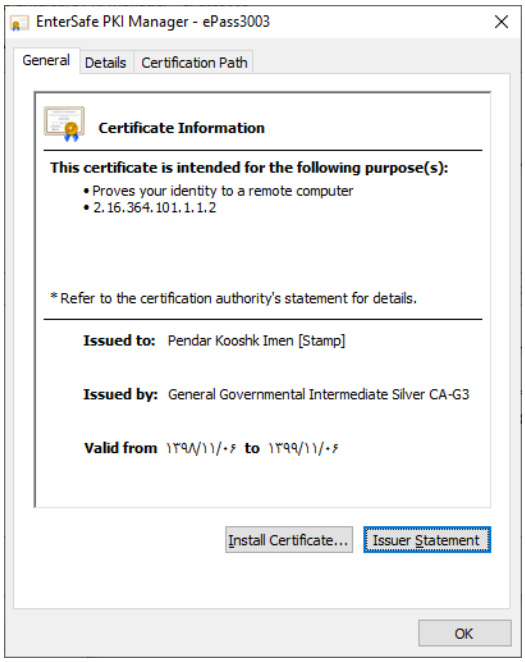
در فرآیند رمزنگاری به منظور حفظ محرمانگی و جلوگیری از دسترسی افراد غیر مجاز به اسناد و فایل های موردنظر از کلید عمومی شخص گیرنده برای رمزنگاری استفاده می شود چرا که این فایل رمز شده تنها با استفاده از کلید خصوصی متناظر با کلید عمومی وی که برای رمزنگاری استفاده شده است قابل رمزگشایی می باشد و این کلید خصوصی نیز تنها در اختیار مالک آن یا گیرنده فایل رمز قرار دارد بنابراین تنها او می تواند اسناد و فایل های رمز شده را رمزگشایی کند.

[۱] Hashing

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۲,۲ گواهینامه دیجیتال

گواهینامه دیجیتال یک فایل دیجیتال است که مالکیت کلید عمومی و کلید خصوصی متناظر با آن را ثابت می کند و شامل کلید عمومی، مدت اعتبار، کاربرد گواهی و یکسری اطلاعات درمورد صاحب گواهی، صادر کننده گواهی و زنجیره گواهی است.



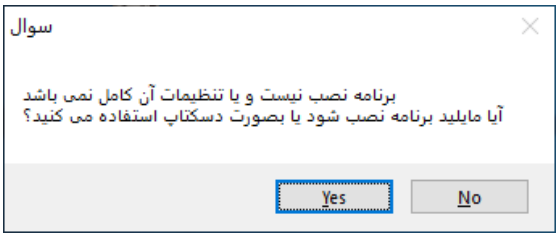
گواهینامه دیجیتال به همراه زوج کلید عمومی و خصوصی داخل یک key store یا مخزن کلید ذخیره می شود. توکن و کارت هوشمند از انواع key store های سخت افزاری هستن که به آن ها ماژول رمز نگاری نیز گفته می شود و برای key store های نرم افزاری هم می توان به فایل p12 اشاره نمود و از آن به عنوان توکن نرم افزاری نام برد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

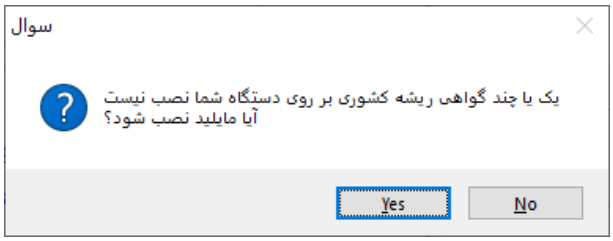
۳ نصب برنامه مهر و موم

فایل نصبی برنامه مهر و موم را می توانید با مراجعه به سایت www.pki.co.ir و یا از طریق اسکن QRCode زیر دریافت کنید و سپس طبق روال گفته شده برای نصب آن اقدام نمایید.

۱. در قدم اول ارتباط سیستم با اینترنت را برقرار نموده و سپس فایل نصبی برنامه را با دسترسی مدیر سیستم اجرا نمایید و در پیام نمایش داده شده برروی گزینه "Yes" کلیک کنید.

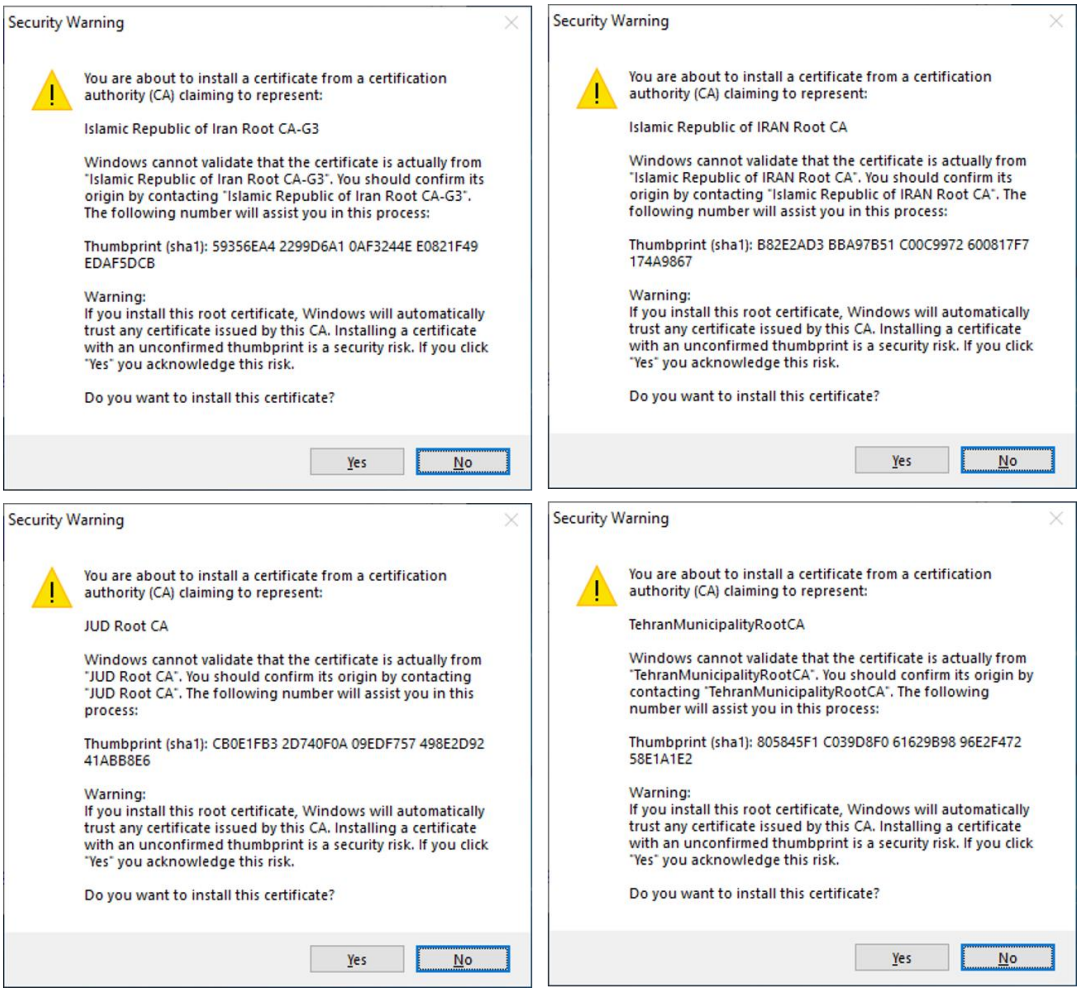


۲. با اولین بار اجرا شدن برنامه مهر و موم، پنجره ای جهت نصب گواهی های ریشه کشوری نمایش داده می شود در این پنجره با کلیک برروی گزینه "Yes" فرآیند نصب را آغاز نمایید.



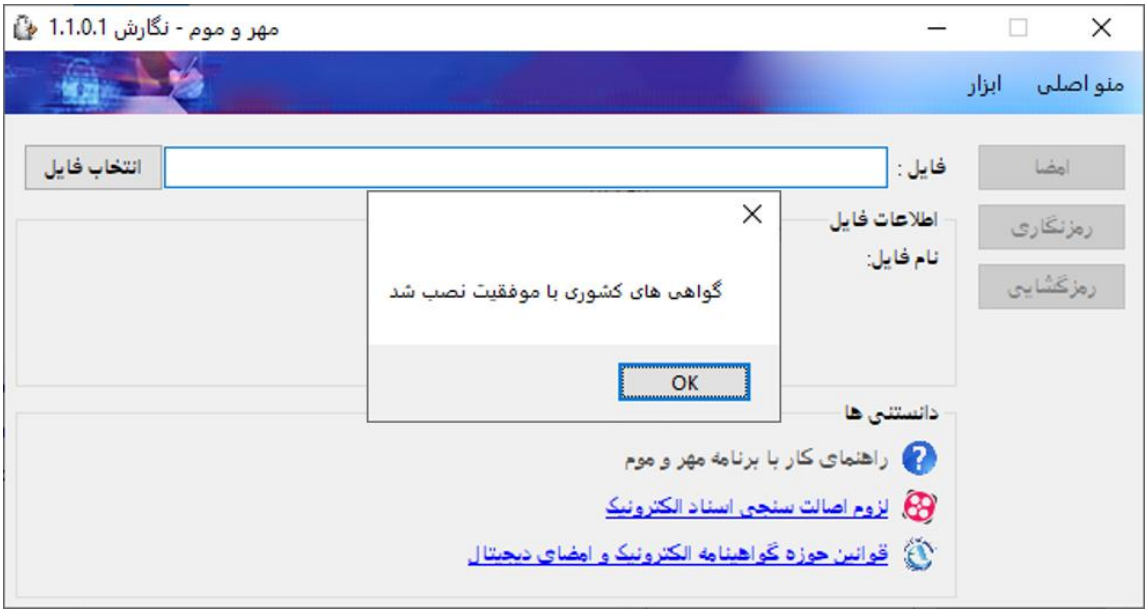
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳. سپس در پیام های نمایش داده شده با انتخاب گزینه "Yes"، مجوز نصب گواهی های ریشه کشوری را صادر کنید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۴. با اتمام موفقیت آمیز فرآیند نصب گواهی های ریشه کشوری، پیام زیر نمایش داده می شود. در پیام نمایان شده برروی گزینه ok کلیک نمایید.



۵. اکنون می توانید جهت انجام عملیات امضای دیجیتال و رمزنگاری مطابق با توضیحات بند ۵ اقدام نمایید.

توجه:

درنظر داشته باشید که به منظور استفاده از برنامه مهر و موم می بایست ارتباط سیستم با اینترنت برقرار باشد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۴ استفاده از برنامه مهر و موم

۴,۱ امضای دیجیتال

با نظر به این که برخی از فایل ها دارای ماهیت حقوقی می باشند و نیاز است تا صحت محتویات آن ها توسط شخص/اشخاص مربوطه مورد تایید قرارگیرد، برنامه مهر و موم این امکان را فراهم آورده است تا بتوان فایل های موردنظر را جهت سندیت بخشی و انکار ناپذیری به دفعات موردنیاز توسط افراد مربوطه امضا نمود. از این رو در پایان فرآیند امضای دیجیتال از کاربر پرسیده می شود " آیا شخص دیگری هم فایل را امضا می کند یا نه" . در ادامه این سند، روال امضای فایل های موردنظر به صورت کامل شرح داده می شود.

۱. به منظور امضای اسناد و فایل های موردنظر ابتدا برنامه مهر و موم را اجرا نموده و با کلیک برروی گزینه "انتخاب فایل"، فایل مورد نظر را انتخاب نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۲. پس از انتخاب فایل موردنظر برروی گزینه "امضا" کلیک کنید.



۳. گزینه های نمایش داده شده در پنجره امضا، می بایست مطابق با توضیحاتی که در ادامه بیان شده است، در وضعیت فعال یا غیر فعال قرارگیرند.



➢ **فقط با توکن یا کارت هوشمند امضا می کنم**

درصورتی که گواهی امضا دیجیتال، برروی ماژول رمزنگاری قرار دارد ابتدا ماژول را به سیستم متصل نمایید و سپس گزینه "فقط با توکن یا کارت هوشمند امضا می کنم" را در حالت فعال قراردهید. بدیهی است که برای استفاده از توکن نرم افزاری این گزینه باید غیرفعال باشد.

به منظور نصب توکن نرم افزاری می توانید به توضیحات پیوست "الف" مراجعه نمایید.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

توجه:

درحال حاظر این نسخه از محصول مهرم و موم، توکن نرم افزاری را پشتیبانی نمی کند.

