راهنمای کامل استفاده و پشتیبانی از

توکن iPass

نصب، استفاده، مدیریت PIN، گواهی، امضای دیجیتال و عیب‌یابی

شرکت منشور سیمین

نسخه ۰.۶ -مرداد ۱۴۰۵

فهرست مطالب

توجه :این راهنما با فرض انتخاب زبان فارسی در Installerو برنامه‌های iPassنوشته شده است .نام انگلیسی گزینه‌ها فقط جایی آمده که در ابزارهای فنی یا Windowsاستفاده می‌شود.

۱ .معرفی محصول و دامنه راهنما

۱-۱ .معرفی محصول

توکن iPass یک ابزار سخت‌افزاری برای نگهداری امن کلید خصوصی و انجام امضای دیجیتال است .کلید خصوصی داخل توکن تولید و نگهداری می‌شود و خروجی‌گیری عادی از آن امکان‌پذیر نیست Windows سخت‌افزار را به‌صورت USB HID شناسایی می‌کند؛ با این حال برای استفاده از گواهی، امضای دیجیتال و نرم‌افزارهای سازمانی باید بسته iPass Token Installer نصب شود.

دامنه این راهنما :این سند بر نصب، استفاده روزمره، مدیریت PIN، مشاهده و مدیریت گواهی، امضای دیجیتال، ابزارهای بررسی سلامت و عیب‌یابی تمرکز دارد.

۱-۲ .مشخصات فنی و قابلیت‌های پشتیبانی‌شده

Details	Technical Specification
iPass Digital Signature Token	Product Name
Manshoor-e Simin Co.	Manufacturer
Windows 10 / Windows 11 (x86 and x64)	Supported Operating Systems
• PKCS#11 • Microsoft CryptoAPI (CSP) • Microsoft CNG (KSP)	Cryptographic Interfaces
• RSA-1024 / RSA-2048 • SHA-1 / SHA-256 / SHA-384 / SHA-512 • MD5 (Legacy compatibility only)	Supported Cryptographic Algorithms
• Raw RSA Sign / Verify • RSA PKCS#1 v1.5 Sign / Verify with SHA-1 and SHA-256 • CMS / PKCS#7 Signature with SHA-1 and SHA-256 • With and without CMS Signed Attributes	Validated Signature Operations

۱-۳ .اجزای نرم‌افزاری محصول

جزء	نقش
iPass Token Manager	مدیریت توکن، PINها، کلیدها، گواهی‌ها و مشاهده اطلاعات دستگاه
iPass Token Checker	برنامه نظارت در System Tray، نمایش وضعیت، همگام‌سازی گواهی و ابزارهای Verify Install، HIDو CSP/KSP
iPass Token Service	سرویس Windowsبرای شناسایی توکن و ثبت/حذف خودکار گواهی در LocalMachine\My
iPass.dll	کتابخانه PKCS#۱۱برای ارتباط برنامه‌ها با توکن
iPassCSP.dll	ارائه‌دهنده Crypt APIبا نام iPassCSPv۱و Provider Type ۱
iPassKSP.dll	ارائه‌دهنده CNGبا نام iPass Key St rage Providerو Aliasبرابر iPassCSPv۱

۱-۴ .نیازمندی‌های سیستم

مورد	نیازمندی
سیستم‌عامل	Windows ۱۰یا Windows ۱۱
معماری	x۸۶ / x۶۴ Installer هر دو مجموعه مورد نیاز را نصب می‌کند
دسترسی نصب	Administrator
پورت اتصال	USB
درایور USB	درایور استاندارد HIDدر Windows
فضای خالی	حداقل ۱۰۰ مگابایت برای نصب و گزارش‌ها

۲ .نصب و راه‌اندازی اولیه

۲-۱ .آماده‌سازی پیش از نصب

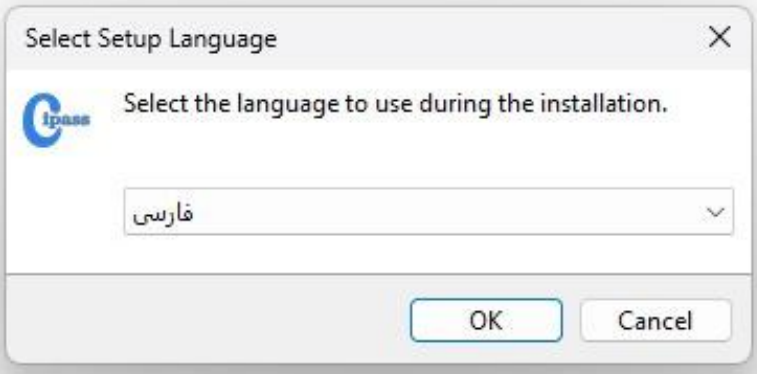
- توکن را پیش از شروع نصب از رایانه جدا کنید.
- فایل نصب را با همان حساب Windowsاجرا کنید که قرار است از توکن استفاده کند.
- در صورت نمایش پیام UAC، دسترسی Administratorرا تأیید کنید.
- برنامه‌های امضا، مرورگرها و نسخه‌های قدیمی Token Manager/Checkerرا ببندید.

نکته : در اغلب نصب‌های تمیز نیازی به Restartنیست .هنگام ارتقا از نسخه قدیمی یا باقی‌ماندن DLLدر حافظه، پس از نصب یک بار Windowsرا Restartکنید.

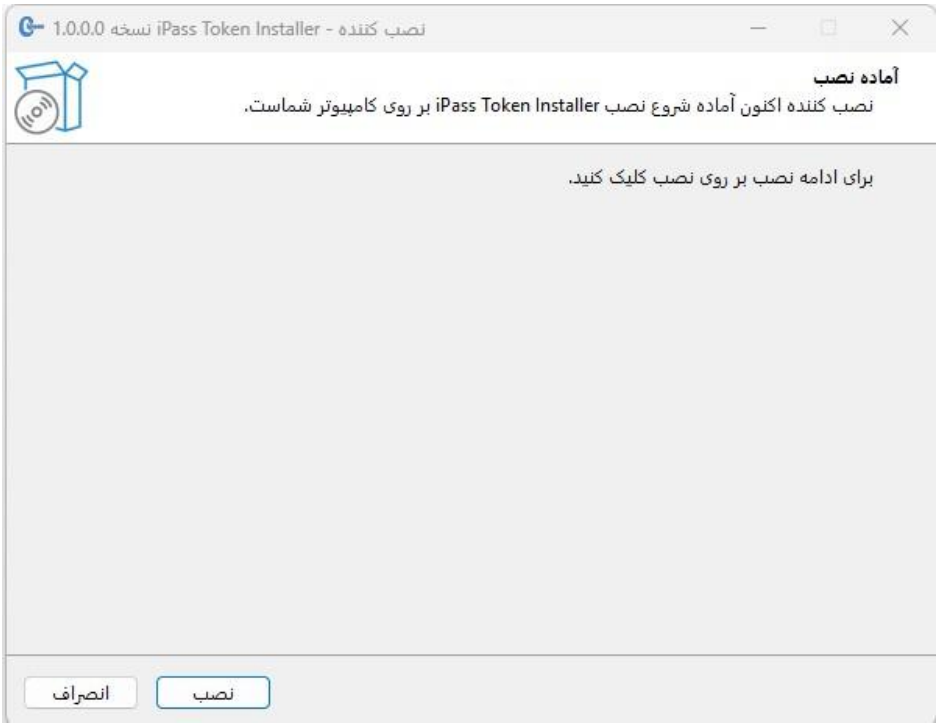
۲-۲ .انتخاب زبان و شروع نصب

۱ .فایل iPassTokenInstaller.exeرا اجرا کنید.

۲ .در پنجره Select Setup Languageگزینه مورد نظر را انتخاب کرده و روی Kکلیک کنید.



۳ .در صفحه آماده نصب :روی دکمه نصب کلیک کنید.

