

سند راهنمای کارکرد توکن راستین طلایی



مركز تورعه تجارت الكترونيكي



تاریخچه سند

اقدام کننده	آدرس ایمیل	توضيحات	تاريخ	ويرايش
مهيار غلامپور	mahyar@ras.ir	ايجاد	١٣٩٤/١١/٠٤	٠,•١
سمانه على محمديان	samane@rsa.ir	ويرايش	1295/11/+0	•,11
مهيار غلامپور	mahyar@ras.ir	ويرايش	1290/0/17	•,•0
سمانه على محمديان	samane@rsa.ir	ويرايش	1290/+0/17	•,0
شیدا صفائی	sheyda@rsa.ir	ويرايش	1297/07/0	0
اسمعيل فياضى	fayyazi@rsa.ir	ويرايش	1297/07/07	٠,•٩
شیدا صفائی	sheyda@rsa.ir	ویرایش پیش از انتشار	1297/07/0	٠,٩

نمایندگان شرکت جهت ارتباط تجاری و پاسخگویی

پست الکترونیک	شمارہ تماس	سمت	نام ونام خانوادگی	رديف
ima@rsa.ir	$\lambda\lambda$	کارشناس توسعه بازار	ایما امینی	١
Ali.nosrati@rsa.ir	ארורור	کارشناس توسعه بازار	علی نصرتی	٢

حق تأليف:

شركت ره آورد سامانه هاي امن – ره سا، سند حاضر را به منظور ارائه به "مركز توسعه تجارت الكترونيكى " تهيه نموده است. استفاده از اين سند و محتويات آن در راســــــتاى راهنماى استفاده اين محصول مى باشد. اين سند حاوي اطلاعات محرمانه و خصوصي بوده و هرگونه كپي بـــرداري، نــــشر، افشا سازي يا استفاده تجارى از مطالب سند بدون اجازه از شركت ره آورد سامانه هاي امن مجاز نمي باشد.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۲ از ۱۷



فهرست

مقدمه3	()
هدف0	(۲
مراحل نصب0	۳)
کنترل صحت عملکرد توکن و اطلاعات داخل آن۷	٤)
مدیریت گواهی ها۸	(0
نمایش اطلاعات گواهی۹	۲)
افزودن گواهی	(Y
استخراج گواهی	(λ
حذف گواهی	(٩
تغییر نام توکن۱۳	()•
تغيير رمز توکن۳	())
رفع مشکل قفل شدن توکن و فراموش کردن رمز توکن(مخصوص نسخه Admin)۱٤	(۱۲



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۳ از ۱۷

۱) مقدمه

شرکت ره آورد سامانه های امن در سال ۱۳۸۳ با هدف پاسخگوئی به نیاز مبرم کشور در حوزه تأمین امنیت فضای تبادل اطلاعات (افتا) تأسیس شد. موضوع فعالیت شرکت در زمینه تخصصی افتا یعنی تولید سامانه ها، عرضه محصولات و ارائه مشاوره و خدمات در این حوزه به ویژه CA/PKI می باشد.در این مدت، شرکت ره آورد سامانه های امن از پیشگامان عرصه تأمین امنیت اطلاعات و ارتباطات در فضای مجازی و مبدع کاربردها و مفاهیم نو در این زمینه و عرضه تجهیزات و محصولات مربوطه بوده است.

این شرکت با انجام پروژه های ملی و کلیدی متعدد در مقوله امنیت و امضاء الکترونیکی، با سابقه ترین مجموعه کاملا تخصصی و بی رقیب در این حوزه می باشد.

راه اندازی مراکز صدور گواهی الکترونیکی و امضاء دیجیتال، تهیه و ارائه سامانه های راه اندازی و مدیریت مراکز صدور گواهی الکترونیکی(CA/PKI) ،تدوین و ارائه بسته توانا ساز سامانه های کاربردی برای به کارگیری امضاء دیجیتال (PKE) ، ارائه مشاوره و خدمات تخصصی در حوزه افتا، ارائه تجهیزات احراز و تصدیق هویت، تجهیزات رمزیاب و تولید رمز یک بار مصرف(OTP) ، سخت افزارهای شتاب دهنده رمز نگاری و امنیت (HSM و Token) و ... برخی از محصولات و خدمات متنوع امنیتی این شرکت است.