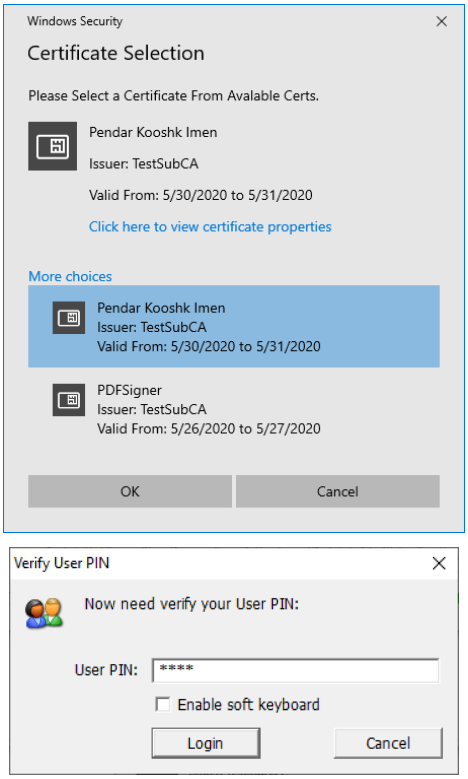
➢ **در قالب pdf اطلاعات امضا کننده را طبق قوانین مرکز دولتی ریشه اضافه کن**

درصورتی که فایل انتخابی از نوع pdf می باشد، با فعال نمودن این گزینه، اطلاعات شخص امضا کننده در قالب تصویر امضا، در فایل pdf امضا شده درج خواهد شد.

درنظر داشته باشید درصورتی که فایل انتخابی از نوع pdf نباشد، این گزینه به صورت پیش فرض غیرفعال خواهد بود.

در پایان پس از آن که تنظیمات موردنظر را طبق توضیحات شرح داده شده اعمال نمودید، بروی گزینه "امضا" کلیک نمایید.

۴. در پنجره نمایش داده شده گواهی موردنظر را برای امضا انتخاب کنید و سپس پین توکن را وارد نمایید.

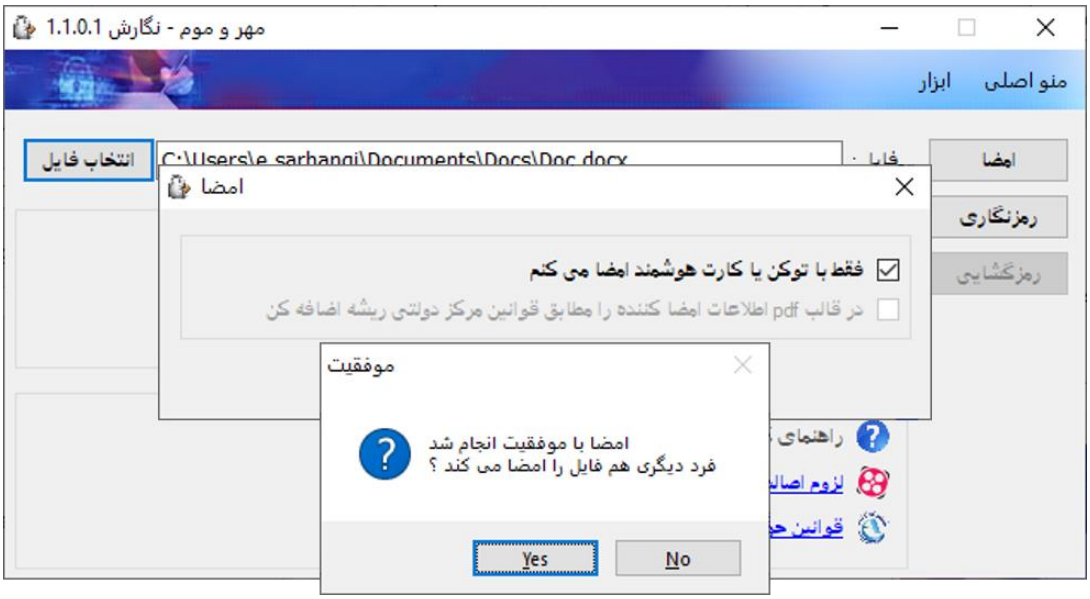


نکته:

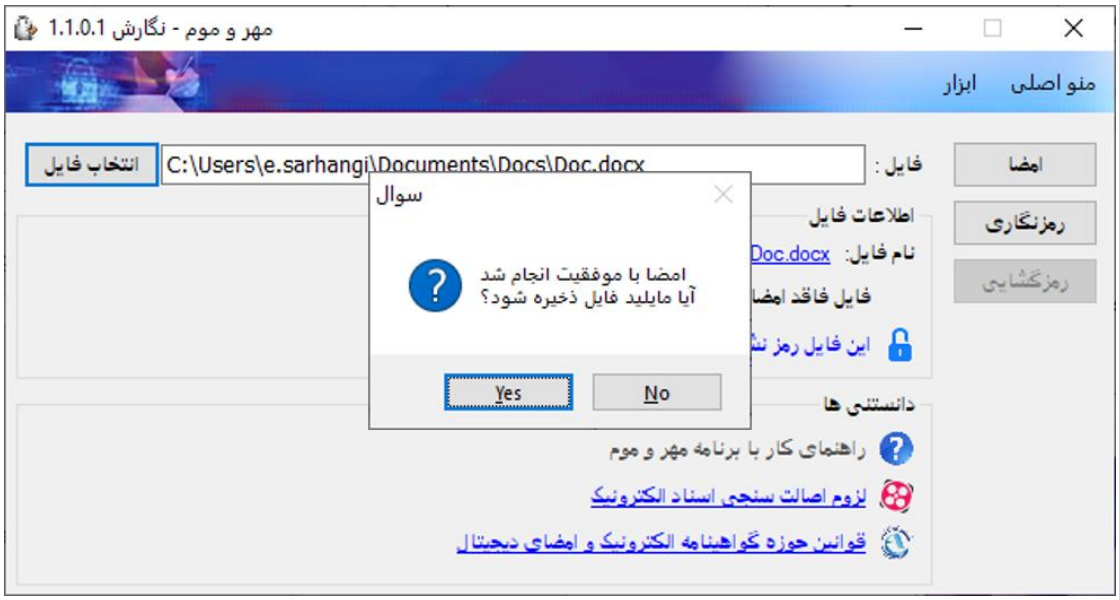
پنجره انتخاب گواهی زمانی نمایش داده می شود که بروی ماژول رمزنگاری، بیش از یک گواهی برای کاربرد امضای دیجیتال قرار داشته باشد در غیر این صورت پنجره ای برای انتخاب گواهی نمایان نمی شود و از همان یک گواهی موجود برروی ماژول رمزنگاری جهت امضا استفاده خواهد شد و تنها کافی است پین ماژول را وارد نمایید.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۵. درصورتی که فرآیند امضا دیجیتال با موفقیت پایان پذیرد ، نتیجه فرآیند طی یک پیام نمایش داده می شود. چنانچه تعداد امضاهای موردنظر به اتمام رسیده است گزینه "No" را انتخاب نمایید. در غیر این ابتدا ماژول رمزنگاری فرد دیگر را به سیستم متصل نموده و سپس در پیام نمایش داده شده برروی گزینه "Yes" کلیک نمایید و اقدامات گفته شده در مراحل ۳ و ۴ را مجددا تکرار نمایید.



۶. با اتمام موفقیت آمیز عملیات امضای دیجیتال ، پنجره زیر نمایان می شود. با کلیک برروی گزینه "Yes" یک فایل با پسوند esf به عنوان فایل امضا در مسیر فایل اصلی ذخیره خواهد شد. **شایان ذکر است** که فایل امضا تولید شده در فرمت esf، تنها از طریق برنامه مهر و موم قابل ارزیابی می باشد.

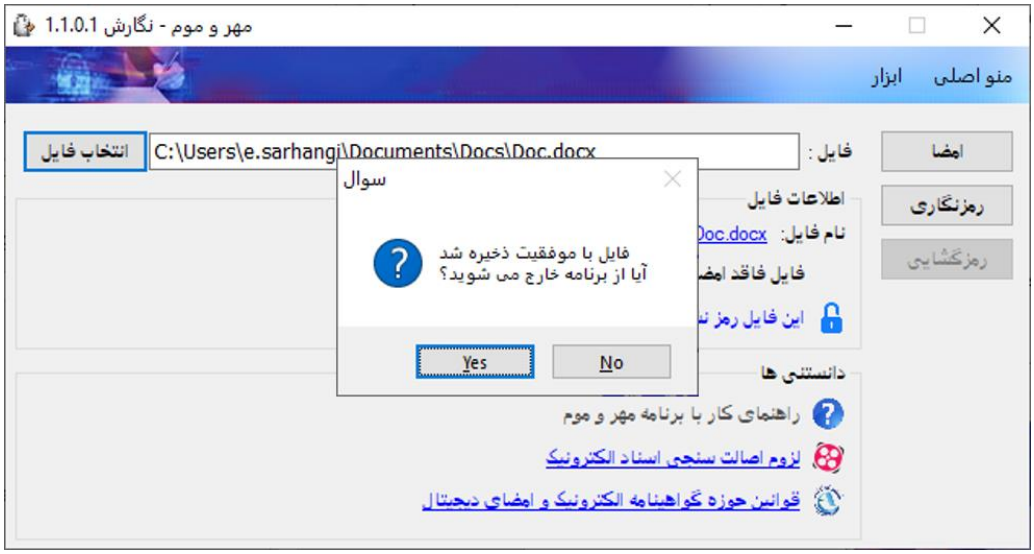


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

نکته:

درصورتی که فایل انتخاب شده جهت امضا، از نوع pdf باشد، علاوه بر فایل امضا، یک فایل pdf امضا شده نیز در محل فایل اصلی ذخیره می شود که این فایل pdf امضا شده، توسط برنامه های استانداردی که برای نمایش و استفاده از اسناد با فرمت pdf استفاده می شوند قابل اجرا می باشد. برنامه هایی همانند Adobe Acrobat Reader و Foxit reader.

۷. با اتمام موفقیت آمیز فرآیند ذخیره سازی فایل امضا، پیام زیر نمایان می شود. درصورتی که قصد دارید فایل امضا تولید شده را ارزیابی نمایید برروی گزینه "No" کلیک کنید. در غیر این صورت چنانچه عملیات موردنظر به اتمام رسیده است با انتخاب گزینه "Yes" از برنامه خارج شوید.



۸. با پایان یافتن فرآیند ارزیابی امضا، نتیجه بررسی طی یک پیام نمایان می شود.

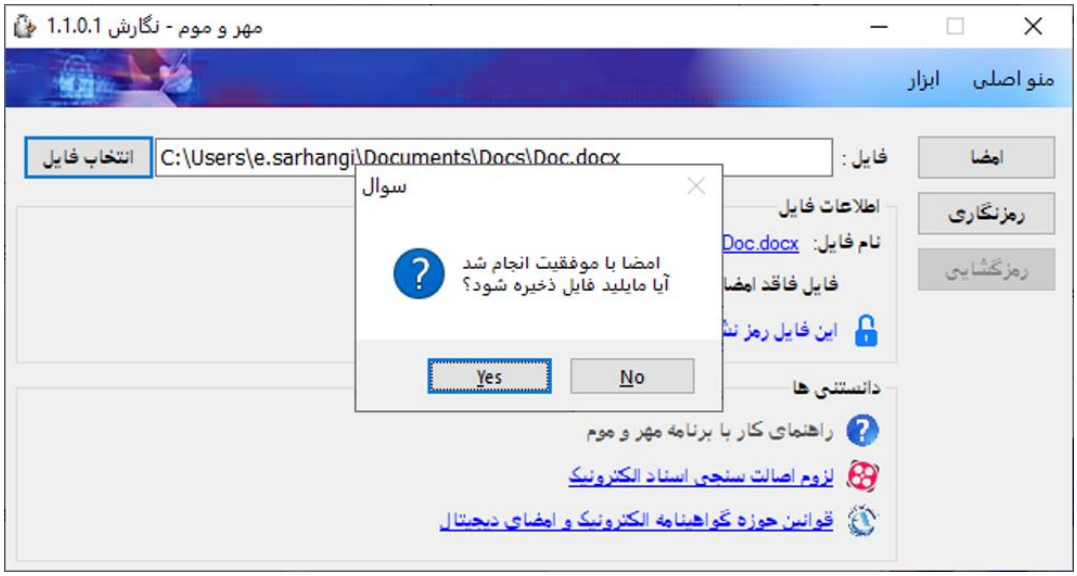


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

درنظر داشته باشید که در بخش بررسی امضا، فرآیند ارزیابی اسناد و فایل های امضا شده به صورت کامل شرح داده شده است بنابراین می توانید جهت آشنایی بیشتر با این فرآیند، به توضیحات بند ۴,۲ مراجعه نمایید.

نکته:

درصورتی که تمایل دارید فایل امضا را در مسیری مجزا از مسیر فایل اصلی ذخیره نمایید، کافی است در مرحله ذخیره سازی فایل امضا (**مرحله ۵**)، در پیام نمایان شده گزینه "No" را انتخاب کنید.



سپس با انتخاب گزینه "ذخیره"، مسیر مورد نظر خود را برای ذخیره سازی فایل امضا مشخص نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

بیشتر بدانیم:

لازم به توضیح است که در برنامه مهر و موم می بایست از یک گواهی معتبر جهت امضا و رمزنگاری اسناد و فایل های موردنظر استفاده شود و یک گواهی زمانی معتبر است که از لحاظ زنجیره گواهی[1]، مدت زمان اعتبار و کاربرد مورد تایید باشد که درصورت معتبر نبودن هر یک از موارد گفته شده پیغامی مناسب نمایش داده خواهد شد.