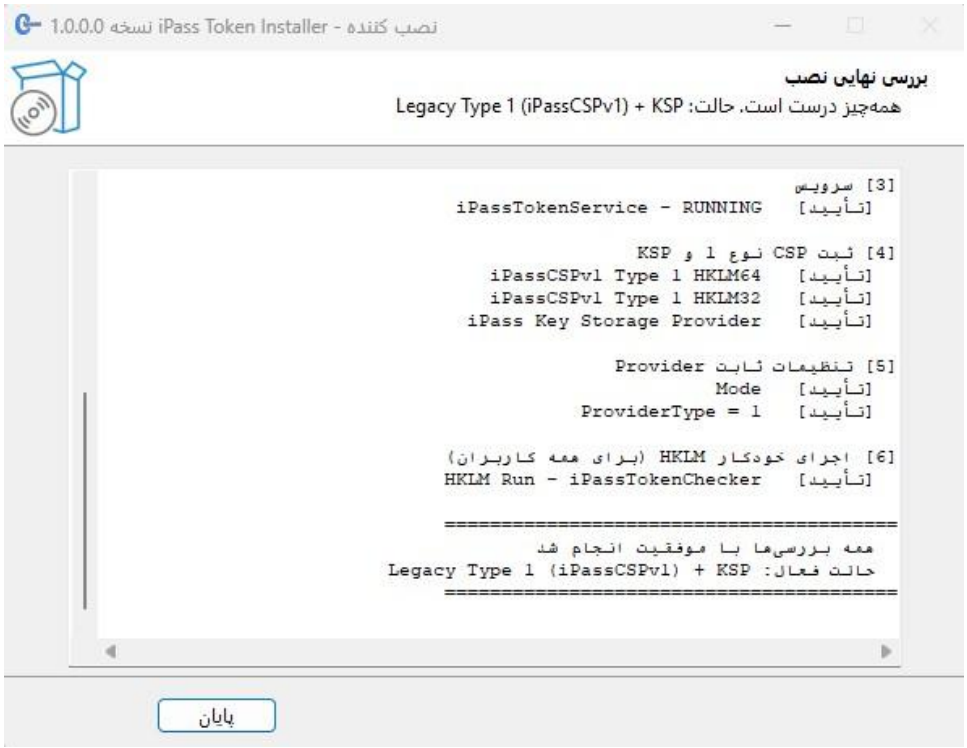


۳-۲ .نصب فایل‌ها و مؤلفه‌های سیستم

Installerفایل‌ها، سرویس، CSP، KSP، تنظیمات Registry، اجرای خودکار Checkerو میانبرهای برنامه را نصب می‌کند .در طول عملیات، پنجره را نبندید و رایانه را خاموش نکنید.

۴-۲ .بررسی خودکار نصب

پس از کپی فایل‌ها، Installerوضعیت سرویس، CSPنوع ۱، KSP، Aliasو اجرای خودکار برنامه Checkerرا بررسی می‌کند . نتیجه مطلوب آن است که تمام موارد با عبارت تأیید نمایش داده شوند.



در صورت خطا :از صفحه نتیجه تصویر بگیرید و عملیات نصب را با دسترسی Administratorتکرار کنید .فایل‌های System۳۲، SysWOW۶۴یا Registryرا بدون هماهنگی پشتیبانی دستی حذف نکنید.

۵-۲ .پایان نصب و اتصال توکن

در صفحه پایانی می‌توانید راهنمای کاربر یا راهنمای سریع را باز کنید .روی »پایان «کلیک کرده، سپس توکن را به پورت USB متصل کنید و چند ثانیه صبر کنید.

۶-۲ .چرخه خودکار گواهی در Windows

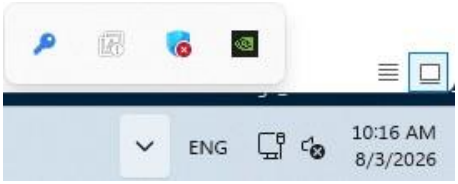
پس از اتصال توکن، iPass Token Serviceگواهی موجود در توکن را خوانده و آن را در LocalMachine\My ثبت می‌کند . iPass Token Checker نیز گواهی را برای حساب کاربری جاری در CurrentUser\My قابل استفاده می‌سازد .با جداکردن توکن، گواهی‌های مربوطه به‌صورت خودکار از مخزن‌های Windowsحذف می‌شوند.

نتیجه عملی :گواهی فقط زمانی در نرم‌افزارهای کاربری قابل استفاده است که توکن متصل باشد، سرویس در حال اجرا باشد و iPass Token Checkerدر حساب کاربر فعال باشد.

۳ .نظارت و عیب‌یابی با iPass Token Checker

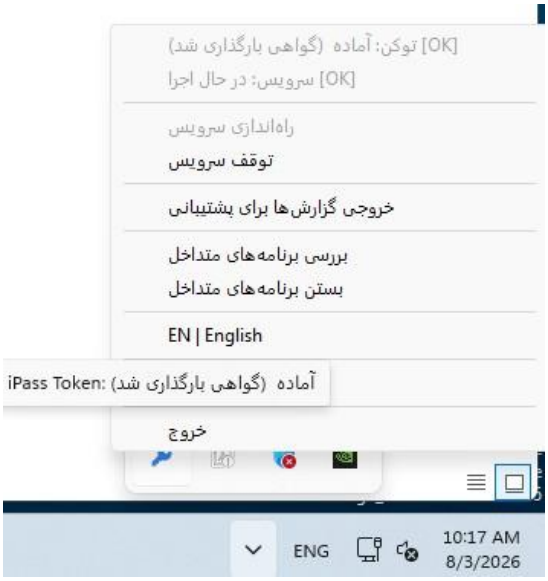
۳-۱ .آیکون کنار ساعت و اجرای خودکار

iPass Token Checker پس از ورود به Windowsبه‌صورت خودکار در System Trayاجرا می‌شود .پس از اتصال توکن، آیکون آبی iPassرا کنار ساعت بررسی کنید.



اگر آیکون دیده نشد :برنامه iPass Token Checkerرا از منوی Startیا مسیر نصب اجرا کنید .اجرای Checkerبرای همگام‌سازی گواهی با حساب کاربر اهمیت دارد.

۳-۲ .منوی راست‌کلیک Checker



گزینه	کاربرد
وضعیت توکن و سرویس	نمایش خلاصه وضعیت در بالای منو
راه‌اندازی سرویس	اجرای iPassTokenService در صورت توقف
توقف سرویس	توقف سرویس برای نگهداری یا عیب‌یابی
خروجی گزارش‌ها برای پشتیبانی	جمع‌آوری لاگ‌ها و گزارش‌های فنی
بررسی برنامه‌های متداخل	شناسایی Process هایی که DLLهای iPassرا در حافظه دارند
بستن برنامه‌های متداخل	بستن موارد شناسایی‌شده با تأیید کاربر
EN | English	تغییر رابط از فارسی به انگلیسی
نمایش پنجره	بازکردن پنجره اصلی Checker
خروج	خروج کامل از Checker

