



مرکز تنظیم مقررات، نظام پایانه‌های فروشگاهی و سامانه مودیان

«سوال‌های متداول در مورد امضای دیجیتال امر سازمانی»

شناسه سند: RC_FAQU.DS_V01



فروردین ۱۴۰۲

(۱) امضای دیجیتال چیست؟

یک رشته عددی که به روش پیچیده‌ای از متن یک سند استخراج و پس از رمزگذاری با کلید خصوصی صاحب سند، به اصل سند ضمیمه و ارسال می‌شود به گونه‌ای که هر گیرنده اطلاعات بتواند منبع و تمامیت اطلاعات را تشخیص دهد.

(۲) دلایل ضرورت به کارگیری امضای دیجیتال در صدور و ارسال صورتحساب‌های الکترونیکی چیست؟

تامین نیازمندی‌های امنیتی جامعیت، احراز هویت و انکارناپذیری در سامانه مودیان.

(۳) گواهی الکترونیکی امضای دیجیتال / مهر سازمانی چیست؟

یک سند الکترونیکی حاوی اطلاعاتی در مورد مرکز صادر کننده گواهی، مالک گواهی، تاریخ صدور و انقضاء کلید عمومی مالک و یک شماره سریال که توسط مرکز میانی تولید شده به گونه‌ای که هر شخصی می‌تواند به صحت ارتباط بین کلید عمومی و مالک آن اعتماد کند.

(۴) انواع گواهی الکترونیکی قابل قبول در سامانه مودیان چیست؟

- **گواهی الکترونیکی امضای دیجیتال (شخص حقیقی مستقل)**

این گواهی برای اشخاص حقیقی جهت امضای اسناد، صورتحساب‌های الکترونیکی و ارسال درخواست‌ها مورد استفاده قرار می‌گیرد.

- **گواهی الکترونیکی مهر سازمانی**

این گواهی برای اشخاص حقوقی به عنوان مهر سازمانی آن شرکت یا سازمان در قالب امضای دیجیتال جهت امضای اسناد، صورتحساب‌های الکترونیکی و ارسال درخواست‌ها مورد استفاده قرار می‌گیرد.

(۵) نحوه تشخیص گواهی الکترونیکی امضای دیجیتال و مهر سازمانی چیست؟

روی فایل گواهی دوبار کلیک می‌کنیم. سپس در برگه Details فیلد Subject را انتخاب می‌کنیم. به مقدار زیرفیلد CN توجه می‌کنیم. اگر کنار نام صاحب گواهی عبارت [sign] درج شده باشد نشان دهنده گواهی امضای دیجیتال و در صورتی که [stamp] درج شده باشد، گواهی مهر سازمانی است.

۶) سطح اطمینان قابل قبول گواهی الکترونیکی برای اشخاص حقیقی و حقوقی در سامانه مودیان چیست؟

از میان چهار سطح اطمینانی که مرکز دولتی صدور گواهی الکترونیکی ریشه برای صدور گواهی های الکترونیکی تعریف نموده است سطح ۲ یا نقره برای گواهی الکترونیکی اشخاص حقیقی و حقوقی در سامانه مودیان قابل استفاده می باشد. جزییات سطوح اطمینان در سند سیاست های گواهی الکترونیکی زیر ساخت کلید عمومی کشور در وبسایت اطلاع رسانی مرکز دولتی صدور گواهی الکترونیکی ریشه به نشانی www.rca.gov.ir قابل مشاهده می باشد.

۷) مرکز دولتی صدور گواهی الکترونیکی ریشه چیست؟

مرکزی است که بر اساس مفاد بند الف از ماده ۴ آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست گذاری گواهی الکترونیکی کشور در مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور، تعلیق/رفع تعلیق و ابطال گواهی الکترونیکی مراکز صدور گواهی میانی را دریافت کرده است.