- **گواهی انتخاب شده باطل شده است.**
- **گواهی انتخاب شده منقضی شده است.**
- **گواهی انتخاب شده برای کاربری امضای دیجیتال صادر نشده است.**
- **امکان اعتبارسنجی گواهی وجود ندارد.**
- **امکان اعتبارسنجی زنجیره گواهی وجود ندارد.**

درنظر داشته باشید درصورتی که گواهی امضا منقضی شده یا باطل شده باشد و یا برای کاربری امضای دیجیتال صادر نشده باشد باید جهت دریافت مجدد گواهی به مرکز صدور گواهی مراجعه کنید و درصورتی که امکان اعتبارسنجی گواهی و زنجیره گواهی وجود نداشته باشد، ابتدا باید از اتصال به اینترنت اطمینان حاصل نمایید و سپس زنجیره گواهی را طبق توضیحات "پیوست ب" بررسی کنید.

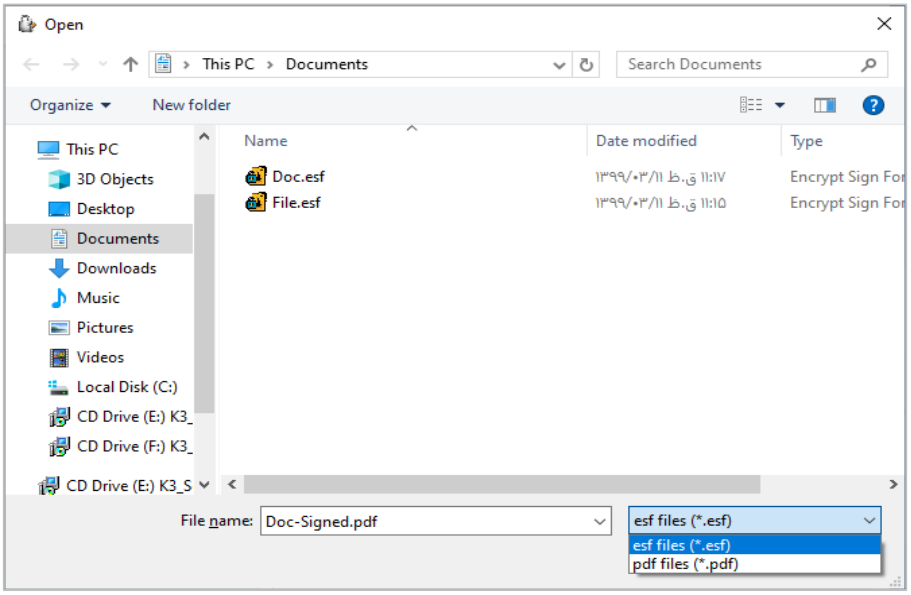
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۴,۲ بررسی امضا

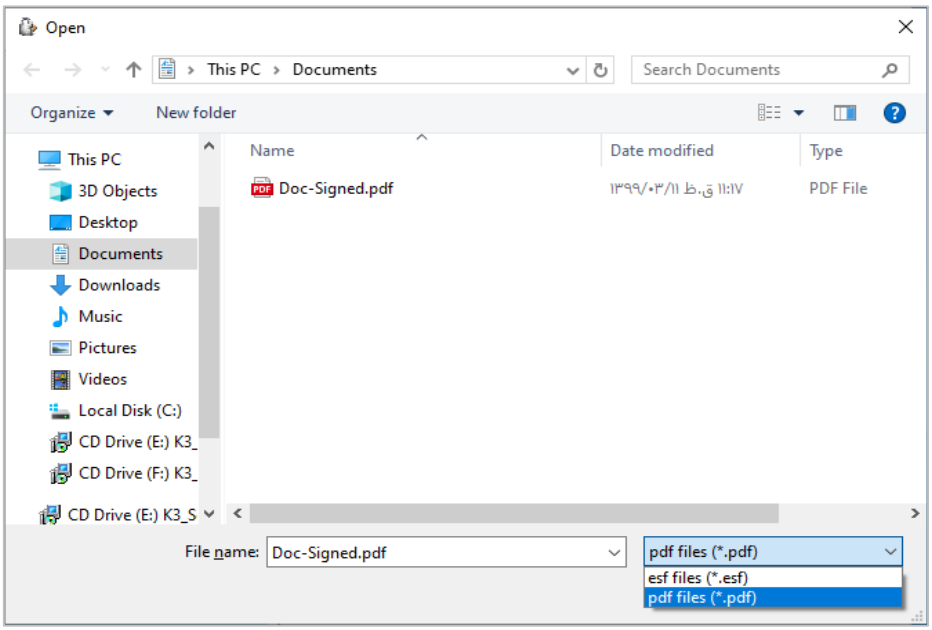
به منظور ارزیابی فایل امضای موردنظر جهت اطمینان از صحت محتویات آن و تصدیق هویت امضا کننده، کافی است برنامه مهرم و موم را اجرا نموده و برروی گزینه "انتخاب فایل" کلیک نمایید.



در پنجره نمایش داده شده می توانید فایل های esf تولید شده در فرآیند امضای دیجیتال و همچنین اسناد امضا شده با فرمت PDF را انتخاب نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.



با انتخاب فایل امضا، فرآیند ارزیابی آغاز می شود و در پایان نیز، نتیجه فرآیند طی یک پیام گزارش می شود.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

نتیجه بررسی امضا شامل یکی از موارد زیر می باشد:

- امضا معتبر است.
- فایل امضا قابل اعتماد نیست
- امضا اعتبار ندارد.

امضا معتبر است

درصورتی که نتیجه ارزیابی فایل امضا مورد تایید باشد پیغام "کلیه امضا ها معتبر بود" نمایش داده می شود و فایل اصلی نیز جهت رویت، اجرا می گردد.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

فایل امضا قابل اعتماد نیست

درصورتی که امکان ارتباط با مرکز اعتبار سنجی گواهی های امضا برقرار نباشد پیغام " امکان اعتبارسنجی کامل وجود ندارد. به این فایل نمی توان اعتماد کرد" نمایش داده می شود.



امضا اعتبار ندارد

درصورتی که نتیجه ارزیابی فایل امضا مورد تایید نباشد پیغام "یک یا چند امضا اعتبار ندارد" نمایش داده می شود .



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

دلایل نامعتبر بودن امضا شامل یکی از موارد زیر است :

- زنجیره گواهی امضا نامعتبر است.
- گواهی امضا منقضی است.
- گواهی امضا باطل است.
- محتوای فایل امضا نامعتبر است.

در یک نگاه کلی:

نمایش علامت تیک **سبز** رنگ به معنی معتبر بودن امضا و قابل استناد بودن فایل امضا شده است.

نمایش علامت تعجب **زرد** رنگ به معنی عدم برآورده شدن الزامات استناد پذیری فایل امضا شده است

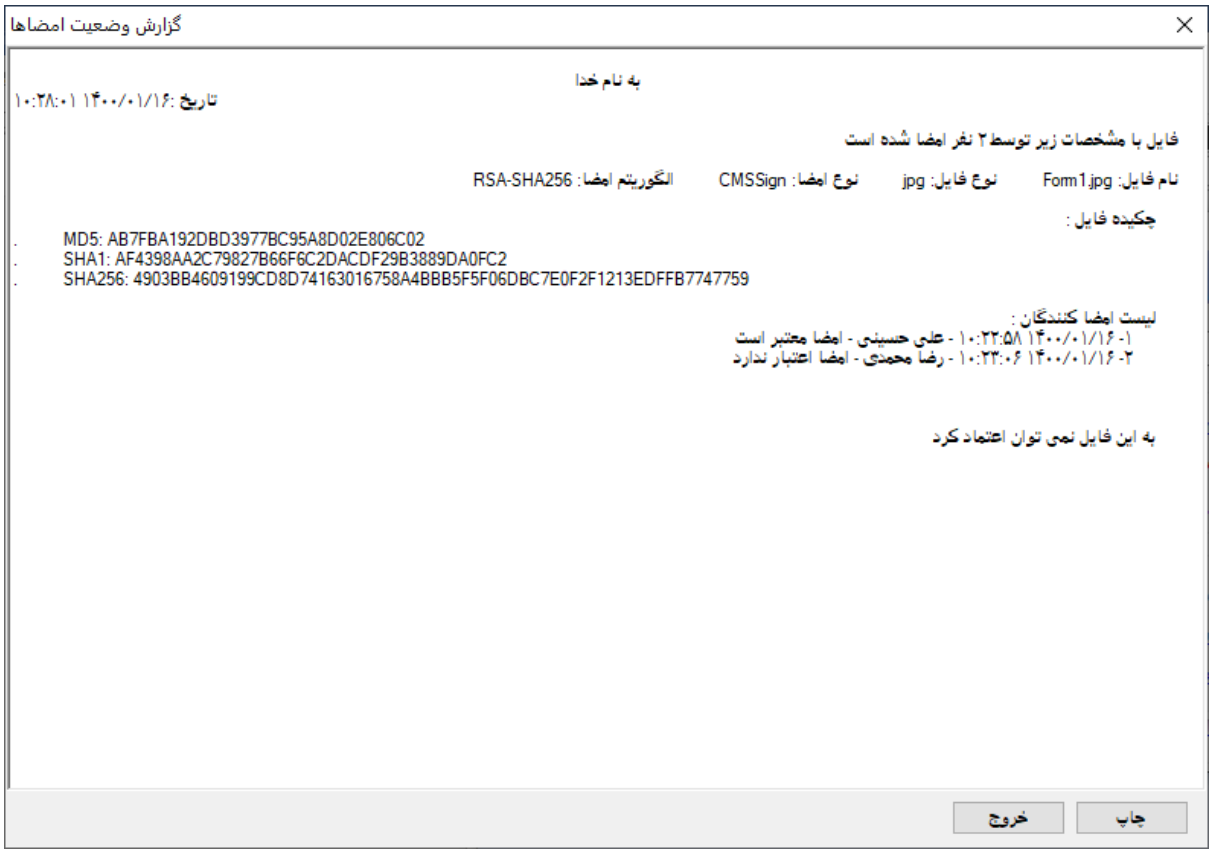
نمایش علامت ضربدر **قرمز** رنگ به معنی نامعتبر بودن امضا و غیرقابل استناد بودن فایل امضا شده است.

توجه:

در فرآیند بررسی امضا، علاوه بر گزارش نتیجه نهایی و تعداد امضاکنندگان فایل، یکسری اطلاعات تکمیلی نیز در ارتباط با فایل امضا شده نمایش داده می شود که با کلیک برروی گزینه "گزارش تفصیلی" می توانید این اطلاعات را مشاهده نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.



اطلاعات آورده شده در بخش گزارش تفصیلی، به شرح زیر می باشد:

- **تاریخ و زمان ارزیابی امضا**
- **تعداد امضای های فایل انتخاب شده**
- **نام و نوع فایل**

(نام و پسوند فایل امضا شده را مشخص می نمایید)

- **نوع امضا و الگوریتم امضا**

(قالب امضا و الگوریتم استفاده شده برای امضای فایل را مشخص می کند)

- **چکیده فایل**
- **لیست امضا کنندگان**

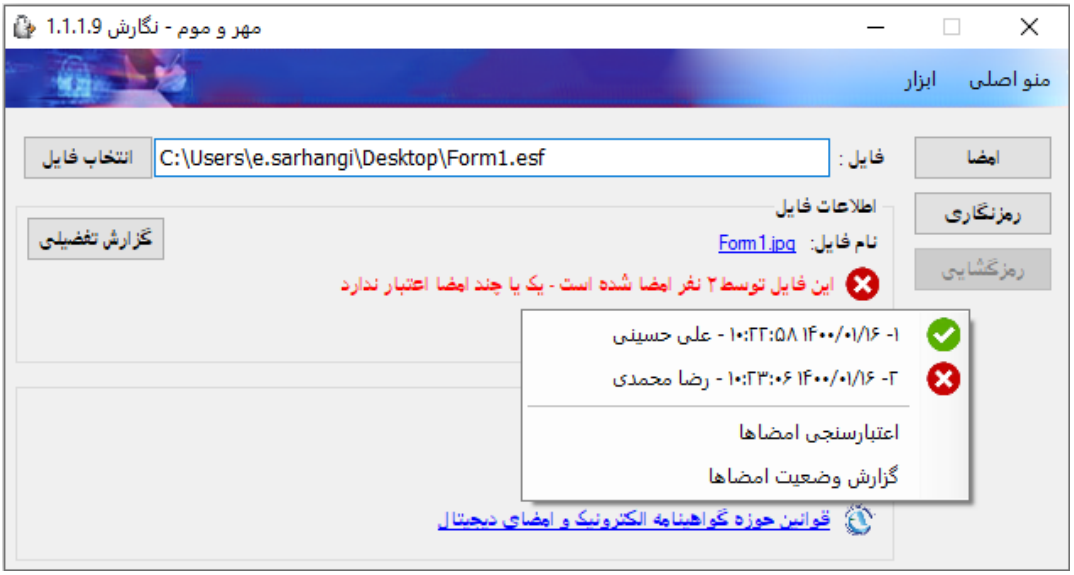
(نام امضا کنندگان، تاریخ و زمان امضا و نتیجه ارزیابی به ازای هر امضا را مشخص می کند)