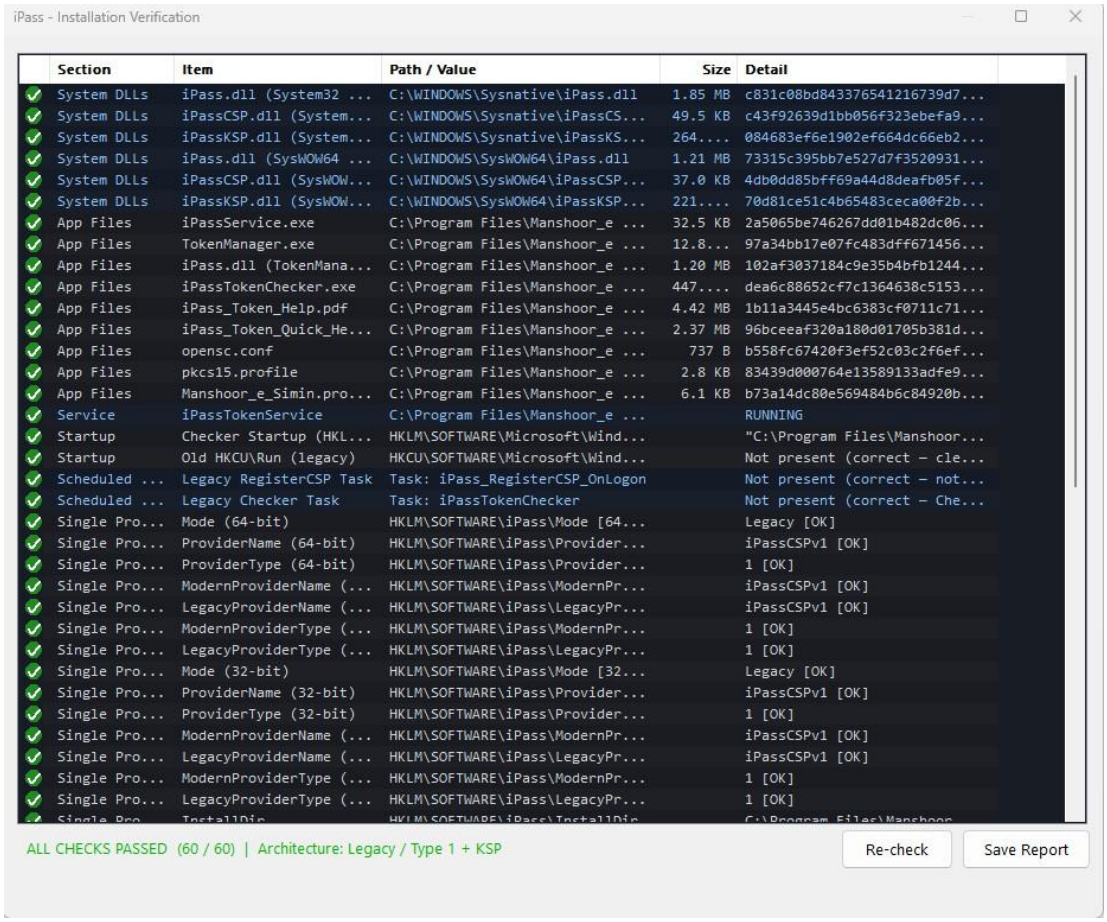
۳-۳ .پنجره اصلی و تفسیر وضعیت‌ها

در حالت سالم، پنجره باید وضعیت آماده (گواهی بارگذاری شد)، نام دستگاه، معماری Legacy / Type ۱ + KSP، نام iPassCSPv۱و اجرای سرویس را نشان دهد.

وضعیت	معنی	اقدام
آماده)گواهی بارگذاری شد(	توکن، کلید و گواهی آماده‌اند	برنامه امضا را اجرا کنید
متصل)بدون گواهی(	توکن دیده شده اما گواهی هنوز آماده نیست	چند ثانیه صبر کرده و »به‌روزرسانی «را بزنید
متصل نیست	توکن در HIDدیده نشده است	پورت USBو اتصال فیزیکی را بررسی کنید
سرویس در حال اجرا	iPassTokenServiceفعال است	وضعیت مطلوب
سرویس متوقف	سرویس فعال نیست	»راه‌اندازی سرویس «را انتخاب کنید

۴-۳ .بررسی کامل نصب (Verify Install)

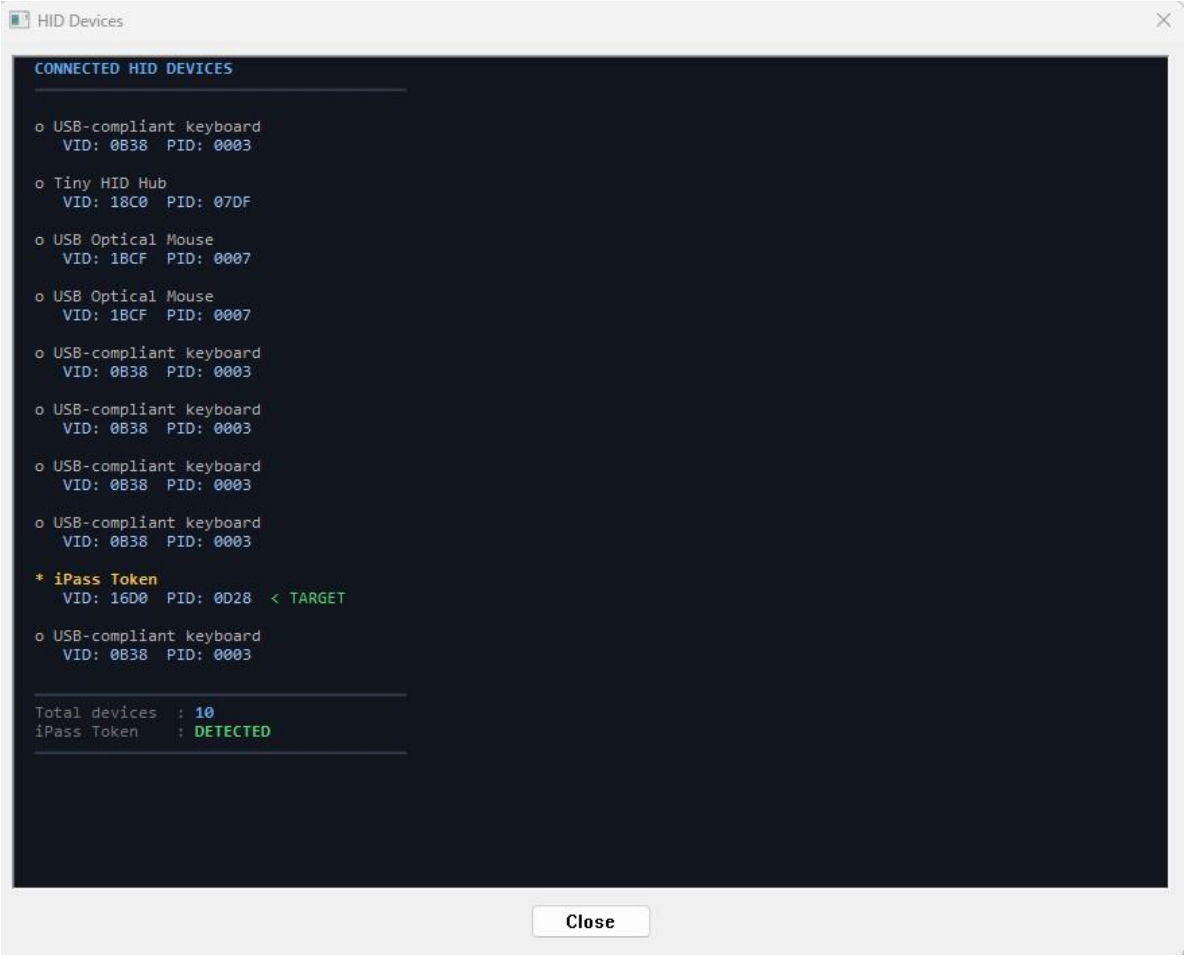
روی »بررسی نصب «کلیک کنید .این ابزار فایل‌های x۸۶/x۶۴، سرویس، اجرای خودکار، Registry، CSP، KSP، Aliasو فایل‌های برنامه را کنترل می‌کند.



معیار اصلی موفقیت، نمایش ALL CHECKS PASSEDو نبود ردیف خطا است .تعداد کنترل‌ها ممکن است در نسخه‌های بعدی تغییر کند.

۵-۳ .بررسی USB HID

روی »دستگاه‌های HID«کلیک کنید .باید ردیفی با نام iPass Token وضعیت DETECTEDدیده شود .در نسخه فعلی شناسه سخت‌افزاری VID=۱۶D۰ وPID=۰D۲۸ است.