۸) مرکز میانی چیست و مراکز میانی فعال در زیرساخت کلید عمومی کشور کدامند؟

مرکز صدور گواهی میانی یا به اختصار مرکز میانی، موجودیتی است که با کسب مجوز از مرکز دولتی صدور گواهی الکترونیکی ریشه وظیفه صدور و مدیریت گواهی های الکترونیکی را بر عهده دارد و پیوند بین اطلاعات گواهی را ضمانت می نماید. مرکز میانی، گواهی خود را از مرکز دولتی صدور گواهی الکترونیکی ریشه دریافت می نماید. در حال حاضر ۸ مرکز میانی فعال در کشور وجود دارند که عبارتند از:

جدول ۱: مراکز میانی فعال

ردیف	نام مرکز میانی	وبسایت
۱	مرکز میانی دولتی عام	https://www.gica.ir/portal
۲	مرکز میانی دولتی نفت	http://www.petrotrust.ir
۳	مرکز میانی دولتی بازار سرمایه	http://www.icmca.ir
۴	مرکز میانی دولتی سلامت	http://healthca.behdasht.gov.ir
۵	مرکز میانی دولتی بانک ملی ایران	https://trust.bmi.ir
۶	مرکز میانی خصوصی اعتماد هوشمند	https://ca.smarttrustco.ir
۷	مرکز میانی خصوصی فناوران اعتماد راهبر	http://ca.raahbartrust.ir
۸	مرکز میانی خصوصی پارس ساین	http://www.parssignca.ir

لیست مراکز میانی، نشانی و سایر اطلاعات تماس این مراکز در وبسایت اطلاع رسانی مرکز دولتی صدور گواهی الکترونیکی ریشه به آدرس www.rca.gov.ir قابل مشاهده می باشد.

۹) آیا بین مراکز میانی دولتی و خصوصی برای اخذ گواهی الکترونیکی جهت استفاده در سامانه مودیان تفاوتی وجود دارد؟

خیر. تفاوتی وجود ندارد. مودیان می توانند گواهی الکترونیکی خود را از کلیه مراکز میانی دارای مجوز از مرکز دولتی صدور گواهی الکترونیکی ریشه اخذ نمایند.

۱۰) مودیان در کدام یک از روش های ارسال صورتحساب الکترونیکی به سامانه مودیان نیاز به اخذ گواهی الکترونیکی دارند؟

در صورتیکه مودی در کارپوشه سامانه مودیان نحوه ارسال صورتحساب الکترونیکی را یکی از روش های الف- توسط مودی یا

ب- توسط شرکت معتمد / سامانه های دولتی - با کلید مودی

انتخاب نماید، نیازمند اخذ گواهی از یکی از مراکز میانی است. جزییات روش های ارسال صورتحساب الکترونیکی در اسناد بارگذاری شده در درگاه سازمان امور مالیاتی کشور به نشانی www.intamedia.ir بخش "پایانه های فروشگاهی و سامانه مودیان" قسمت "آیین نامه ها، دستورالعمل ها و نرم افزارهای مرتبط" قابل دسترسی می باشد.

۱۱) آیا اشخاص حقوقی می توانند از گواهی امضای دیجیتال شخصی مدیر عامل یا سایر صاحبان امضای شرکت در سامانه مودیان استفاده نمایند؟

خیر اشخاص حقوقی می بایست صرفاً از گواهی الکترونیکی مهر سازمانی در سامانه مودیان استفاده نمایند.

۱۲) آیا مودیان امکان استفاده از گواهی الکترونیکی موجود را جهت استفاده در سامانه مودیان دارند؟

• **اشخاص حقوقی:** در صورتی که گواهی الکترونیکی مهر سازمانی منطبق با مشخصات ذکر شده در اسناد سامانه مودیان را دارند به شرط رعایت موارد امنیتی مورد نظر مرکز دولتی صدور گواهی الکترونیکی ریشه، می توانند از همان گواهی، در سامانه مودیان استفاده نمایند. اشخاص حقوقی نمی توانند از گواهی الکترونیکی، امضای دیجیتال اشخاص حقیقی وابسته، در سامانه مودیان استفاده کنند.

• **اشخاص حقیقی:** در صورتی که گواهی الکترونیکی امضای دیجیتال (گواهی شخص حقیقی مستقل) با مشخصات ذکر شده در اسناد سامانه مودیان را دارند به شرط رعایت موارد امنیتی مورد نظر مرکز دولتی صدور گواهی الکترونیکی ریشه، می توانند از همان گواهی، در سامانه مودیان استفاده نمایند.

۱۳) آیا کپی برداری از کلید خصوصی مجاز است؟

خیر کپی برداری کلید خصوصی مجاز نیست و مسئولیت حقوقی نگهداری و حفاظت از آن صرفاً به عهده مالک گواهی است.

۱۴) آیا امکان کپی برداری از گواهی الکترونیکی وجود دارد؟

بله کپی برداری و انتشار گواهی الکترونیکی امضای دیجیتال/مهر سازمانی امکان پذیر است.