شرکت ره آورد سامانه های امن با بهره گیری از متخصصان و کارشناسان متبحر خود، موفق به ارائه توکن بومی و ایرانی راستین شده است. این توکن ، با امکان استفاده از زیر ساخت کلید عمومی و نگهداری امن کلید خصوصی برای احراز هویت دو عاملي بسیار امن با قابلیت انکارناپذیري می باشد.

توکن بومی راستین با پردازنده قوی ۳۲ بیتی ، سرعت بسیار بالایی در تولید زوج کلید و رمزنگاری و امضای دیجیتال دارد و الگوریتم های بسیار متنوعی را پشتیبانی می کند.

یکی از خصایص بی نظیر این توکن، قابلیت Plug & Play بودن آن است به این معنی که کاربر احتیاج به نصب هیچ گونه نرم افزار یا درایور برای استفاده از این توکن ندارد.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ٤ از ١٧



۲) هدف

سند پیش رو به منظور ارائه سند راهنمای کارکرد راستین طلایی تهیه شده است.

۳) مراحل نصب

با توجه به عملکرد خودکار این نوع توکن ها، به محض اتصال توکن USB به سیستم، راه انداز مربوطه نصب و آیکن آن در کنار ساعت سیستم ظاهر میشود، با دو بار کلیک کردن روی این آیکن، نرم افزار مدیریت توکن اجرا میشود. همچنین می توانید نرم افزار مدیریت توکن را از مسیر زیر اجرا نمایید.





این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه 0 از ۱۷







در صورت غیر فعال بودن AutoRun برای CD-ROM، نصب خودکار نرمافزار مدیریت توکن انجام نمی شود. در این حالت درMyComputer برروی CD-ROM جدید ایجاد شده توسط توکن که با یک آیکون سبز رنگ شبیه به



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ٦ از ١٧

توکن مشخص شده، دوبار کلیک نمایید. در این مرحله نرم افزار مدیریت توکن برروی سیستم شما نصب خواهد شد. دقت کنید که برای کنترل نصب شدن توکن می توانید مراحل بالا را انجام دهید.

کنترل صحت عملکرد توکن و اطلاعات داخل آن

بعد از اطمینان از صحت نصب توکن ، لازم است پیش از استفاده به منظور امضاء در برنامه های مختلف، اطلاعات داخل توکن را کنترل و برای امنیت بیشتر رمز اولیه توکن را تغییر دهید. بدین جهت نرم افزار مدیریت توکن را به طریق مذکور در بخش قبل اجرا نمایید. در پنجره ظاهر شده بر روی دکمه تغییر رمز توکن کلیک کرده و در پنجره باز شده ابتدا رمز قدیمی در قسمت رمز قبلی توکن و سپس رمز جدید مورد نظر را در قسمت رمز جدید توکن و بازنویسی رمز وارد نمایید.

در ادامه برروی دکمه ورود کلیک و رمز توکن را وارد کنید، سپس برروی دکمه تأیید کلیک کنید. توجه داشته باشید که رمز پیش فرض و اولیه توکن ها ۱۲۳٤۵٦۷۸میباشد و این تنها در صورتی است که مرکز صدور گواهی رمز دیگری به شما نداده باشد. دقت نمایید در صورتی که 0 بار رمز ورود را اشتباه وارد کنید، توکن به طور خودکار قفل(block) خواهد شد.

			د به Rastin
مایش داده	وکن به طو <mark>ر</mark> کامل ن	عد از ورود به تر	لاعات داخل توکن به هد شد
		1	رمز توک <mark>ن:</mark>
ى	ن صفحه کلید مجاز	📃 فعال کرد	
لغو	یبد 📄	تا تا	

در صورت ورود رمز اشتباه، پنجره زیر نمایان شده و برای تلاش مجدد باید برروی گزینه بله کلیک کنید :



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۷ از ۱۷



0) مدیریت گواهی ها

پس از ورود موفق به توکن، در سمت راست پنجره و در قسمت لیست توکنها اطلاعات توکن کاربر شامل : نام توکن، نام گواهی مخصوص کاربر (Certificate)، کلید عمومی و کلید خصوصی نمایان خواهد شد. با کلیک روی هر یک از گزینه ها، باید اطلاعات مربوط به آنها در زیر همان قسمت ظاهر شود.