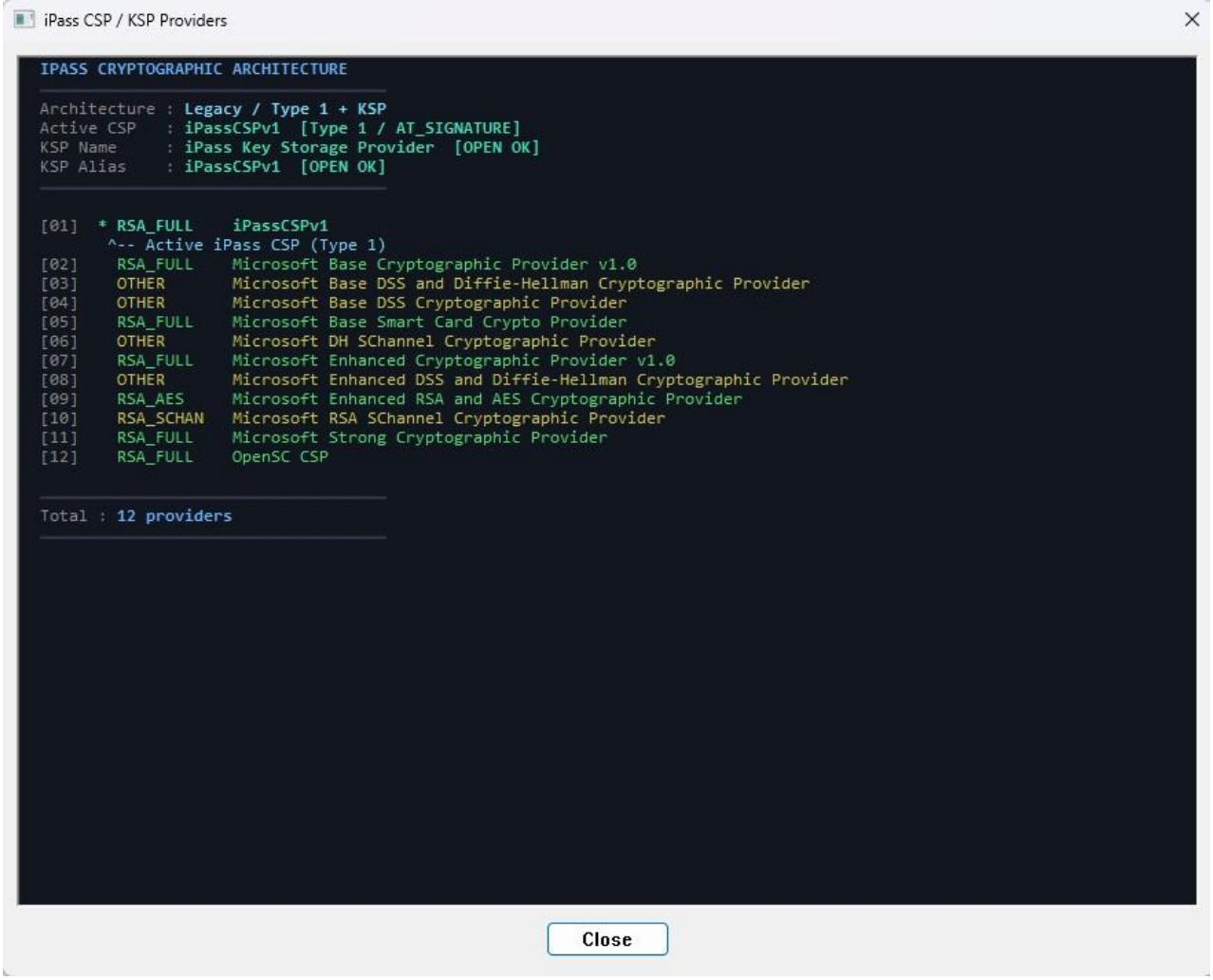


تفکیک خطا :اگر توکن در HIDدیده نشود، مشکل سخت‌افزاری یا USBاست .اگر در HIDدیده شود ولی گواهی آماده نباشد، سرویس، CSP/KSPو اطلاعات داخل توکن را بررسی کنید.

۶-۳ .بررسی CSPو KSP

در اطلاعات CSP، وضعیت معماری و Providerها باید به شکل زیر باشد:

- **Architecture: Legacy / Type ۱ + KSP**
- **Active CSP: iPassCSPv۱ [Type ۱ / AT_SIGNATURE]**
- **KSP Name: iPass Key St rage Provider [OPEN OK]**
- **KSP Alias: iPassCSPv۱ [OPEN OK]**



اهمیت :Alias بازشدن KSP با نام اصلی و Alias برای مسیر امضای CMS SHA-۲۵۶ ضروری است .در صورت خطای CMS SHA-۲۵۶، ابتدا این صفحه و Verify Install را بررسی کنید.

۷-۳ .تهیه گزارش برای پشتیبانی

از منوی Tray گزینه »خروجی گزارش‌ها برای پشتیبانی «را انتخاب کنید .برنامه پوشه iPass_Logs را روی Desktop ایجاد می‌کند و فایل‌های لازم را در آن قرار می‌دهد.

- **پوشه iPass_Logs را بدون تغییر برای پشتیبانی ارسال کنید.**
- **تصویر پنجره Checkerو گزارش Verify Installرا نیز ضمیمه کنید.**
- **نام سامانه مقصد، نسخه Windowsو شرح دقیق خطا را بنویسید.**

مسیر مستقیم لاگ سرویس برای کاربران فنی:

```
C:\Pr gramData\iPass\Logs\iPassService.l g
```

۸-۳ .بستن پنجره و جداکردن صحیح توکن

بستن پنجره اصلی Checkerباعث خروج برنامه نمی‌شود و Checkerدر System Trayفعال می‌ماند .برای خروج کامل، از منوی Trayگزینه »خروج «را انتخاب کنید.

- **پیش از جداکردن توکن، برنامه‌ای را که در حال استفاده از گواهی یا انجام امضا است ببندید.**
- **توکن را جدا کرده و چند ثانیه صبر کنید تا وضعیت Checkerبه »متصل نیست «تغییر کند.**
- **پس از جداسازی، گواهی‌های مربوط به توکن به‌صورت خودکار از Windows Certificate St reحذف می‌شوند.**

۴ .استفاده از iPass Token Manager

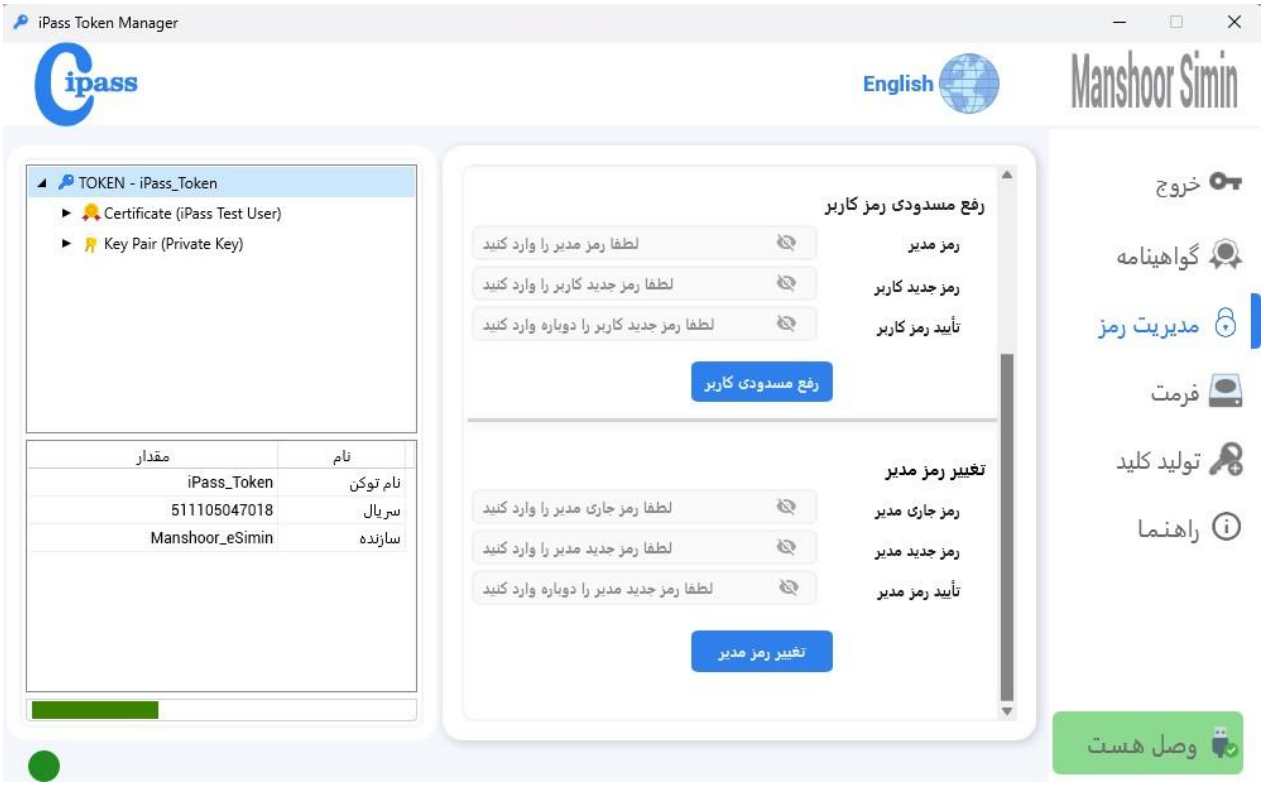
۴-۱ .معرفی و ورود

iPass Token Managerبرای مشاهده توکن، گواهی و کلید خصوصی، تغییر PINها، رفع مسدودی User PIN، تولید کلید و مدیریت گواهی استفاده می‌شود .برنامه را از منوی Startیا میانبر نصب‌شده اجرا کنید.