۱۵) فرایند کلی دریافت گواهی الکترونیکی از مراکز میانی به چه صورت است؟

به عنوان نمونه فرایند کلی دریافت گواهی الکترونیکی از مرکز میانی دولتی عام به شرح ذیل می باشد. (اخذ اطلاعات در مورد فرایند سایر مراکز با مراجعه به سایت مربوطه، امکان پذیر است).

• توکن سخت افزاری

- ثبت نام در سامانه مرکز میانی عام
- ورود به سامانه از طریق نام کاربری و کلمه عبور دریافت شده در زمان ثبت نام
- ثبت درخواست گواهی الکترونیکی و دریافت کد رهگیری
- تهیه توکن سخت افزاری ارزیابی شده و مورد تأیید مرکز دولتی صدور گواهی الکترونیکی ریشه
- انتخاب نزدیکترین دفتر ثبت نام و مراجعه حضوری جهت احراز هویت و صدور گواهی الکترونیکی

• از طریق CSR (نرم افزاری/HSM)

- ثبت نام در سامانه مرکز میانی عام
- ورود به سامانه از طریق نام کاربری و کلمه عبور دریافت شده در زمان ثبت نام
- ثبت درخواست گواهی الکترونیکی، بارگذاری فایل CSR و دریافت کد رهگیری

○ انتخاب نزدیکترین دفتر ثبت نام و مراجعه حضوری جهت احراز هویت و صدور

گواهی الکترونیکی

۱۶) روش‌های نگهداری کلید خصوصی متناظر با گواهی الکترونیکی به چه صورت است؟

• سخت افزاری: توکن سخت افزاری/HSM

• نرم افزاری: نگهداری در سرور/سیستم

۱۷) توکن سخت افزاری چیست؟

سخت افزاری از نوع Plug and Play است که از طریق درگاه USB به سیستم رایانه کاربر متصل می‌شود. توکن سخت افزاری دارای تراشه کارت هوشمندی است که الگوریتم‌های رمزگذاری پایه را به صورت onboard پشتیبانی می‌کند و در آن امکان نگهداری چندین گواهی الکترونیکی وجود دارد. توکن‌های سخت افزاری دارای رمز پیشفرض می‌باشند که می‌بایست از محل تهیه توکن سخت افزاری دریافت گردد.

۱۸) رمز توکن سخت افزاری از کجا بدست می‌آید و چه کاربردی دارد؟

رمز پیشفرض کاربر توکن (User PIN) از طرف شرکت تولید کننده توکن سخت افزاری ایجاد شده و هنگام تهیه توکن به خریدار اعلام می‌شود. هنگام اتصال و استفاده از توکن، ورود این رمز توسط کاربر الزامی است. پیشنهاد می‌گردد برای جلوگیری از سوء استفاده از توکن، رمز عبور پیش فرض تغییر داده شود. در صورت فراموشی کد pin یا قفل شدن توکن باید با به بخش پشتیبانی و راهنمای شرکت تولید کننده آن مراجعه کرد.

۱۹) در صورت فراموشی کد pin یا قفل شدن توکن به دلیل ورود کد pin اشتباه چه

اقدامی باید انجام داد؟

در صورت فراموشی کد pin یا قفل شدن توکن باید با به بخش پشتیبانی و راهنمای شرکت تولید کننده آن مراجعه کرد.

۲۰) مودیان از چه نوع توکن سخت افزاری جهت استفاده در سامانه مودیان استفاده کنند؟

مودیان در صورت نیاز به توکن سخت افزاری می‌بایست از توکن‌های مورد تایید مرکز دولتی صدور گواهی الکترونیکی ریشه به آدرس www.rca.gov.ir استفاده نمایند.

۲۱) آیا کلید خصوصی مورد نیاز برای امضای صورتحساب‌های الکترونیکی از توکن

سخت افزاری قابل استخراج است؟

خیر، کلید خصوصی از توکن سخت افزاری قابل استخراج نیست. پایانه فروشگاهی/سیستم صدور و ارسال صورتحساب الکترونیکی می‌بایست مجهز به قابلیت ارتباط و استفاده از کلید خصوصی موجود در توکن برای امضای صورتحساب‌های الکترونیکی و درخواست‌های ارسالی به سامانه مودیان باشد.

(۲۲) آیا کلید خصوصی مورد نیاز برای امضای صورتحساب‌های الکترونیکی تولید شده به روش CSR (نرم افزاری) قابل استخراج است؟
 بله، در این روش کلید خصوصی توسط خود مالک گواهی تولید می‌گردد و مسئولیت حقوقی نگهداری و حفاظت از آن صرفاً به عهده مالک گواهی است.