- **نتیجه نهایی ارزیابی امضا**

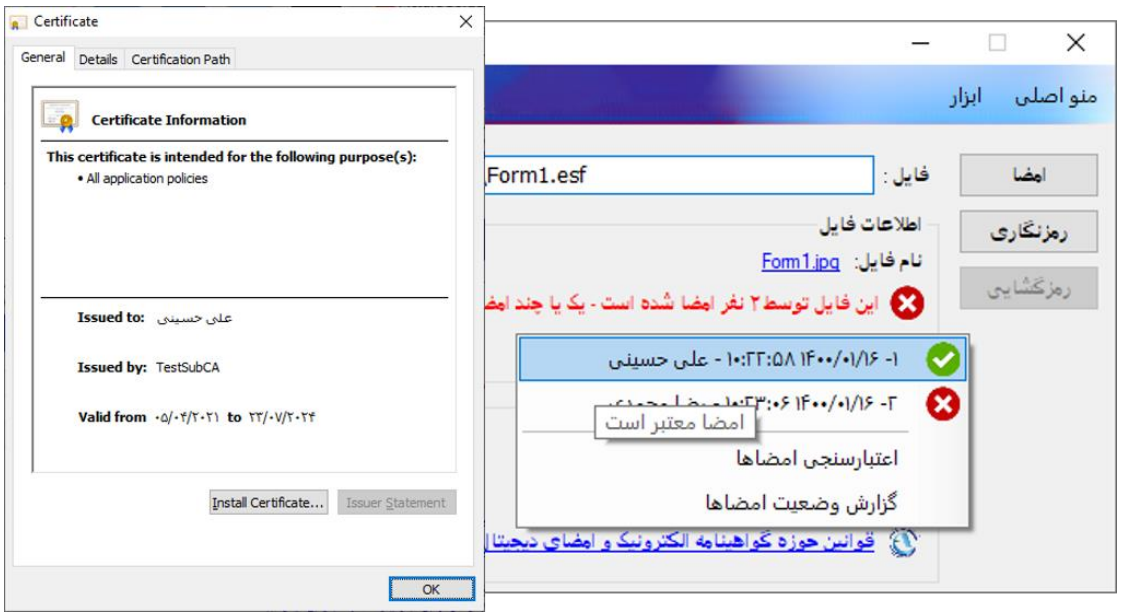
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

بیشتر بدانیم:

توجه شود که در پایان فرآیند ارزیابی امضا، می توانید با راست کلیک برروی نتیجه گزارش شده، مشخصات فرد/افراد امضا کننده را دریافت نمایید و درصورت لزوم با کلیک برروی گزینه "اعتبارسنجی امضاها"، مجددا فایل امضا را ارزیابی کنید. همچنین می توانید با انتخاب گزینه "گزارش وضعیت امضاها"، اطلاعات تکمیلی مرتبط با فایل امضا شده را دریافت نمایید.



شایان ذکر است که درصورت نیاز به مشاهده گواهی امضا، کافی است در پنجره نمایان شده برروی نام امضا کننده موردنظر کلیک نمایید تا گواهی صاحب امضا نمایش داده شود.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۴,۳ رمزنگاری فایل

یک فرد می تواند با دو هدف برای رمزنگاری اطلاعات موردنظر اقدام نماید :

- رمزنگاری اسناد و فایل های موردنظر جهت حفظ محرمانگی آن ها هنگام ارسال اطلاعات برای فرد گیرنده

(در این حالت شخص رمزکننده باید گواهیی را برای رمزنگاری انتخاب نماید که گیرنده فایل رمز آن گواهی و کلید خصوصی متناظر با آن را در اختیار قرار دارد و می تواند از طریق آن ها برای رمزگشایی فایل اقدام نماید)

- رمزنگاری اسناد و فایل های موردنظر جهت حفظ محرمانگی آن ها در طول دوره بایگانی و نگهداری اطلاعات

(در این حالت شخص رمز کننده باید علاوه بر گواهی رمزنگاری، کلید خصوصی متناظر با آن را نیز در اختیار داشته باشد تا درصورت نیاز بتواند اسناد و فایل های رمزشده را رمزگشایی نماید.)

به منظور دستیابی به اهداف گفته شده می بایست با مراجعه به توضیحات "پیوست پ" محصول را به نسخه پیشرفته ارتقا دهید و سپس مطابق با روال زیر اقدام کنید:

۱. برنامه مهر و موم را اجرا نموده و با کلیک برروی گزینه "انتخاب فایل" فایل موردنظر را برای رمزنگاری انتخاب کنید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۲. پس از انتخاب فایل موردنظر، برروی گزینه "رمزنگاری" کلیک نمایید.



۳. باتوجه به هدف فرد از رمزنگاری اطلاعات، ۳ امکان برای انتخاب گواهی رمزنگاری در برنامه مهر و موم تعریف شده است که در ادامه کاربرد هر امکان به تفصیل شرح داده می شود.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

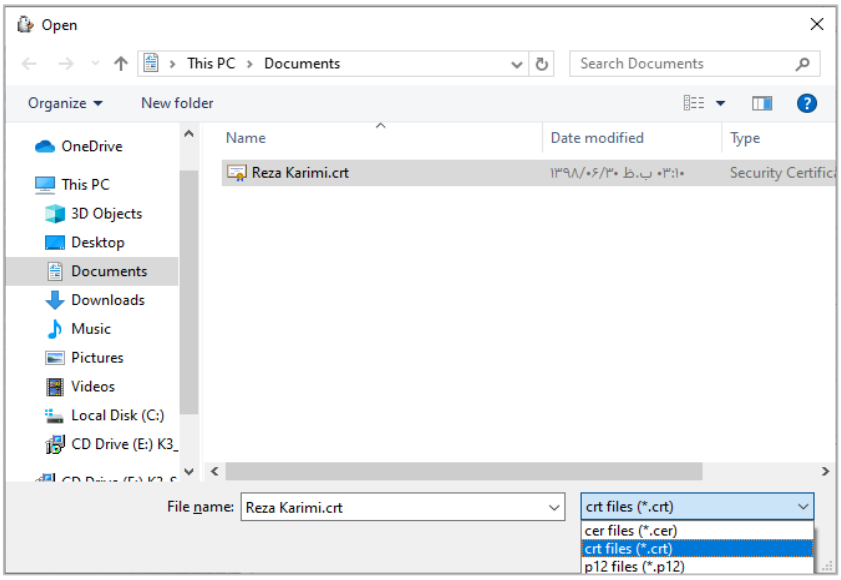
۳/۱ رمزنگاری اسناد و فایل های موردنظر برای شخص گیرنده

درصورتی قصد دارید فایل موردنظر را برای شخص خاصی رمز و ارسال نماید در قدم اول باید گواهی شخص گیرنده را که دارای پسوند cer یا crt می باشد دریافت کنید و سپس طبق روال زیر اقدام نمایید:

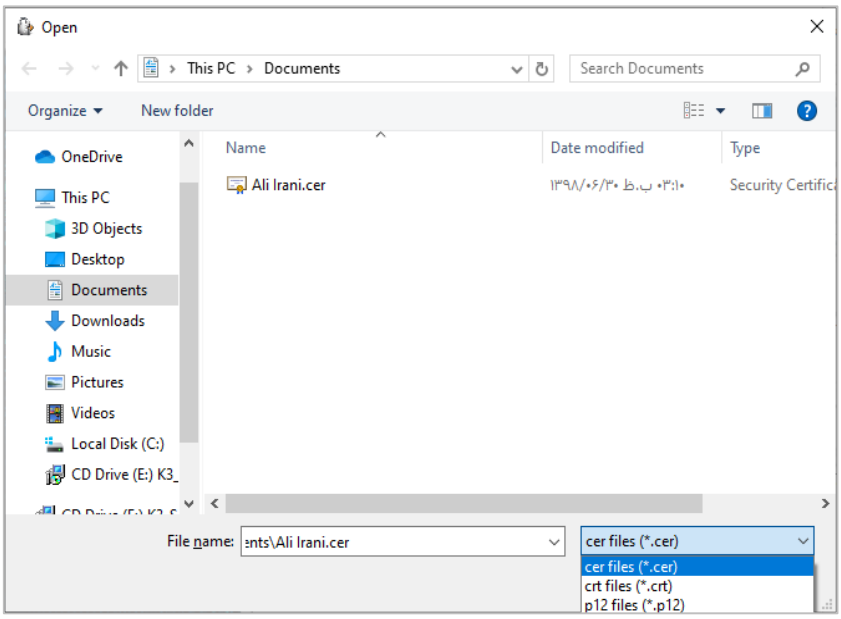
۱. در پنجره رمزنگاری اطلاعات برروی گزینه "انتخاب از فایل" کلیک نمایید.



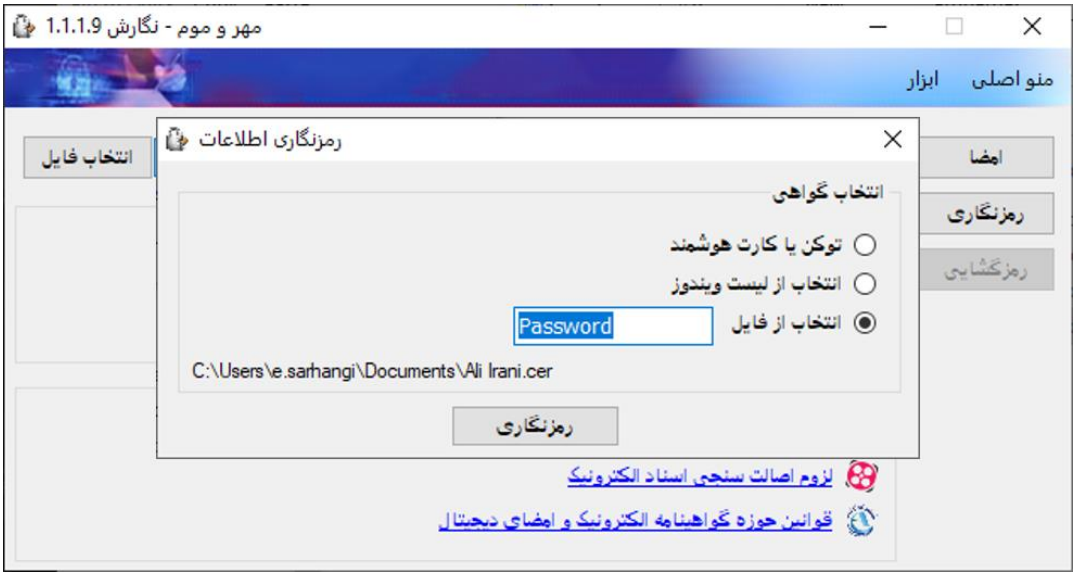
۲. سپس در پنجره نمایش داده شده، گواهی گیرنده را که دارای پسوند cer یا crt می باشد انتخاب کنید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.



۳. پس از انتخاب گواهی شخص گیرنده، روی گزینه "رمزنگاری" کلیک نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳/۲ رمزنگاری اسناد و فایل های موردنظر جهت بایگانی و نگهداری

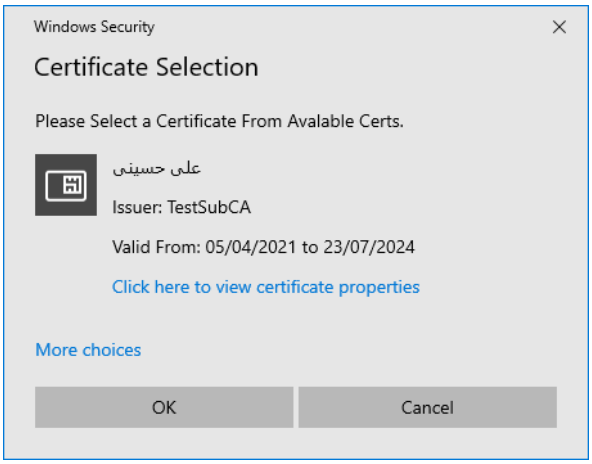
به منظور رمزنگاری اسناد و فایل های موردنظر در صورتی که فایل cer یا crt گواهی رمزنگاری را در اختیار دارید طبق توضیحات قبلی با استفاده از گزینه "انتخاب از فایل" فایل گواهی را انتخاب نموده و روی گزینه "رمزنگاری" کلیک کنید. و درصورتی که فایل cer یا crt گواهی را دراختیار ندارید می بایست مطابق با توکنی که برای رمزنگاری در اختیار دارید یکی از گزینه های موجود در پنجره رمزنگاری اطلاعات را انتخاب نمایید.

۳/۲/۱ استفاده از توکن سخت افزاری

اگر گواهی موردنظر برروی توکن سخت افزاری قراردارد، ابتدا توکن را به سیستم متصل نمایید و سپس در قسمت رمزنگاری اطلاعات ، گزینه "توکن یا کارت هوشمند" را انتخاب کرده و برروی گزینه "رمزنگاری" کلیک کنید.