پس از اتصال توکن، وضعیت پایین برنامه باید »وصل هست «یا Connectedباشد .برای عملیات مدیریتی، از بخش ورود، User PINرا وارد کنید.

PINهای اولیه User PIN :پیش‌فرض 111111 و SO PIN پیش‌فرض 123456 است؛ اما ممکن است سازمان صادرکننده یا تحویل‌دهنده آن‌ها را پیش از تحویل تغییر داده باشد.

۴-۲ .تغییر PINو رفع مسدودی User PIN



در بخش »مدیریت رمز «سه عملیات اصلی وجود دارد:

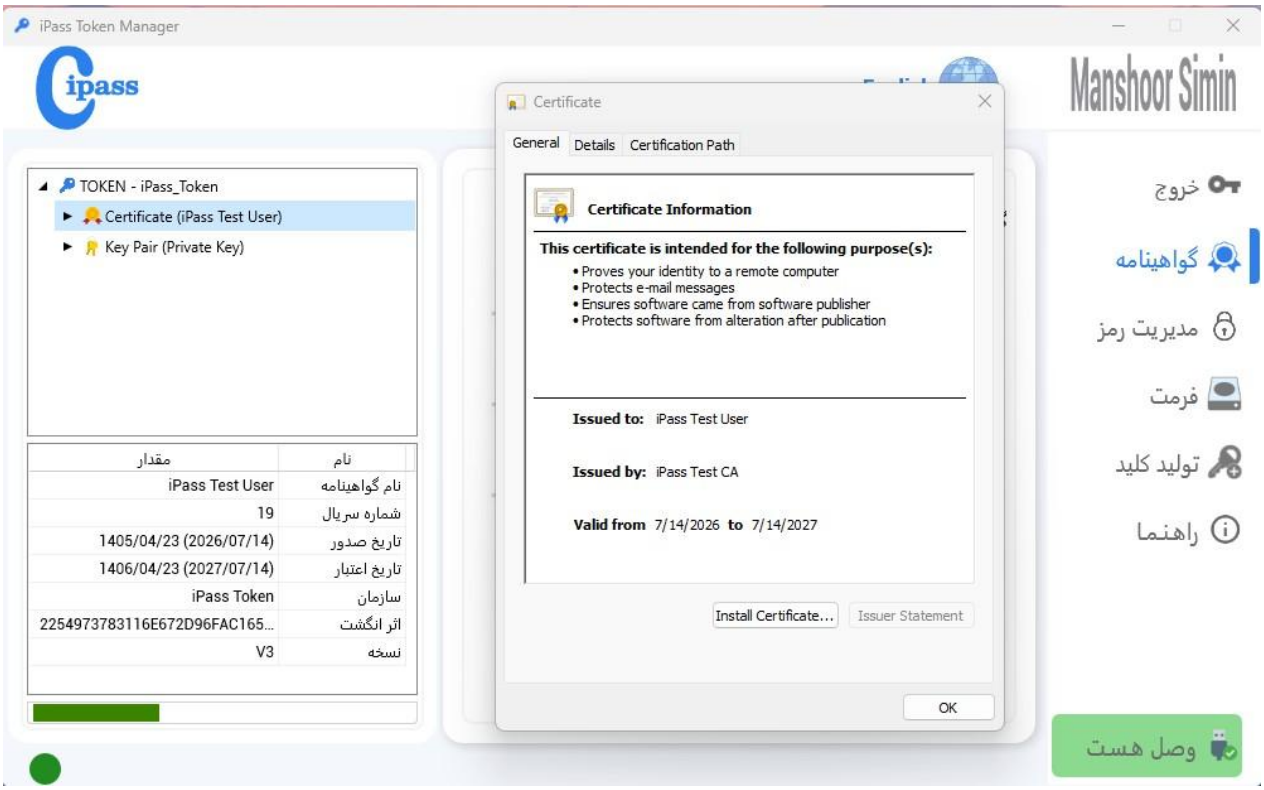
- **تغییر User PIN: ورود User PINفعلی، تعیین User PINجدید و تکرار آن.**
- **رفع مسدودی User PIN: ورود SO PINو تعیین User PINجدید و تکرار آن.**
- **تغییر) SO PINرمز مدیر :(ورود SO PINفعلی، تعیین SO PINجدید و تکرار آن.**

پارامتر امنیتی	مقدار و توضیح
User PIN (Default)	۱۱۱۱۱۱ برای ورود روزمره و انجام امضا
SO PIN / Administrator PIN (Default)	۱۲۳۴۵۶ برای عملیات مدیریتی
User PIN Retry Limit	۱۰ تلاش ناموفق؛ سپس User PINمسدود می‌شود
SO PIN Retry Limit	۳ تلاش ناموفق؛ سپس ادامه آزمون را متوقف کرده و با پشتیبانی تماس بگیرید

امنیت User PIN :و SO PINپیش‌فرض را در اولین استفاده تغییر دهید .پس از سه ورود ناموفق SO PINاز واردکردن رمزهای بیشتر خودداری کنید.

۳-۴ .مشاهده اطلاعات توکن و گواهی

در پنل سمت چپ، نام توکن، شماره سریال، سازنده و میزان فضای استفاده‌شده نمایش داده می‌شود .با انتخاب Certificate، اطلاعات صاحب گواهی، صادرکننده، شماره سریال، تاریخ صدور، تاریخ اعتبار و اثر انگشت قابل مشاهده است.



برای مشاهده پنجره استاندارد Windows Certificate Viewer، گواهی را باز کنید و Valid fr m / Valid t را بررسی کنید .
تمدید گواهی باید از طریق مرجع یا دفتر مجاز صدور گواهی انجام شود.

۴-۴ .خروج امن از Token Manager

- پس از پایان عملیات مدیریتی، از گزینه Logoutاستفاده کنید.
- Token Managerرا ببندید تا Sessionو منابع توکن آزاد شوند.
- سپس در صورت پایان کار، برنامه امضا را نیز بسته و توکن را جدا کنید.

۵ .استفاده از گواهی و انجام امضای دیجیتال

۵-۱ .آماده‌بودن برای امضا

۱ .توکن را متصل کنید و منتظر وضعیت »آماده گواهی بارگذاری شد در Checkerبمانید.

۲ .اعتبار گواهی را در Token Managerیا Windows Certificate Viewerبررسی کنید.

۳ .برنامه یا سامانه مقصد را پس از آماده‌شدن گواهی باز کنید.

۴ .گواهی iPassرا انتخاب کرده و هنگام درخواست، User PINرا وارد کنید.

۵ .پس از موفقیت عملیات، نتیجه امضا یا فایل خروجی را بررسی کنید.

۵-۲ .مسیر ساده عملیات امضا

مرحله	شرح
برنامه مقصد	درخواست امضا با گواهی iPass
Windows Crypt API / CNG	انتخاب Providerو آماده‌سازی Hash/CMS
iPassCSPv۱ / iPass KSP	بازکردن Containerو هدایت عملیات به توکن
توکن سخت‌افزاری	انجام عملیات RSAبا کلید خصوصی داخل توکن
برنامه مقصد	دریافت امضا و تکمیل سند یا پیام CMS

۵-۳ .امضاهای تأییدشده در پروژه

- Raw RSA Sign / Verify
- RSA PKCS#۱ v۱.۵ باSHA-۱ وSHA-۲۵۶
- CMS / PKCS#۷ باSHA-۱ وSHA-۲۵۶
- CMS باSigned Attributes وبدونSigned Attributes

توجه :وجود SHA-۳۸۴، SHA-۵۱۲یا MD۵در فهرست الگوریتم‌های Providerبه معنی تأیید همه مسیرهای CMSبا آن‌ها نیست .مسیرهای عملی تأییدشده در نسخه فعلی SHA-۱وSHA-۲۵۶هستند.

۴-۵ .پس از پایان امضا

- فایل یا پیام امضاشده را در برنامه مقصد Verifyکنید.
- برنامه مقصد را ببندید تا Handleهای توکن و DLLها آزاد شوند.
- توکن را جدا کنید و تغییر وضعیت Checkerرا بررسی کنید.