(۲۳) HSM چیست؟

ماژول امن سخت افزاری (Hardware Security Module)، سخت افزاری مخصوص عملیات رمزنگاری است که جهت تولید و نگهداری امن کلیدهای رمزنگاری ساخته شده است. از وظایف HSM می‌توان به تولید و نگهداری امن کلیدهای رمزنگاری، و ارائه سرویس‌های مرتبط با رمزگذاری، رمزگشایی، احراز هویت و امضای دیجیتال اشاره کرد. استفاده از HSM در صورتی توصیه می‌شود که به تعداد بالای امضای صورتحساب‌های الکترونیکی در ثانیه نیاز است.

(۲۴) آیا برای یک مودی حقوقی امکان اخذ چند گواهی الکترونیکی مهر سازمانی از یک یا چند مرکز میانی وجود دارد؟

بله این امکان وجود دارد. اشخاص حقوقی می‌توانند در صورت نیاز برای هر یک از واحدهای سازمانی ذیربط چند گواهی الکترونیکی مهر سازمانی دریافت کنند.

(۲۵) آیا برای یک مودی حقیقی امکان اخذ چند گواهی الکترونیکی امضای دیجیتال از مراکز میانی وجود دارد؟

در حال حاضر امکان دریافت چند گواهی الکترونیکی امضای دیجیتال برای شخص حقیقی از یک مرکز میانی وجود ندارد لیکن در صورت نیاز، مودی حقیقی می‌تواند چند گواهی الکترونیکی امضای دیجیتال را از مراکز میانی مختلف دریافت نماید.

(۲۶) آیا در صورتی که یک مودی حقوقی توکن سخت افزاری مهر سازمانی را در اختیار داشته باشد جهت اتصال به سامانه مودیان نیاز به تهیه مهر سازمانی به روش CSR (نرم افزاری) دارد؟

در صورتی که مودی

- گواهی الکترونیکی توکن سخت افزاری منطبق با مشخصات اسناد سامانه مودیان در اختیار داشته باشد.
 - تعداد صورتحساب‌های محدود یا متوسطی داشته باشد.
 - دارای پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی مجهز به قابلیت ارتباط و استفاده از کلید خصوصی موجود در توکن برای امضای صورتحساب‌های الکترونیکی و درخواست‌های ارسالی به سامانه مودیان باشد.
- نیازی به تهیه گواهی دیگری ندارد. در غیر این صورت با توجه به نیاز کسب و کاری و پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی خود، می‌تواند نسبت به تهیه گواهی الکترونیکی مهر سازمانی به روش CSR (نرم افزاری) اقدام نماید. مسئولیت حقوقی نگهداری و حفاظت از کلید خصوصی در این روش صرفاً به عهده مالک گواهی است.

۲۷) جهت اتصال به سامانه مودیان و ارسال صورتحساب‌های الکترونیکی، کدام گواهی

الکترونیکی (توکن سخت افزاری، ماژول نرم افزاری یا HSM) اخذ و استفاده شود؟

مودی با توجه به نیاز کسب و کاری و قابلیت پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی در ارتباط و استفاده از کلید خصوصی مرتبط با گواهی الکترونیکی یکی از روش‌های زیر را برای درخواست و دریافت گواهی الکترونیکی انتخاب می‌کند:

- **توکن سخت افزاری:** با توجه به بررسی‌های صورت گرفته و نظر به اینکه تعداد امضا در ثانیه توکن سخت افزاری حدوداً ۲ می‌باشد، کسب و کارهای کوچک و متوسط با تعداد صورتحساب محدود یا متوسط، می‌توانند از توکن جهت نگهداری کلید خصوصی و ارسال صورتحساب‌های الکترونیکی استفاده نمایند. (لازم به ذکر است جهت استفاده از توکن سخت افزاری می‌بایست پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی قابلیت ارتباط و استفاده از توکن سخت افزاری را داشته باشد).
- **HSM:** با توجه به بررسی‌های صورت گرفته و نظر به اینکه تعداد امضا در ثانیه HSM‌های داخلی ۲۵۰ و بیش از آن می‌باشد، توصیه می‌شود مودیان / شرکت‌های معتمد با تعداد صورتحساب‌های بالا از HSM جهت نگهداری کلید خصوصی و ارسال صورتحساب‌های الکترونیکی استفاده نمایند تا علاوه بر تأمین

امنیت کلید خصوصی، امکان امضای تعداد بیشتری صورتحساب در ثانیه را داشته باشند. شایان ذکر است منعی برای استفاده از HSM برای سایر مودیان وجود ندارد.