سپس در پنجره نمایان شده گواهی موردنظر برای رمزنگاری را انتخاب کنید.

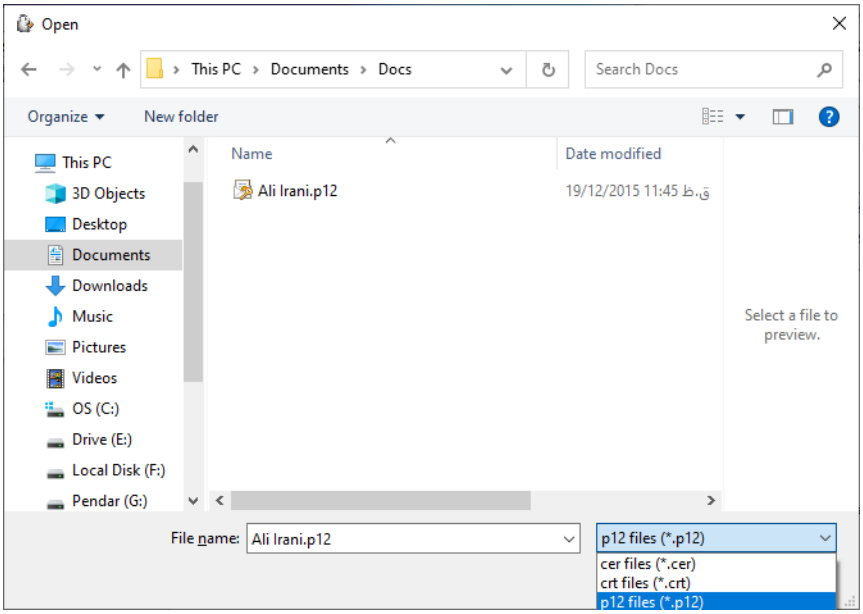


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳/۲/۲ استفاده از توکن نرم افزاری

درصورتی که گواهی موردنظر برای رمزنگاری، برروی توکن نرم افزاری قراردارد می بایست در قسمت رمزنگاری اطلاعات، برروی گزینه "انتخاب از فایل" کلیک کرده و در پنجره نمایان شده توکن نرم افزاری خود را انتخاب نمایید.





تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

سپس رمز توکن نرم افزاری را در قسمت "Password" وارد نموده و برروی گزینه "رمزنگاری" کلیک کنید.

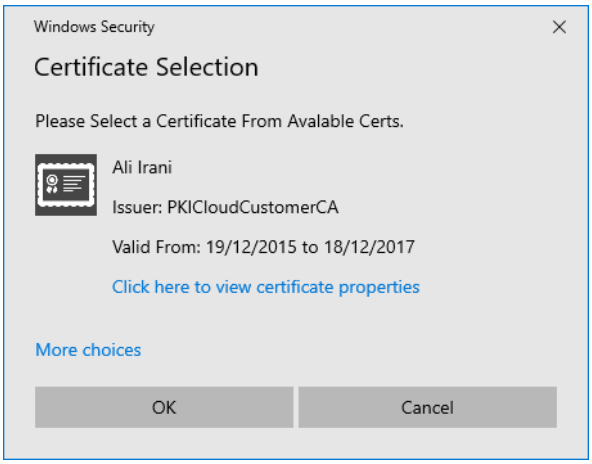


درنظر داشته باشید درصورتی که توکن نرم افزاری را قبلا در مخزن کلید ویندوز وارد نموده اید می توانید برروی گزینه "انتخاب از لیست ویندوز" کلیک کنید و سپس گزینه "رمزنگاری" را انتخاب نمایید تا گواهی مورد نظر برای رمزنگاری را در پنجره نمایان شده مشاهده کنید.

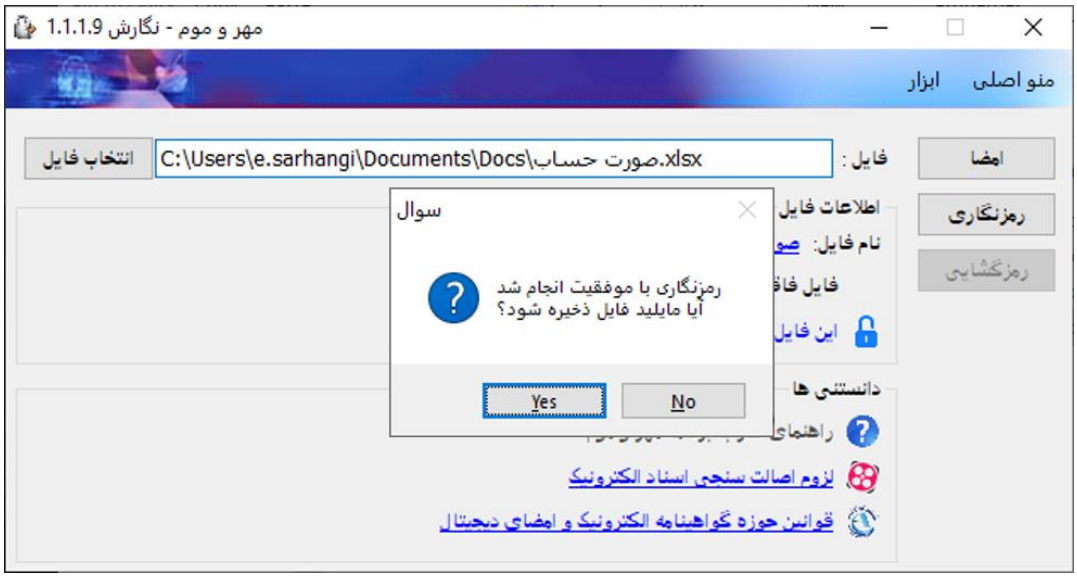


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

با مشاهده گواهی موردنظر برای رمزنگاری، آن را انتخاب نمایید

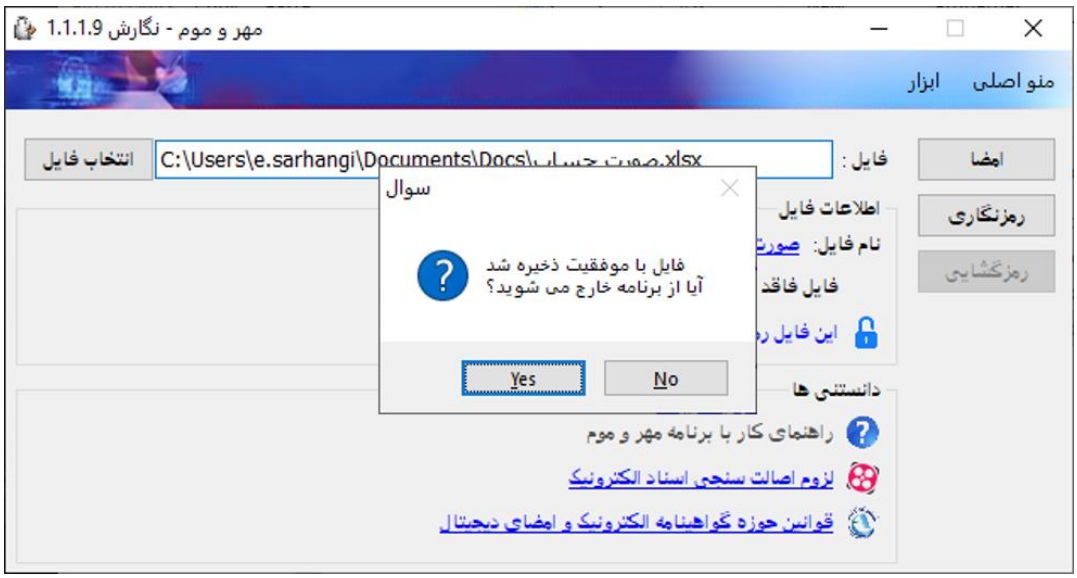


۴. پس از انتخاب گواهی رمزنگاری به یکی از سه روش گفته شده، و انتخاب گزینه "رمزنگاری" فرآیند آغاز شده و درصورت موفقیت آمیز بودن نتیجه، پنجره زیر نمایان می شود. با کلیک برروی گزینه "Yes" یک فایل با پسوند esf به عنوان فایل رمزشده در مسیر فایل اصلی ذخیره می گردد.



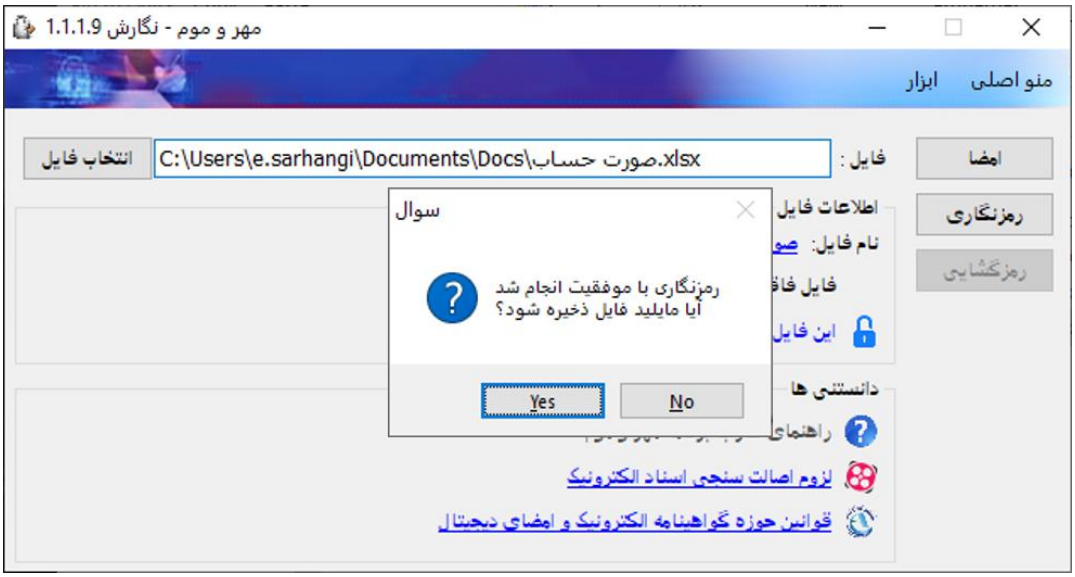
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۵. اکنون عملیات مورد نظر به اتمام رسیده است. با کلیک برروی گزینه "Yes" از برنامه خارج شوید.



نکته:

درصورتی که تمایل دارید فایل رمزشده را در مسیری مجزا از مسیر فایل اصلی ذخیره نمایید، کافی است در مرحله ذخیره سازی فایل رمز (**مرحله ۴**)، در پیام نمایان شده گزینه "No" را انتخاب کنید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

سپس با کلیک برروی گزینه "ذخیره" می توانید فایل رمز را در مسیر موردنظر ذخیره نمایید.



شایان ذکر است که فایل رمز تولید شده در فرمت esf، تنها از طریق برنامه مهر و موم قابل رمزگشایی می باشد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۴,۴ رمزگشایی فایل

به منظور رمزگشایی فایل esf، ابتدا برنامه مهر و موم را اجرا نموده و سپس مطابق با مراحل زیر اقدام نمایید: برای انجام این عملیات دسترسی به کلید خصوصی و گواهی موردنیاز برای رمزگشایی الزامی است

۱. درصورتی که گواهی موردنظر بروی ماژول رمزنگاری قرار دارد، ماژول را به سیستم متصل نمایید و درصورت استفاده از توکن نرم افزاری ابتدا آن را مطابق با توضیحات "پیوست الف" در مخزن کلید ویندوز وارد کنید و در نهایت با کلیک برروی گزینه انتخاب فایل، فایل رمزشده به فرمت esf را انتخاب نمایید.

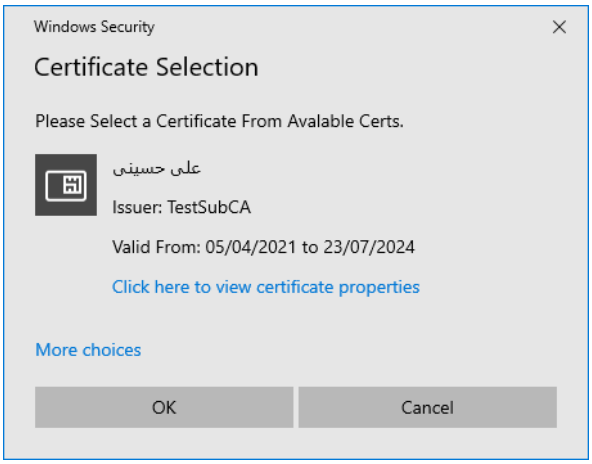


۲. پس از انتخاب فایل esf برروی گزینه "رمزگشایی" کلیک نمایید.