141	ن راستین خوش آمدید	نرم افزار مديريت توكر
خروج افزودت گواهی	F3E6D7329CE5E1186EC0B99F01786D678 کلید(رمزگذاری/رمزگشایی)	لیست توکن ها ۲۰۰۵ مهیار غلامیور 5807221 🗀 55807221 تیادل ک
استخرام گواهی	Mahyar Gholampour [Emai]'s Test-Root-CA بد عمومی بد خصوصی	ی سے ایک کے
حذف	ست، جانات 💌	
	مقدار	فيلد
	Mahyar Gholampour [Email]'s Test-Root-CA ID	نامر گواهی
ىغيير رمز نوكن	E2E6D7220CE5E1196EC0900E01796D67959D7221	نامر مخزن
ىغپىر رمز توكن	F3E007329CE3E1160EC0B99F0176000763607221	all a state of the
نغییر رمز نودن تغییر نام توکن	0A 31 39 38 34 36 38 30 35 39 38 198468 02 4D 61 68 79 61 72 20 47 68 6F 6C 61 6D 70 6F 75	شماره شریان شناسه گواهی
نغییر نام توکن نغییر نام توکن مشاهده گواهی	0A 31 39 38 34 36 38 30 35 39 38 198468 02 4D 61 68 79 61 72 20 47 68 6F 6C 61 6D 70 6F 75	شماره سریان شناسه گواهی



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۸ از ۱۷



در صورتی که تمامی موارد ذکرشده را با دقت کنترل کرده و اطلاعات داخل توکن کامل و درست می باشد، توکن شما به طور صحیح نصب شده و آماده کار با برنامه مورد نظر می باشد.

٦) نمایش اطلاعات گواهی

با کلیک روی نام گواهی بارگذاری شده در توکن و انتخاب آن و کلیک بر روی گزینه "مشاهده گواهی" می توانید اطلاعات گواهی مورد نظر را نمایش دهید.

	ن راستین خوش آمدید	ه ترم افزار مدیریت توکر
خروج		🔖 لیست توکن ها
افزودن گواهی	F3E6D7329CE5E1186EC0B99F01786D678 کلید(رمزگذاری/رمزگشایی) Mahyar Gholampour [Emai]'s Test-Root-CA	مهیار علامیور 5807221 💼 ط تیادل ک آ
استخراج گواهی	ید عمومی ید خصوصی	مبر 24 - ایج کل
حذف	Villo star	
	مقدار	فيلد
تغيير رمز توكن	Mahyar Gholampour [Email]'s Test-Root-CA ID	نام گواهی
	F3E6D7329CE5E1186EC0B99F01786D67858D7221	نام مخزن
تغيير نام توكن	4D 61 68 79 61 72 20 47 68 6F 6C 61 6D 70 6F 75	شماره سریان شناسه گواهی
مشاهده گواهی		



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۹ از ۱۷

ویرایش : ۰٫۰۹ ۹٦/۰٦/۰٦

طبقه بندی : عادی



1900	
Window this cer	s does not have enough information to verify tificate.
Ise	ued to: Mahyar Gholampour [Email]
	ued by: Test-Root-CA
Is	
Is: Va	lid from 5/8/2016 to 5/8/2017

۷) افزودن گواهی

در حال حاضر توکن راستین طلایی قابلیت پشتیبانی از گواهی های نوع P۱۲, PFX, PVB, CRT و CER را دارد، با کلیک روی گزینه افزودن گواهی در صفحه اصلی برنامه طبق شکل زیر می توانید گواهی مورد نظر برای افزودن را انتخاب کنید. اینک قابلیت ایجاد یک مخزن جدید یا انتخاب مخزن موجود را نیز خواهید داشت.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۰ از ۱۷