۶ .تولید کلید و مدیریت گواهی

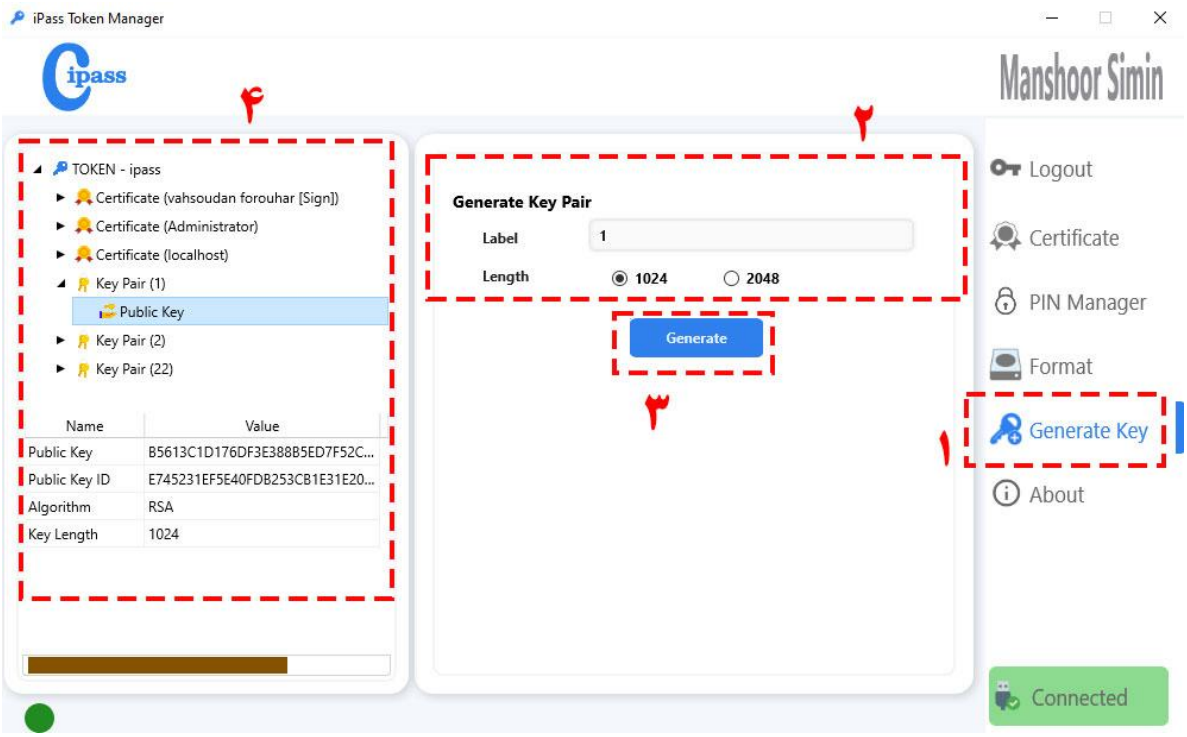
۶-۱ .تولید جفت کلید RSA

پس از ورود به Token Manager، گزینه »تولید کلید «یا Generate Keyرا انتخاب کنید .برای کلید یک نام مشخص تعیین کرده و طول کلید را انتخاب کنید.

RSA-۲۰۴۸: •گزینه توصیه‌شده برای استفاده‌های جدید و امضای دیجیتال.

RSA-۱۰۲۴: •فقط برای سازگاری با سامانه‌های قدیمی و در صورت الزام سازمان مقصد.

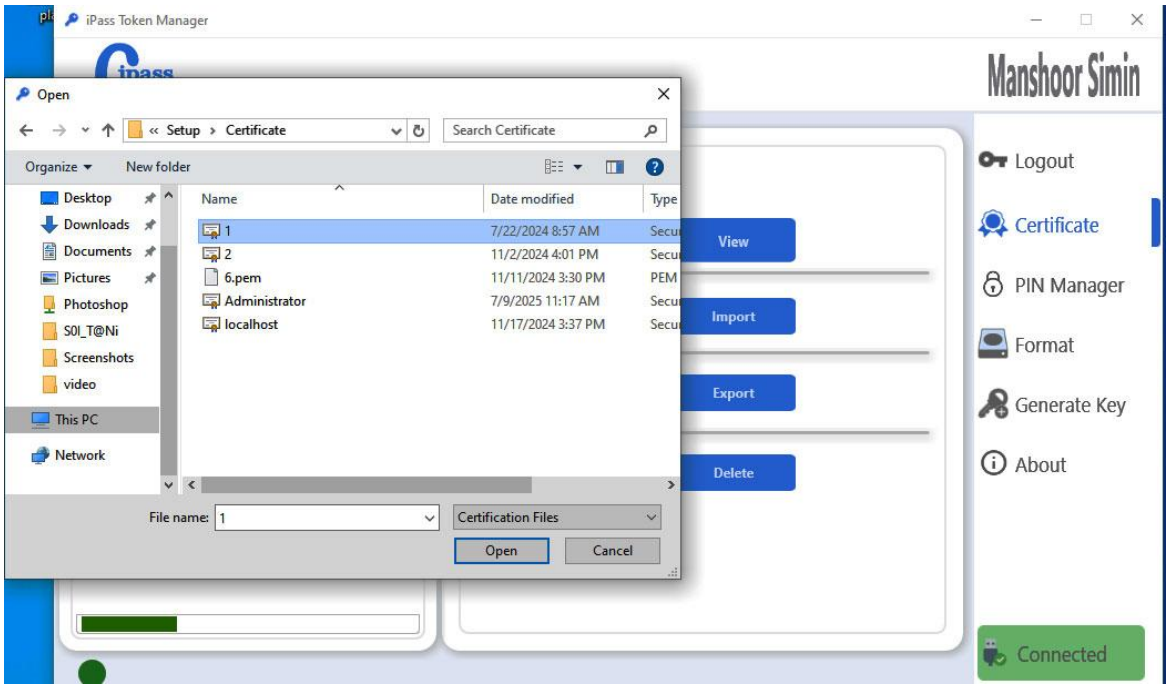
نکته امنیتی :کلید خصوصی داخل توکن تولید و نگهداری می‌شود و نباید امکان خروجی‌گیری از آن فراهم شود .حذف کلید خصوصی می‌تواند گواهی مرتبط را غیرقابل استفاده کند.



۶-۲ .بارگذاری گواهی

گواهی صادرشده باید با کلید عمومی موجود روی توکن مرتبط باشد .از بخش »گواهی‌نامه «گزینه بارگذاری را انتخاب کرده و فایل گواهی را باز کنید .پس از بارگذاری، نام گواهی در درخت سمت چپ نمایش داده می‌شود.

- فرمت‌های معمول: CER ، CRT و PEM
- پیش از بارگذاری، Subject، Issuer، تاریخ اعتبار و تطابق کلید را بررسی کنید.

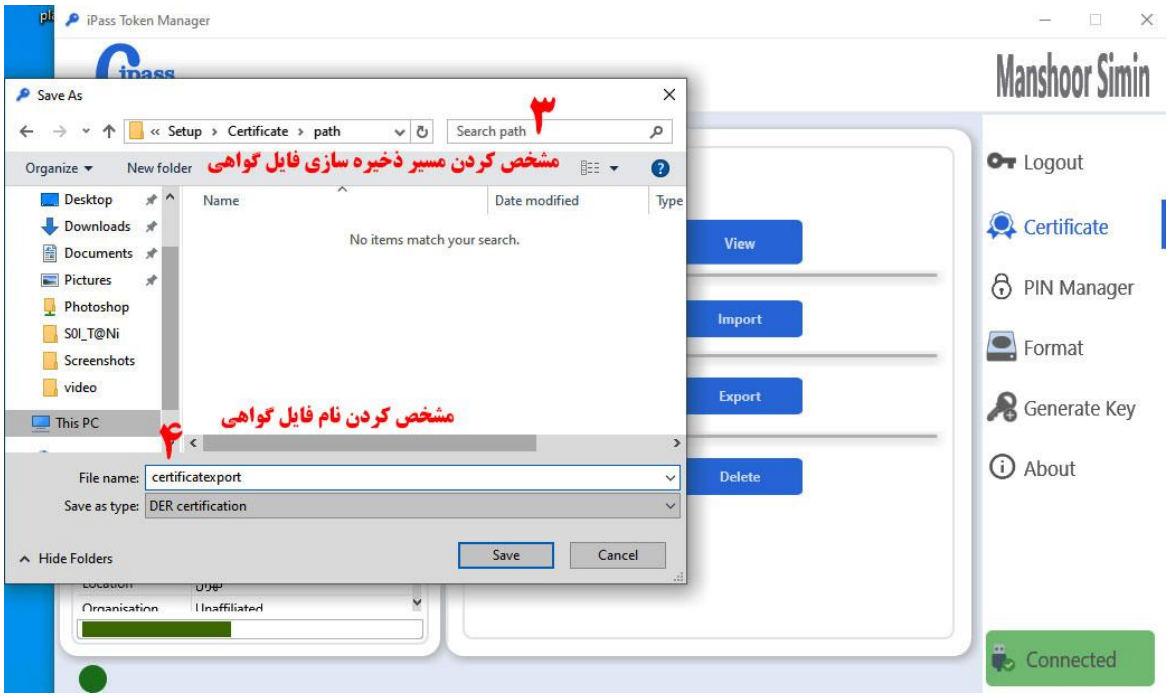


تصویر ۱۷ -نمونه بارگذاری گواهی

۳-۶ .مشاهده و خروجی‌گیری گواهی عمومی

با انتخاب گواهی، اطلاعات آن نمایش داده می‌شود .خروجی‌گیری فقط شامل گواهی عمومی است و کلید خصوصی از توکن خارج نمی‌شود.