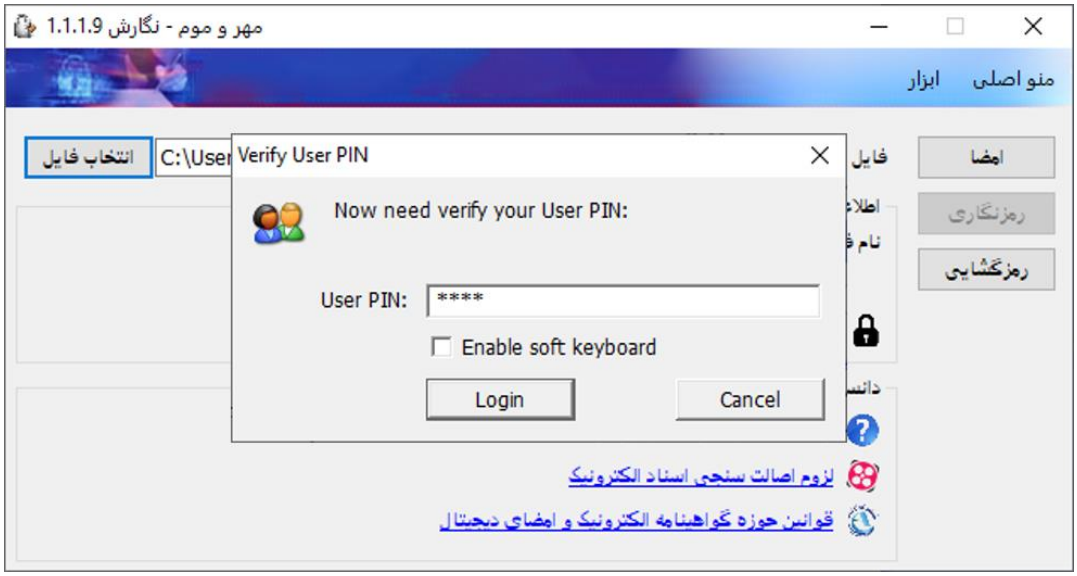


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳. در پنجره نمایان شده گواهی موردنیاز برای رمزگشایی را انتخاب نمایید.

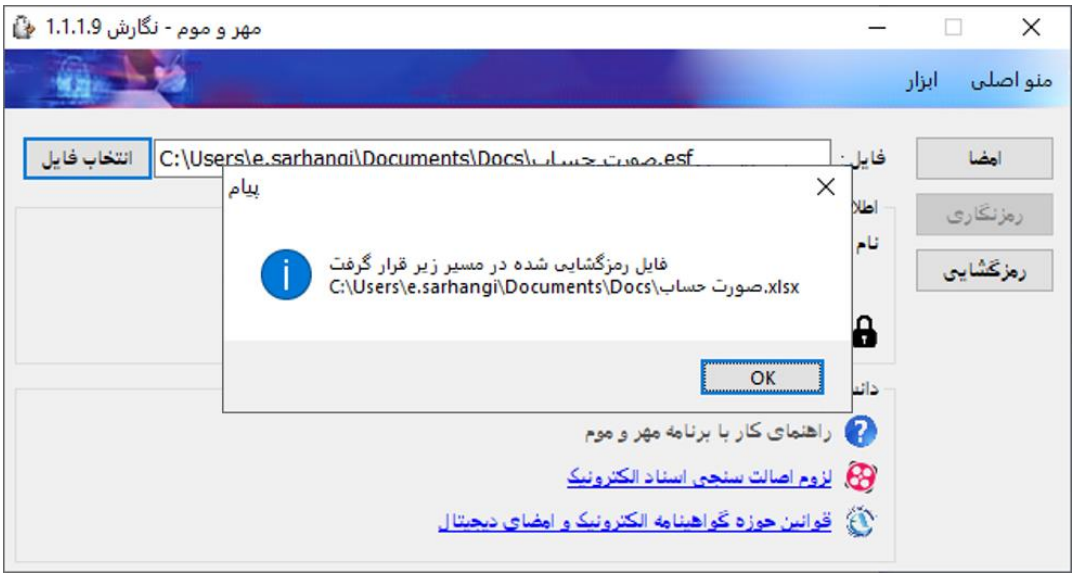


۴. درصورت استفاده از ماژول رمزنگاری پین توکن را وارد کنید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۵. با اتمام موفقیت آمیز فرآیند رمزگشایی، فایل اصلی در مسیر نمایش داده شده ذخیره خواهد شد.



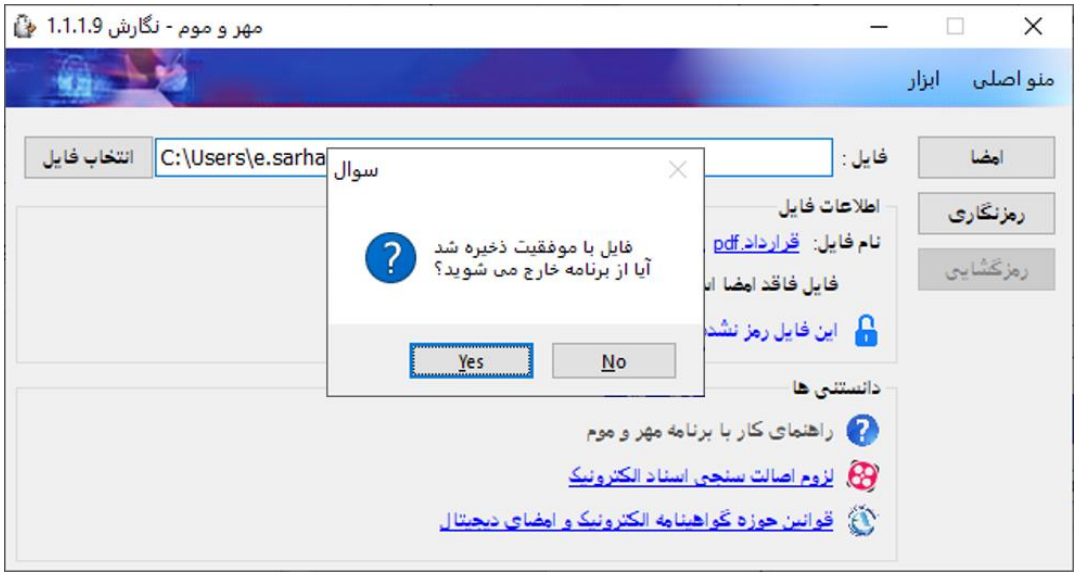
۶. با کلیک برروی گزینه "ok" فایل اصلی جهت رویت، اجرا خواهد شد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۵ امضا و رمزنگاری

درصورتی که نیاز است فایل امضا شده جهت حفظ محرمانگی اطلاعات، رمز هم شود، می بایست مطابق با روال زیر اقدام نمایید:

۱. در قدم اول باتوجه به توضیحات بند ۴,۱ با کلیک برروی گزینه "امضا"، فایل موردنظر را توسط شخص یا اشخاص موردتایید امضا نمایید و در پایان برروی گزینه "No" کلیک کنید.

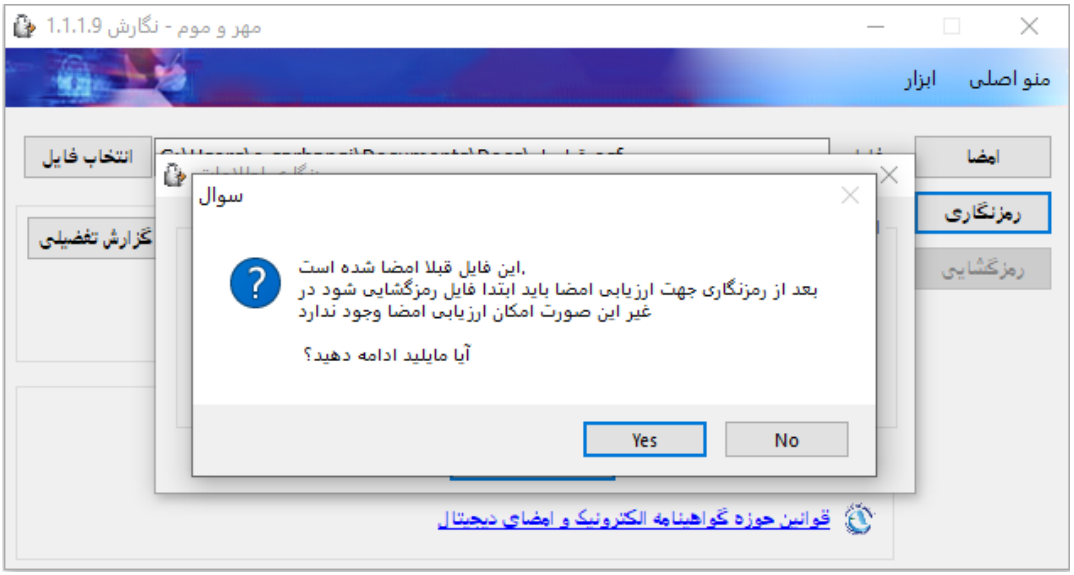


۲. اکنون می توانید مطابق توضیحات بند ۴,۳ با کلیک برروی گزینه "رمزنگاری"، فایل امضا شده به فرمت esf را رمز نمایید.

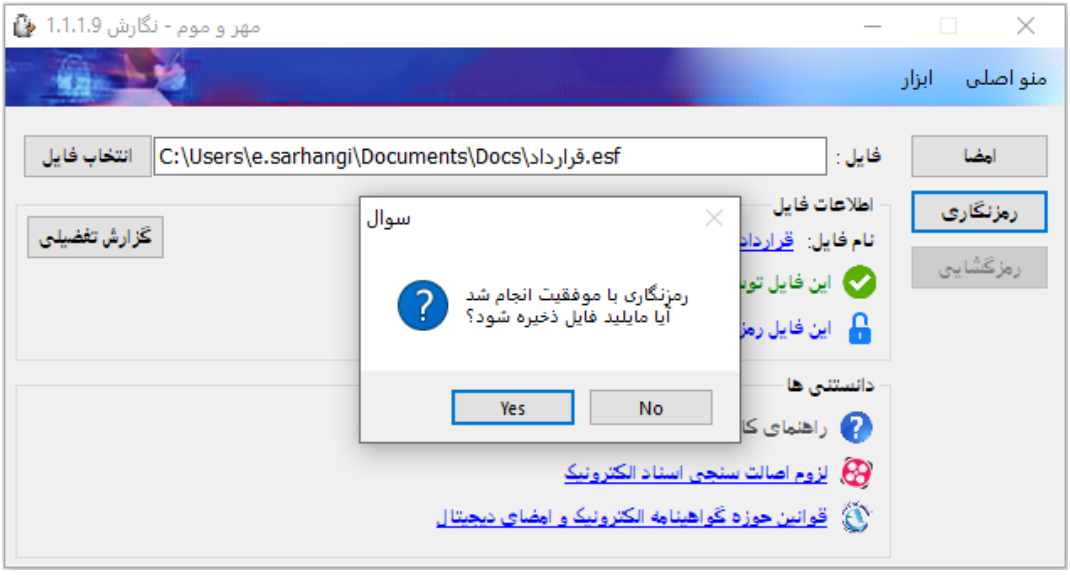


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳. درنظر داشته باشید که جهت ارزیابی امضای یک فایل امضا شده و رمزشده، ابتدا باید مطابق با توضیحات بند ۴,۷برای رمزگشایی فایل اقدام شود و سپس ارزیابی امضا صورت گیرد. بنابراین در پیام نمایش داده شده برروی گزینه "yes" کلیک نمایید تا فرآیند رمزنگاری ادامه یابد.

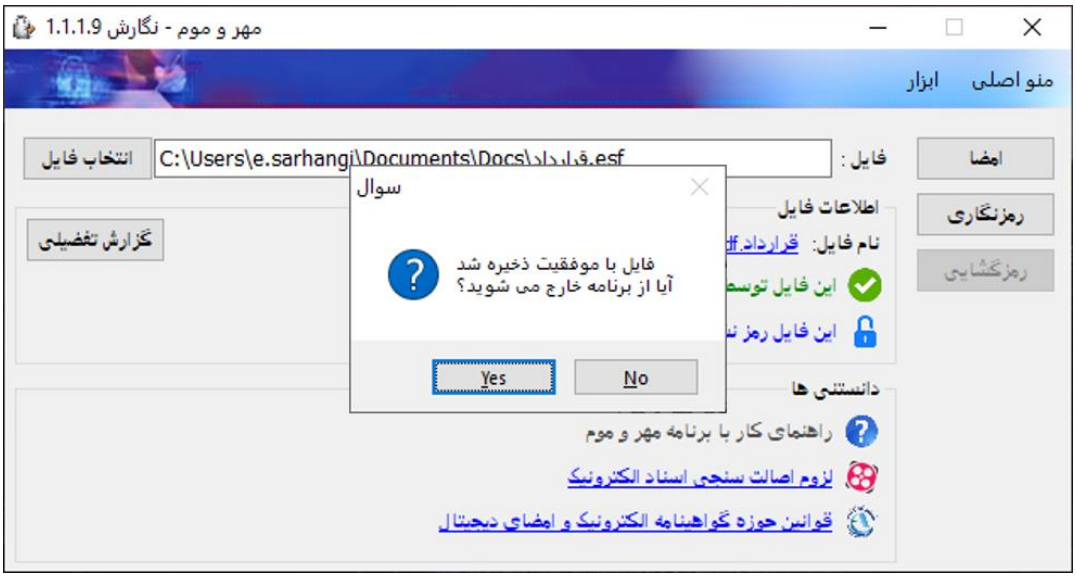


۴. همان طور که پیش تر نیز اشاره شد با اتمام موفقیت آمیز فرآیند رمزنگاری پیغام زیر نمایش داده می شود. با کلیک برروی گزینه "yes" یک فایل با فرمت esf به عنوان فایل امضا شده و رمز شده تولید و در مسیر فایل اصلی ذخیره خواهد شد.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۵. اکنون می توانید با کلیک برروی گزینه "yes" از برنامه خارج شوید. تصویر اصلاح شود ن نمایش داده نشود