- **ماژول رمزنگاری نرم افزاری:** امکان استفاده از این ماژول برای مودیانی است که به دلایل مختلف امکان استفاده از توکن سخت افزاری یا HSM را ندارند این دسته از مودیان می توانند با مسئولیت خود از گواهی های نرم افزاری جهت اتصال به سامانه مودیان و ارسال صورتحساب های الکترونیکی استفاده کرده و کلید خصوصی متناظر با گواهی را در ماژول رمزنگاری نرم افزاری نگهداری نمایند.

مرکز دولتی صدور گواهی الکترونیکی ریشه با توجه به ریسک های امنیتی مورد اشاره در سند «استاندارد ملی الزامات امنیتی پودمان های رمزنگاری زیر ساخت کلید عمومی» که در وبسایت مرکز ریشه به نشانی www.rca.gov.ir موجود است، مؤکداً توصیه می کند مالکان گواهی از ماژول های رمزنگاری سخت افزاری (شامل توکن و HSM) جهت نگهداری کلید خصوصی استفاده نمایند. با این وجود، با توجه به الزامات موجود، امکان نگهداری کلیدهای خصوصی متناظر با گواهی های الکترونیکی سطح ۲ اطمینان در ماژول های رمزنگاری نرم افزاری، با مسئولیت مالک گواهی، وجود دارد.

۲۸) فرایند امضای صورتحساب با استفاده از توکن به چه صورت می باشد؟

- مجهز کردن پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی به قابلیت ارتباط با توکن و استفاده از گواهی الکترونیکی امضای دیجیتال / مهر سازمانی موجود روی آن
- مراجعه به مرکز میانی مورد نظر و اخذ توکن حاوی گواهی الکترونیکی امضای دیجیتال / مهر سازمانی
- استخراج کلید عمومی از گواهی الکترونیکی امضای دیجیتال / مهر سازمانی مطابق با راهنمای استخراج کلید عمومی از امضای دیجیتال / مهر سازمانی که در درگاه سازمان امور مالیاتی کشور به نشانی www.intamedia.ir بارگذاری شده است.
- بارگذاری کلید عمومی استخراج شده از گواهی الکترونیکی امضای دیجیتال / مهر سازمانی در کارپوشه مودیان
- اتصال توکن سخت افزاری به پایانه فروشگاهی / سیستم صدور و ارسال صورتحساب الکترونیکی

- امضای صورت حساب های الکترونیکی و درخواست های ارسالی به سامانه مودیان مطابق با سند دستورالعمل نحوه اتصال به سامانه مودیان که در درگاه سازمان امور مالیاتی کشور به نشانی www.intamedia.ir بارگذاری شده است.

۲۹) مودیان چگونه با استفاده از گواهی نرم افزاری، صورت حساب های الکترونیکی را امضا و به سامانه مودیان ارسال نمایند؟

- تولید کلید خصوصی و فایل درخواست گواهی (CSR) مطابق با دستورالعمل مرکز میانی مورد نظر
- ارسال فایل CSR به مرکز میانی
- دریافت فایل گواهی الکترونیکی امضای دیجیتال/مهر سازمانی از مرکز میانی
- استخراج کلید عمومی از گواهی الکترونیکی امضای دیجیتال/مهر سازمانی مطابق با راهنمای استخراج کلید عمومی از امضای دیجیتال/مهر سازمانی که در درگاه سازمان امور مالیاتی کشور به نشانی www.intamedia.ir بارگذاری شده است.
- بارگذاری کلید عمومی استخراج شده از گواهی الکترونیکی امضای دیجیتال/مهر سازمانی در کارپوشه مودیان
- وارد کردن کلید خصوصی در پایانه فروشگاهی / سیستم صدور و ارسال صورت حساب الکترونیکی مطابق دستورالعمل شرکت تولید کننده پایانه فروشگاهی / سیستم صدور و ارسال صورت حساب الکترونیکی
- امضای صورت حساب های الکترونیکی و درخواست های ارسالی به سامانه مودیان مطابق با سند دستورالعمل نحوه اتصال به سامانه مودیان که در درگاه سازمان امور مالیاتی کشور به نشانی www.intamedia.ir بارگذاری شده است.