- فایل خروجی گواهی را می‌توان برای Verifyامضا یا ثبت در سامانه‌های مجاز استفاده کرد.
- فایل گواهی را همراه با PINیا اطلاعات محرمانه ارسال نکنید.



۶-۴ .حذف گواهی یا کلید

حذف گواهی یا کلید باید با دقت انجام شود .حذف گواهی از توکن، فایل اصلی نزد مرجع صادرکننده را لغو نمی‌کند؛ اما حذف کلید خصوصی می‌تواند امضای بعدی با آن گواهی را غیرممکن سازد.

پیشنهاد :پیش از حذف، نام کلید، شناسه کلید و اثر انگشت گواهی را ثبت کنید .عملیات حذف را فقط با هماهنگی مدیر سامانه یا پشتیبانی انجام دهید.

۷ .فرمت و بازنشانی توکن

۷-۱ .فرمت چه زمانی استفاده می‌شود؟

Format یا Fact ry Resetبرای بازگرداندن توکن به حالت اولیه استفاده می‌شود .این عملیات معمولاً فقط در شرایطی مانند آماده‌سازی مجدد توکن، خرابی داده‌های داخلی یا دستور واحد پشتیبانی انجام می‌شود.

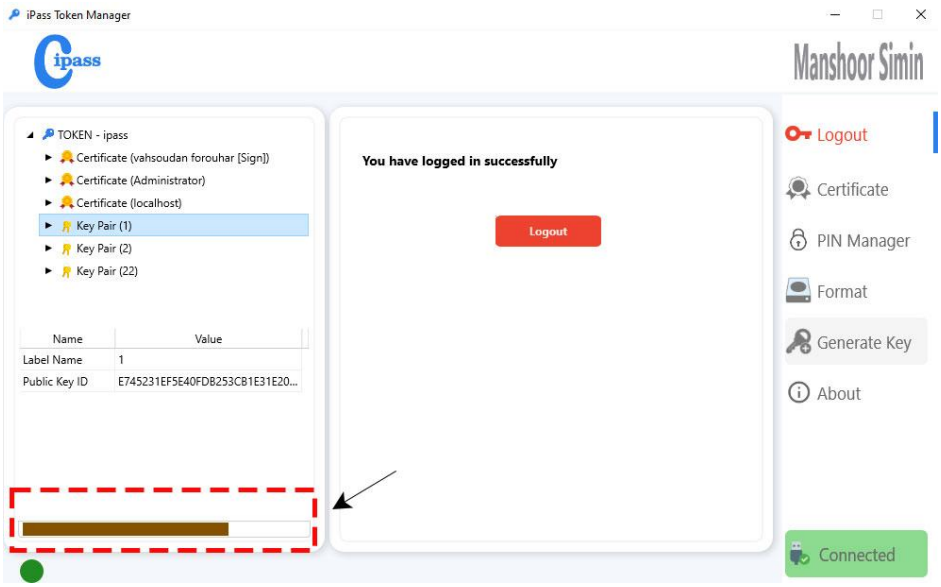
هشدار غیرقابل‌بازگشت Format :تمام کلیدها، گواهی‌ها و اطلاعات ذخیره‌شده روی توکن را حذف می‌کند .پس از آن باید کلید جدید تولید و گواهی جدید صادر یا بارگذاری شود.

۷-۲ .الزامات پیش از فرمت

- **هماهنگی با واحد پشتیبانی یا مدیر امنیت سازمان**
- **اطمینان از در اختیار داشتن SO PIN صحیح**
- **ثبت اطلاعات گواهی‌ها و کلیدهای موجود برای پیگیری**
- **بستن تمام برنامه‌های استفاده‌کننده از توکن**

۷-۳ .روش کلی

- **Token Managerرا اجرا کرده و توکن را متصل کنید.**
- **گزینه »فرمت «را انتخاب کنید.**
- **SO PINو مقادیر جدید مورد نیاز را وارد کنید.**
- **هشدار حذف داده‌ها را با دقت مطالعه و فقط در صورت اطمینان تأیید کنید.**
- **پس از پایان، توکن را مجدداً راه‌اندازی و کلید/گواهی مورد نیاز را ایجاد کنید.**



۸ .راهنمای فنی و یکپارچه‌سازی

۸-۱ .معماری Providerدر Windows

جزء	نام/نوع	کاربرد
CSP	iPassCSPv۱ - Type ۱ / PR V_RSA_FULL	سازگاری با برنامه‌های Crypt APIو Bindingگواهی با AT_SIGNATURE
KSP	iPass Key St rage Provider	مسیر CNGو تکمیل عملیات جدیدتر مانند CMS SHA-۲۵۶
KSP Alias	iPassCSPv۱	ترجمه Handleاز CSPبه KSPتوسط Windows
PKCS#۱۱ Module	iPass.dll	ارتباط مستقیم ابزارها و برنامه‌های PKCS#۱۱با توکن

گواهی با Provider برابر iPassCSPv۱، Provider Type برابر ۱و KeySpec برابر AT_SIGNATURE ثبت می‌شود.

۸-۲ .فایل‌های مهم نصب

فایل	محل معمول	نقش
iPass.dll	System۳۲و SysWOW۶۴	کتابخانه PKCS#۱۱
iPassCSP.dll	System۳۲و SysWOW۶۴	CSPبرای برنامه‌های ۶۴و ۳۲بیتی
iPassKSP.dll	System۳۲و SysWOW۶۴	KSPبرای برنامه‌های ۶۴و ۳۲بیتی
iPassTokenService	Pr gram Files	سرویس مدیریت گواهی
iPassTokenChecker.exe	Pr gram Files	Checkerو System Tray
TokenManager.exe	Pr gram Files	مدیریت توکن

۸-۳ .آزمایش PKCS#۱۱با pkcs۱۱-t l

ویژه کاربران فنی :دستورهای این بخش برای تست و یکپارچه‌سازی هستند .PIN واقعی را در Script، Historyیا فایل گزارش ذخیره نکنید .مسیر ابزار و DLLباید از نظر x۸۶/x۶۴با یکدیگر هماهنگ باشند.

نمونه مشاهده Sl tها و اطلاعات توکن:

```
pkcs۱۱-t l --module C:\Windows\System۳۲\iPass.dll --list-slots\npkcs۱۱-t l --module C:\Windows\System۳۲\iPass.dll --list-mechanisms
```

نمونه فهرست اشیای توکن؛ مقدار <USER_PIN>را فقط در محیط کنترل‌شده جایگزین کنید:

```
pkcs۱۱-t l --module C:\Windows\System۳۲\iPass.dll --l gin --pin <USER_PIN> --list- objects
```

نمونه تولید کلید RSA-۲۰۴۸برای آزمایش فنی:

```
pkcs۱۱-t l --module C:\Windows\System۳۲\iPass.dll --l gin --pin <USER_PIN> --keypairgen --key-type rsa:۲۰۴۸ --id ۰۲ --label Test Key
```

نمونه امضای فایل با SHA-۲۵۶و :RSA PKCS#۱ v۱.۵

```
pkcs۱۱-t l --module C:\Windows\System۳۲\iPass.dll --l gin --pin <USER_PIN> --sign --id ۰۲ --mechanism SHA۲۵۶-RSA-PKCS --input-file testmsg.txt -- output-file testmsg.sig
```

۸-۴ .نکات یکپارچه‌سازی

- برنامه‌های ۳۲بیتی باید DLLهای SysWOW۶۴و برنامه‌های ۶۴بیتی DLLهای System۳۲را استفاده کنند.
- در تست CMS SHA-۲۵۶، KSP Nameو KSP Aliasباید هر دو PEN Kباشند.
- برای عملیات امضا از کلید AT_SIGNATUREاستفاده می‌شود.
- در تست‌های خودکار، ابتدا Size Queryو سپس فراخوانی واقعی Signرا اجرا کنید.
- از اجرای همزمان چند ابزار مدیریتی یا PKCS#۱۱روی توکن خودداری کنید.