نکته:

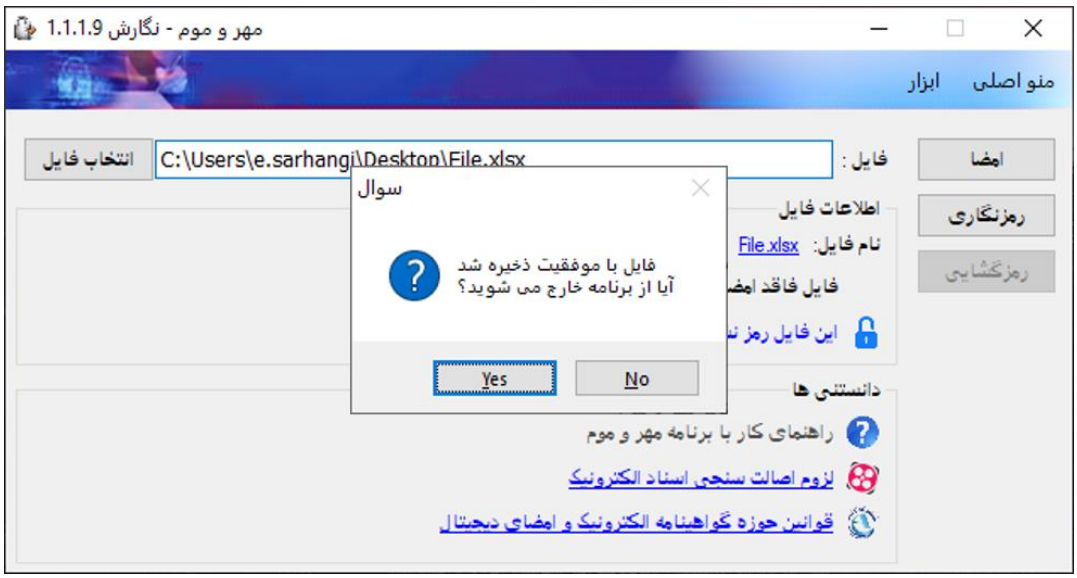
توجه داشته باشید که یک فایل امضا شده به فرمت esf را پس از رمزنگاری نمی توان مجدد امضا نمود. بنابراین ابتدا باید فایل موردنظر را به دفعات موردنیاز امضا نمایید و سپس برای رمزنگاری فایل امضا شده اقدام کنید.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۶ رمزنگاری و امضا

در شرایطی که نیاز است سند یا فایل موردنظر ابتدا رمز و سپس امضا شود می بایست طبق روال زیر اقدام نمایید:

۱. در قدم اول مطابق با توضیحات بند ۴,۳ برای رمزنگاری فایل موردنظر اقدام نمایید و در پایان برروی گزینه "No" کلیک کنید .

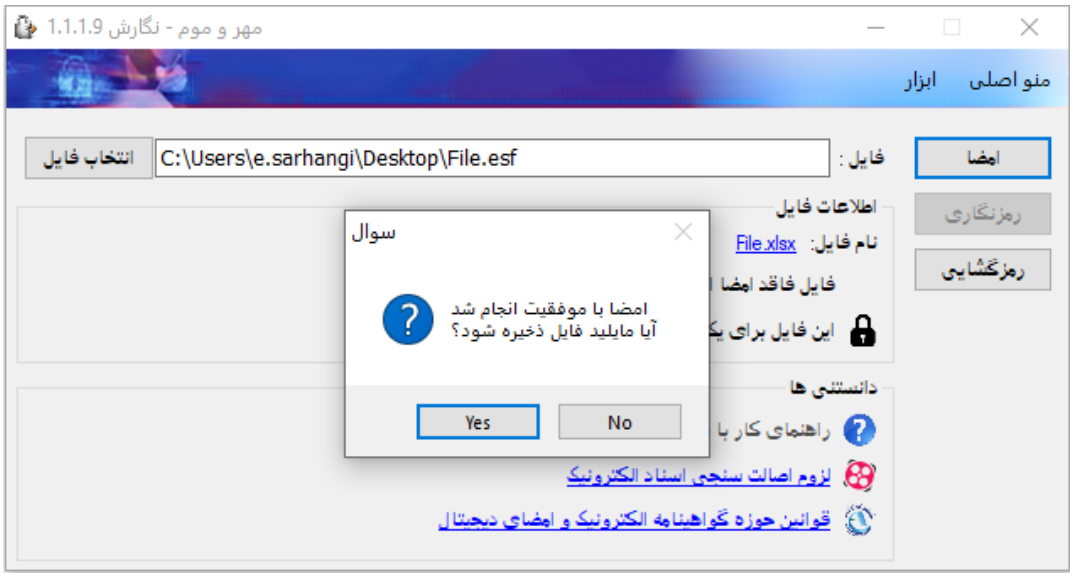


۲. در این مرحله می توانید مطابق با توضیحات بند ۴,۱ با کلیک برروی گزینه "امضا"، جهت امضای فایل رمزشده اقدام نمایید.

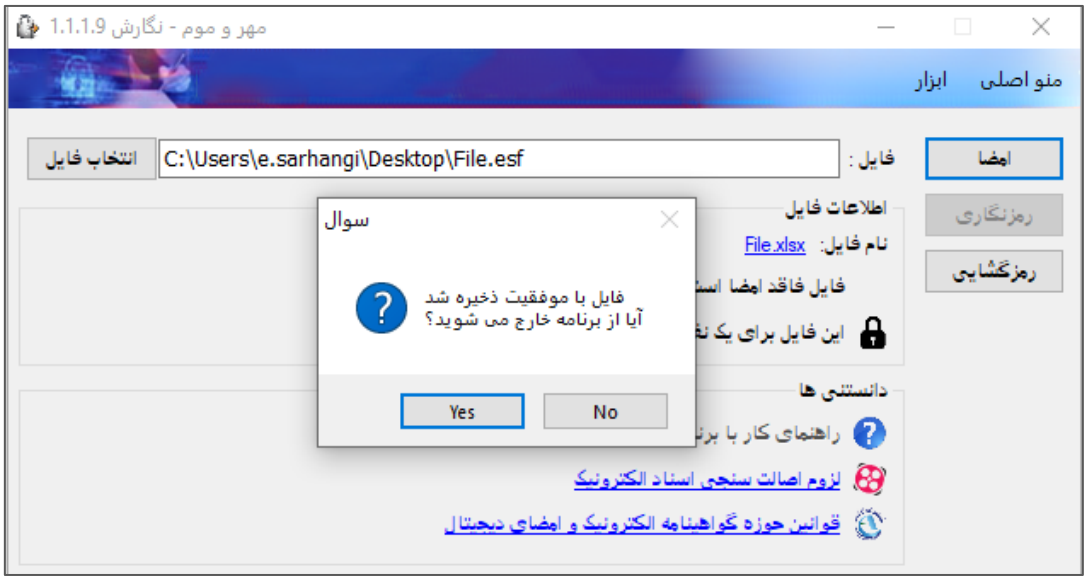


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۳. همان طور که قبلا اشاره شد با اتمام موفقیت آمیز فرآیند امضا، پیغام زیر نمایش داده می شود. با کلیک برروی گزینه "yes" یک فایل با فرمت esf به عنوان فایل رمز شده و امضا شده تولید و در مسیر فایل اصلی ذخیره خواهد شد.



۴. درصورتی که عملیات موردنظر به اتمام رسیده است می توانید با کلیک برروی گزینه "yes" از برنامه خارج شوید.



توجه:

درصورت استفاده از این روش به راحتی و بدون نیاز به رمزگشایی فایل، می توان امضای فایل esf رمزشده و امضا شده را مطابق توضیحات بند ۴,۲ ارزیابی نمایید.

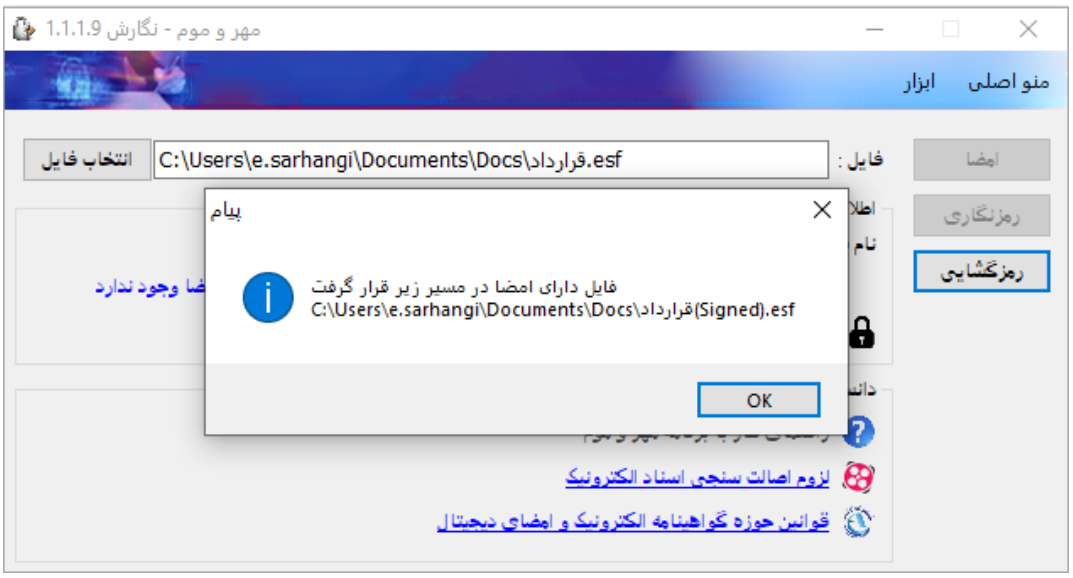
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۷ رمزگشایی و بررسی امضا

همان طور که پیش‌تر اشاره شد امکان ارزیابی امضای، یک فایل امضا شده و رمز شده پیش از رمزگشایی آن وجود ندارد. بنابراین ابتدا باید طبق روال گفته شده در بند ۴،۴، با کلیک برروی گزینه "رمزگشایی"، فایل را رمزگشایی نمایید.

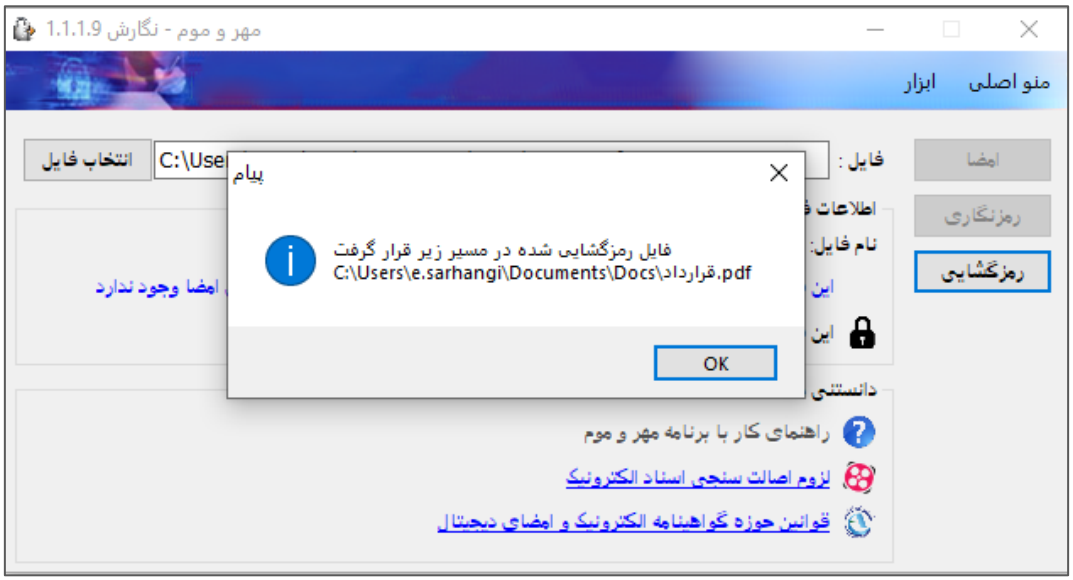


۵. با اتمام موفقیت آمیز فرآیند رمزگشایی، یک فایل با فرمت esf به عنوان فایل امضا در مسیر نمایش داده شده ذخیره می شود. بنابراین در پیام نمایان شده برروی گزینه "ok" کلیک نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۶. پس از ذخیره سازی فایل امضا، فایل اصلی نیز در مسیر نمایش داده شده ذخیره می شود. که با کلیک برروی گزینه "ok" فایل اصلی جهت رویت اجرا خواهد شد.