× 🗆 – 📖	×	ره آورد سامانه های امن - نرم افزار مدیریت توکن را	
ىلايى	دن راستین ط -	انتخاب قایل دواهی برای افرودن به نودن	
خروج		انتخاب فايل	به نرم اوز
		رمز فایل: 	ايس ⊡∼ي
افزودن گواهی)ė
		ا تمام گواهی ها	
استخراج گواهی		🔾 گواهی کاربر	
		انخاب مخنن	
حذف		● المحب المرابعة المامل '\'نباشد)	
			فىلد
تغيير رمز توكن		🔿 استفاده از مخزن موجود:	۔ نام توکر
pa - 12 - 22		F3E6D7329CE5E1186EC0899F01786D67858D7221	سازنده مدل
ىغيير نام بودن			شماره
مثاقده گواهم		نوع:	کل حج حجم خ
ستاهده تواهای		ا تبادل كليد(رمزگذارى/رمزگشايى)	کل حج
			حجم خ

۸) استخراج گواهی

شما می تواند گواهی های موجود روی توکن را همانند شکل زیر از توکن استخراج کنید، توجه کنید که فقط گواهی و کلید عمومی قابل استخراج میباشد و کلید خصوصی به هیچ وجه قابل استخراج نیست.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۱ از ۱۷



۹) حذف گواهی

شما می تواند گواهی های موجود روی توکن را همانند شکل زیر از روی درختواره انتخاب و سپس با زدن کلید حذف آن را حذف کنید.

	ر افزار مدیریت توکن راستین خوش امدین
خروج	يست توكن ها
	ی معیار غلامبور F3E6D7329CE5E1186EC0B99E01786D67858D7221
افزودت کواهی	📄 📄 تبادل کلید(رمزگذاری/رمزگشایی)
	Manyar Gholampour [Email]'s Test-Root-CA ID 🕮 است کلید عمومی
استخراج گواهی	🔤 🎢 کلید خصوصی
حذف	
	ره آورد سامانه های امن - نرم افزار مدیریت توکن راستین ط 💌 🚔
تغيير رمز توكن	
	1 مورد انتخاب شده حذف خواهد شد.
تغيير نام توكن	
مشاهده گواهی	al



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۲ از ۱۷



۱۰) تغییر نام توکن

در حالت کلی وجه تمایز یک توکن شماره سریال آن می باشد اما کاربران توکن این امکان را دارند برای هرتوکن نامی جداگانه انتخاب کنند، برای انجام این کار کافیست همانند شکل زیر از گزینه "تغییر نام توکن" استفاده کنید.

طلایی

ادرار سيريف توص راستين خوس اسين	
ست توک، ها	خروج
ی مهیار غلامبور ۱۹۹۲ - ۲۵۲۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹ - ۲۹۹۹	
⊟™ <u>ا</u> تبادل کلید(رمزگذاری/رمزگشایی)	افزودت گواهی
Mahyar Gholampour [Email]'s Test-Root-CA ID 📴	
سی کید عمومی ۱۹۰۰ کلید خصوصی	استخراج گواهی
ه آورد سامانه های امن - نرم افزار مدیریت توکن راس 🔼	حذف
- Alé I	دزئيات 💌
محيير نام شهيار عدشهور.	م تغییر رمز توکن
لطفا در انتهاک نام، حرف خالی استفاده نشود	
مهيار غلاميور	تغییر نام توکن
تاسد لغه	
	مشاهده گواهم
تجم حافظه خصو 15000	

۱۱) تغییر رمز توکن

شما می توانید با کلیک روی کلید"تغییر رمز توکن" رمز یا پین کد توکن خود را مطابق شکل زیر تغییر دهید.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۳ از ۱۷

سنین طلایی	
	په نرم افزار مدیریت توکن راستین خوش آمدین
خروح افزودن گو	کی لیست توکن ها ⊶کی مهیار غلامبور Grie 53E6D7329CE5E1186EC0B99F01786D6785D221 ⊡-⊡ تیادل کلید(رمزگذاری/رمزگشایی)
استخراج گ	Manyar Gnolampour [Email] s Test-Root-CA ID 🗃 کلید عمومی بید خصوصی
حذف	ره آورد سامانه های امن - نرم افزار مدیریت توکن راس 🗙
تغییر رمز آ	تغییر رمز مهیار غلامپور فیا نام رمز قبلی توکن:
al2 - 61	س مد رمز جدید توکن:
	ش 🛛 🖳 کنترل امنیت رمز

۱۲) رفع مشکل قفل شدن توکن و فراموش کردن رمز توکن(مخصوص نسخه Admin)

در صورتی که توکن شما قفل شده باشد، می توانید برای قفل گشایی توکن از نرم افزار مدیریت توکن نسخه Admin استفاده نمایید. بدین جهت نرم افزار مربوطه را از پشتیبانی رهآورد سامانه های امن بخواهید .