۹ .عیب‌یابی جامع

۹-۱ .سرویس اجرا نمی‌شود

- در Checkerوضعیت سرویس را بررسی و »راه‌اندازی سرویس «را اجرا کنید.
- در Verify Installوجود فایل سرویس و ثبت آن را کنترل کنید.
- در services.mscسرویس iPassTokenServiceرا بررسی کنید.
- لاگ C:\ProgramData\iPass\Logs\iPassService.l gرا بررسی کنید.

۹-۲ .توکن در HIDدیده نمی‌شود

- توکن را جدا و دوباره متصل کنید.
- پورت USBدیگری را امتحان کنید؛ از Hubنامطمئن استفاده نکنید.
- توکن را روی رایانه دیگری آزمایش کنید.
- در صورت تداوم، مشکل سخت‌افزاری یا USBرا به پشتیبانی گزارش کنید.

۹-۳ .گواهی در برنامه مقصد دیده نمی‌شود

- وضعیت Checkerباید آماده (گواهی بارگذاری شد) باشد.
- Serviceو Checkerهر دو باید فعال باشند.
- برنامه مقصد را پس از اتصال توکن ببندید و دوباره باز کنید.
- Verify Install •و اعتبار گواهی را بررسی کنید.

۹-۴ .توکن آماده است ولی امضا خطا می‌دهد

- اعتبار و Key Usageگواهی را در Windows Certificate Viewerبررسی کنید.
- برنامه‌های متداخل را از منوی Checkerبررسی و با تأیید کاربر ببندید.
- KSP Nameو Aliasرا در CSP Infoکنترل کنید.
- پوشه گزارش‌ها و نام دقیق سامانه مقصد را برای پشتیبانی ارسال کنید.

۹-۵ .خطای CMS SHA-۲۵۶

- Verify Installباید ثبت iPassCSPv۱ Type ۱، فایل‌های KSPو Aliasرا تأیید کند.
- در CSP Infoهر دو مورد KSP Nameو KSP Aliasباید PEN Kباشند.
- نسخه‌های x۸۶و iPassCSP.dll x۶۴و iPassKSP.dllباید از یک Releaseباشند.
- پس از ارتقا، Windowsرا Restartکنید تا DLLهای قدیمی از حافظه خارج شوند.

۹-۶ .خطاهای PIN

- User PINپیش‌فرض ۱۱۱۱۱۱است، مگر اینکه تغییر داده شده باشد.
- پس از ۱۰ تلاش ناموفق User PINمسدود می‌شود؛ برای Unblockاز SO PINاستفاده کنید.
- پس از ۳ تلاش ناموفق SO PIN، ادامه آزمون را متوقف و با پشتیبانی تماس بگیرید.
- NumLock و زبان صفحه‌کلید را بررسی کنید.

۷-۹ .نسخه قدیمی DLLدر حافظه است

- مرورگرها، برنامه‌های امضا، Token Managerو ابزارهای خط فرمان را ببندید.
- از Check Conflicting Apps استفاده کنید.
- در صورت نیاز Windowsرا Restartکنید.

۸-۹ .اطلاعات لازم برای درخواست پشتیبانی

اطلاعات	نمونه
نسخه Windowsو معماری	Windows ۱۱ x۶۴ / x۸۶
نام سامانه مقصد	نام وب‌سایت یا نرم‌افزار امضا
شرح خطا	متن کامل خطا و زمان وقوع
وضعیت Checker	تصویر پنجره اصلی
Verify Install	فایل Save Reportیا تصویر ردیف خطا
گزارش‌ها	پوشه iPass_Logs روی Desktop

۱۰ .نکات امنیتی و بهترین روش‌ها

- User PINو SO PINپیش‌فرض را در اولین استفاده تغییر دهید.
- PINرا روی بدنه توکن، در کیف آن یا در فایل بدون حفاظت ذخیره نکنید.
- توکن را در اختیار افراد غیرمجاز قرار ندهید؛ مسئولیت امضای انجام‌شده متوجه مالک توکن است.
- از توکن فقط روی رایانه‌های مطمئن و دارای نرم‌افزار امنیتی به‌روز استفاده کنید.
- پس از پایان کار، برنامه امضا را ببندید، از Token Managerخارج شوید و توکن را جدا کنید.
- فایل‌های گزارش را فقط برای واحد پشتیبانی مجاز ارسال کنید.
- کلید RSA-۲۰۴۸را برای استفاده‌های جدید ترجیح دهید؛ RSA-۱۰۲۴فقط برای سازگاری قدیمی است.
- Format/Factory Resetرا فقط با هماهنگی پشتیبانی انجام دهید.
- از قرار دادن PINدر Command Lineیا Scriptهای دائمی خودداری کنید.

یادآوری :کلید خصوصی داخل توکن نگهداری می‌شود و حذف یا فرمت توکن قابل بازگشت نیست .داشتن فایل گواهی عمومی جایگزین کلید خصوصی نیست.

۱۱ .واژه‌نامه و اطلاعات پشتیبانی

۱۱-۱ .واژه‌نامه

اصطلاح	تعریف
Token	دستگاه سخت‌افزاری نگهداری کلید و گواهی
User PIN	رمز ورود روزمره برای دسترسی به کلید و امضا
SO PIN	رمز مدیریتی برای Unblock، تغییر تنظیمات و Format
Certificate	گواهی دیجیتال مرتبط با کلید عمومی
Private Key	کلید خصوصی غیرقابل استخراج برای انجام امضا
Public Key	کلید عمومی برای Verifyامضا و صدور گواهی
PKCS#۱۱	رابط استاندارد برنامه‌ها با توکن‌های رمزنگاری
CSP	Crypt graphic Service Providerبرای Windows Crypt API
KSP	Key St rage Providerبرای Windows CNG
Provider Type ۱	نوع CSPفعال پروژه با نام iPassCSPv۱
Windows Certificate St re	محل ثبت موقت گواهی در Windows
iPass Token Checker	برنامه نظارت، همگام‌سازی گواهی و بررسی سلامت
Verify Install	ابزار کنترل فایل‌ها، سرویس، Registry، CSPو KSP
Export Logs	جمع‌آوری گزارش‌ها در پوشه iPass_Logs

۱۱-۲ .اطلاعات تماس و دانلود

عنوان	اطلاعات
صفحه محصول	https://usbarm.c m/ipass/
وب‌سایت شرکت	www.dedj.c m
ایمیل پشتیبانی	inf @dedj.c m
تلفن‌های پشتیبانی	۶۶۵۹۵۹۶۱	۶۶۹۴۸۵۳۴	۶۶۹۲۲۶۳۴	۶۶۹۳۴۹۵۲	۶۶۹۳۳۵۲۳تا ۶۶۵۹۵۹۶۵
ساعات کاری	شنبه تا چهارشنبه، ساعت ۸ صبح تا ۵ عصر

۱۱-۳ .روش استاندارد ارسال درخواست پشتیبانی

۱ Checker .را باز کرده و وضعیت توکن، سرویس و معماری را ثبت کنید.

۲ Verify Install .را اجرا و در صورت خطا Save Reportرا انتخاب کنید.

۳ .از منوی Trayگزینه »خروجی گزارش‌ها برای پشتیبانی «را اجرا کنید.

۴ .پوشه iPass_Logs، تصویرها و شرح خطا را بدون تغییر ارسال کنید.

۵ .از ارسال PIN، SO PINیا اطلاعات محرمانه خودداری کنید.

۱۱-۴ .تاریخچه نسخه سند

نسخه	تغییرات
۰.۶	هماهنگی کامل با معماری تک‌حالته iPassCSPv1 Type 1 + KSP؛ جایگزینی تصاویر Installerو Checker؛ بازنویسی PIN، گواهی، امضا، گزارش‌گیری، عیب‌یابی و بخش فنی؛ حذف ادعاها و توضیحات قدیمی
۰.۵	به‌روزرسانی اولیه معماری CSP/KSPو Token Monitor