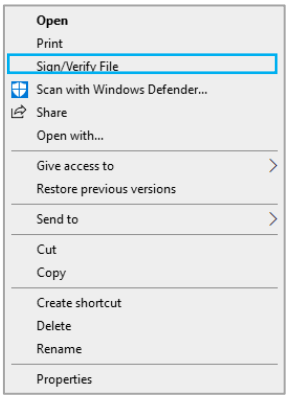
۷. اکنون می توانید با انتخاب فایل امضای تولید شده در مرحله ۶، جهت ارزیابی امضا، مطابق با توضیحات بند ۴,۲ اقدام نمایید.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۸ نکات پایانی

پس از اولین بار اجرا نمودن برنامه مهر و موم با راست کلیک بروی فایل های موجود در سیستم، مشاهده خواهید نمود که گزینه Sign/verify File در منوی ظاهر شده اضافه شده است تا درصورت نیاز به انجام هریک از فرآیند های امضای دیجیتال ،بررسی امضا و رمزنگاری ضرورتی بر اجرای برنامه و انتخاب فایل از داخل آن نباشد بنابراین تنها کافی است بروی فایل موردنظر راست کلیک کنید و از روش میان بر Sign/Verify File استفاده نمایید.



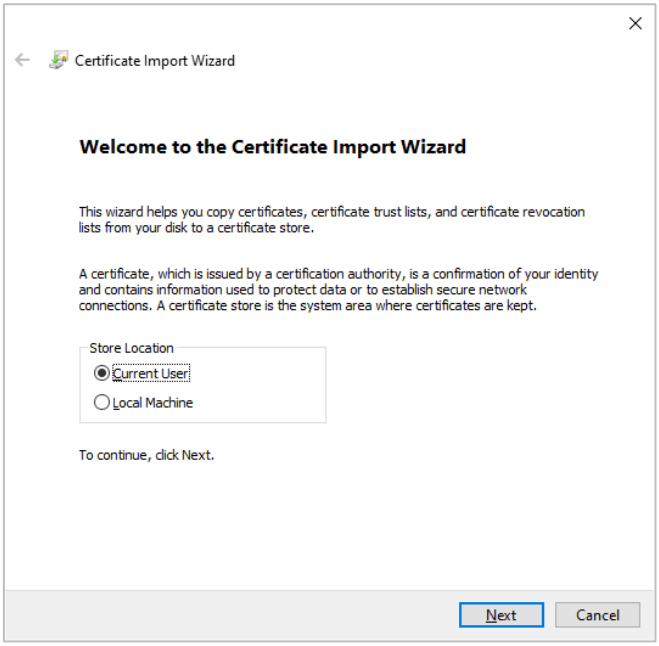
توجه:

لازم به ذکر است که درصورت نیاز برای بررسی امضا و یا رمزگشایی فایل های esf، می توانید به راحتی با ۲ بار کلیک کردن برروی فایل موردنظر، آن را در برنامه مهر و موم اجرا نمایید.

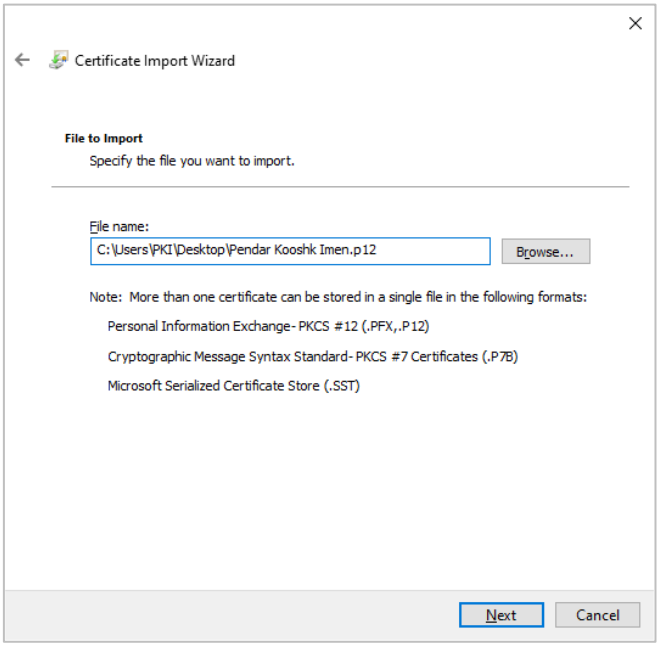
تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۹ پیوست الف

در این بخش نحوه وارد نمودن فایل p12 در مخزن کلید ویندوز شرح داده شده است تا درصورت نیاز بتوانید از توکن نرم افزاری خود جهت امضا و رمز نمودن اسناد و فایل های موردنظر استفاده نمایید. برای این منظور پس از اجرا نمودن فایل p12 می بایست در پنجره نمایش داده شده پس از انتخاب گزینه "Current User" روی گزینه "Next" کلیک کنید.

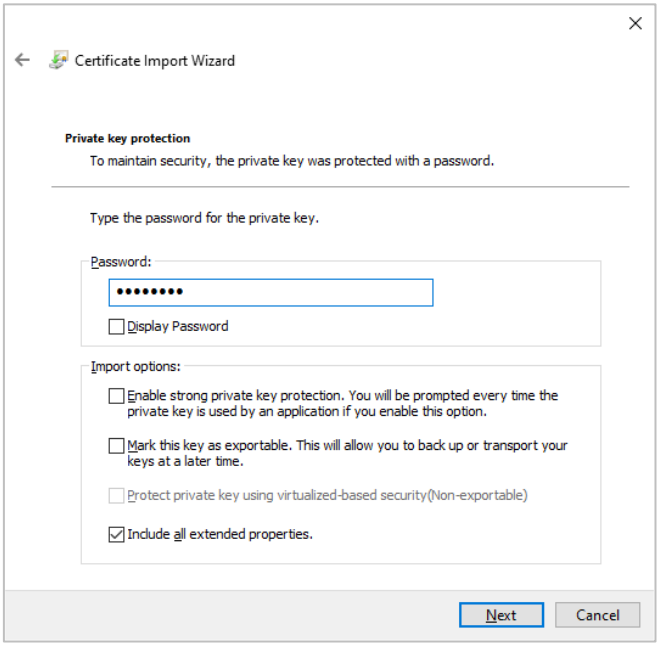


در این پنجره مجدد روی گزینه "Next" کلیک نمایید.

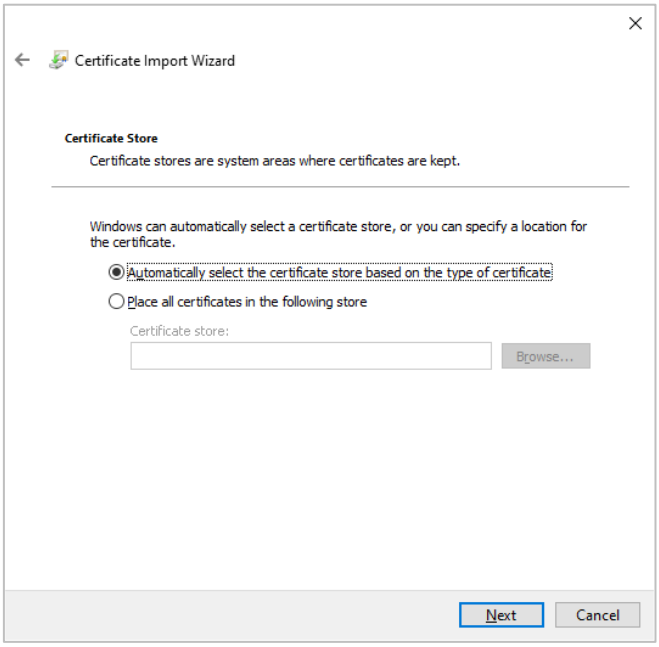


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

پس از وارد نمودن رمز فایل p12، گزینه "Next" را انتخاب کنید.

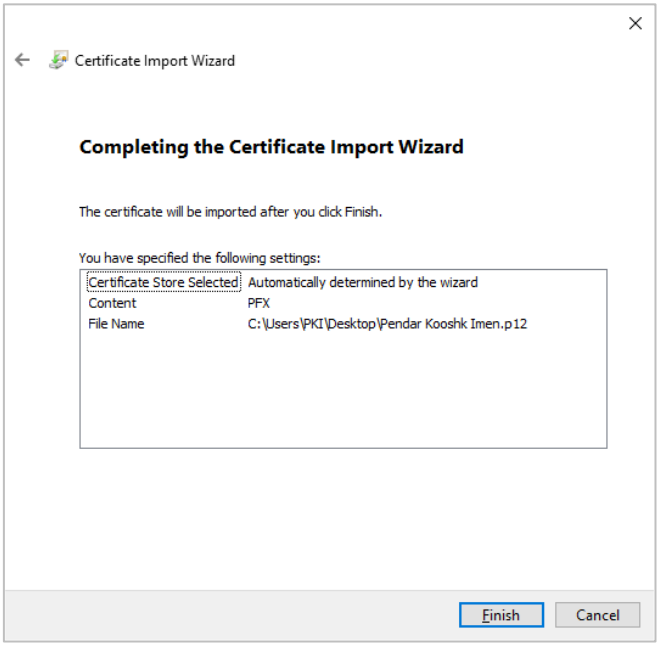


در این پنجره نیز روی گزینه"Next" کلیک نمایید.

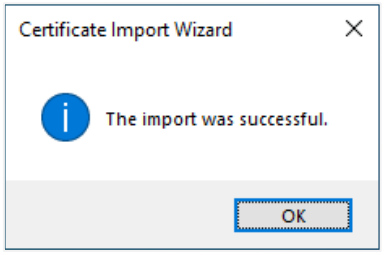


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

سپس گزینه "Finish" را انتخاب کنید.



با قرارگیری موفقیت آمیز گواهی در مخزن کلید ویندوز پیغام "The import was successful" نمایش داده می شود.

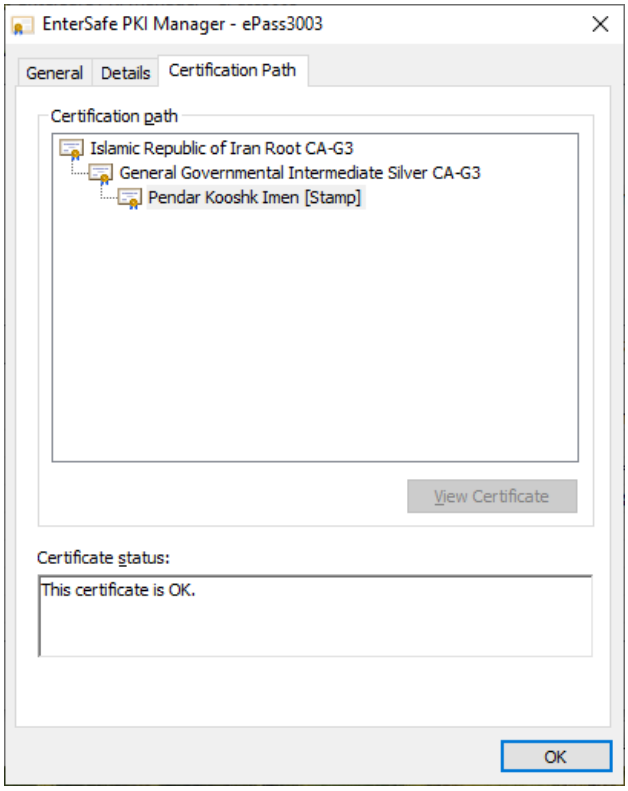


تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۱۰ پیوست ب

همان طور که پیش‌تر اشاره شد گواهی نامه دیجیتال توسط مراکز صدور گواهینامه، صادر می شوند و هنگام اعتبار سنجی یک گواهی باید از مورد اعتماد بودن صادر کننده آن اطمینان پیدا نمود که برای این منظور می توان به سربرگ Certification Path گواهی مراجعه نمود.

در تصویر زیر مشاهده می کنید که گواهی نامه پندار کوشک ایمن توسط مرکز صدور گواهی میانی عام که تحت مرکز صدور گواهی ریشه فعالیت می کند و یک مرکز صدور مورد اطمینان محسوب می شود، صادر شده است بنابراین از لحاظ صادر کننده گواهی می توان به گواهی پندار کوشک ایمن اعتماد نمود.



تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

۱۱ پیوست پ

همانطور که پیش تر اشاره شد به منظور استفاده از قابلیت رمزنگاری و رمزگشایی برنامه مهر و موم می بایست محصول را به نسخه پیشرفته ارتقا دهید که برای این منظور می بایست از قسمت منوی اصلی برروی گزینه "ارتقا برنامه" کلیک نمایید.



در پنجره نمایان شده اطلاعات موردنیاز را وارد کرده و برروی گزینه "فعال سازی" کلیک نمایید.



درصورت موفقیت آمیز بودن فرایند فعال سازی، پیغام زیر نمایش داده می شود. برروی گزینه "ok" کلیک کنید.



توجه:

جهت دریافت کد فعال سازی می تواند به وب سایت شرکت پندار کوشک ایمن مراجعه کنید و یا با واحد پشتیبانی فروش شرکت تماس حاصل نمایید.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن می‌باشد.