پس از اجرای نسخه Admin، نسخه مدیریتی پنجره مدیریت توکن نمایان خواهد شد.

در این پنجره برروی دکمه فلش در سمت راست و بالای کلید بستن نرم افزار کلیک کنید. در ادامه بر روی دکمه بازگشایی قفل ظاهر شده کلیک نمایید.

سپس در پنجره نمایان شده در قسمت رمز مدیر عبارت " rastin " را وارد نمایید. لازم به ذکر است که عبارت مذکور باید با حروف کوچک وارد شود. در مرحله بعد رمز جدید مورد نظر را در قسمتهای "رمز جدید" و "بازنویسی رمز" وارد نموده و در انتها بر روی دکمه تأیید کلیک کنید.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۶ از ۱۷



ویرایش : ۰٫۰۹ ۹٦/۰٦/۰٦

کی مقبار غلامیور		9,92
		افزودن گواهی
		استخراج گواهی
	بستن	جزئیات 💌
فيلد	مقدار	تغيير روز توکن
ام توکن	مهيار غلامپور	
سازنده	ساماته های امن	
ىدل	طلایی	تغيير نام توكن
مايد بيالي	0628350301150515	
	30000	
کل حجم حافظه عمومی	27728	مشاهده گواهی
سیاره شریان کل حجم حافظه عمومی حجم خالی حافظه عم	2//20	
کل حجم حافظه عمومی حجم خالی حافظه عم کل حجم حافظه خمو	15000	
کل حجم حافظه عمومی حجم خالی حافظه عمومی کل حجم حافظه خمو حجم خالی حافظه خ	15000 14587	

بازگشایی قفل	_		🐞 لیست توکن ها اسې مهیار غلامپور
باكسازى اوليه			
	بستن جریان پ	1.2.	
		معدار	فيلد
تغيير رمز مدير توكن		مهيار غلامپور	نام توکن
		سامانه های امن 	سازنده
		طلایی	مدل
		• ۶۲۸۳۵•۳•11۵•۵1۵	شماره سريال
I		7++++	کل حجم حافظه عمومی
		TVVTA	حجم خالی حافظه عم
			1 - 1 61
		10	دل حجم حافظه حصو
		ια ιταλν	دل حجم حافظه حصو حجم خالی حافظه خ



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۵ از ۱۷

ویرایش : ۰٫۰۹ ۹٦/۰٦/۰٦	سند راهنمای کارکرد توکن راستین مرکزومه تجارت المرزیکی طلایی
	ره آورد سامانه های امن - نرم افزار مدیریت توکن راس 🗙 بازکردن قفل Rastin Platinum.
	رمز مدیر: 1
	رمز جديد: کنترل امنیت رمز بانتفسیم درمز:
	برویستای زمر: فعال کردن صفحه کلید مجازی تائید لغو

در صورت ورود صحیح **رمز مدیر**، پنجره زیر نمایان خواهد شد.

	عملیات رفع قفل توکن با موفقیت انجام شد! برای ادامه لطفا مجددا وارد توکن شوید.
تائيد	

در غیر این صورت پنجره پیغام خطای زیر نمایان خواهد شد.





این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۲ از ۱۷



توجه داشته باشید که تنها 0 مرتبه می توانید **رمز مدیر** را اشتباه وارد کنید و اگر بیش از 0 بار مرتکب خطا شوید، توکن دچار (**قفل شدگی رمز مدیر**) خواهد شد و دیگر امکان استفاده از گواهی و زوج کلید داخل توکن میسر نیست. در این صورت باید به مرکز مربوطه (مرکز صدور گواهی) مراجعه فرمایید تا توکن شما را **پاکسازی اولیه** کرده و مجدداً برای شما گواهی صادر نمایند.



این سند حاوی مطالب محرمانه و اختصاصی شرکت سامانههای امن بوده و هر گونه نشر, کپی برداری, انتقال به غیر و افشا سازی محتویات آن بدون اجازه از شرکت مجاز نمی باشد.

صفحه ۱۷ از ۱۷