



جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

مرکز توسعه تجارت الکترونیکی

مرکز صدور کواهی الکترونیکی میانی عام

General Intermediate Certification Authority

راهنمای پروفایل گواهی در تولید CSR

طبقه بندی: عادی

شناسه سند: GICA.SW.User.CertProfilev0.4

شماره بازنگری: ۰,۴

تاریخ بازنگری: ۱۴۰۰/۰۴/۱۶



طبقه‌بندی: عادی	شناسه سند: ICA.SW.User.CertProfilev0.4	شماره بازنگری: ۰,۴	تاریخ بازنگری: ۱۴۰۰/۰۴/۱۶
-----------------	--	--------------------	---------------------------

فهرست مطالب

- ۲..... نامگذاری گواهی موجودیت نهایی
- ۲..... نامگذاری گواهی الکترونیکی امضا شخص حقیقی
- ۳..... نامگذاری گواهی الکترونیکی امضا شخص حقوقی
- ۴..... نامگذاری گواهی الکترونیکی دفتر ثبت نام
- ۵..... فایل تنظیمات ایجاد درخواست گواهی
- ۷..... ایجاد فایل pfx یا p12 از گواهی صادر شده



نامگذاری گواهی موجودیت نهایی

نامگذاری گواهی الکترونیکی امضا شخص حقیقی

Row	Field	Type ^۱	Status	value	Language
۱	C	Gov NGO Una	اجباری	IR	En
۲	O	Gov	اجباری	Governmental	En
		NGO	اجباری	Non-Governmental	En
		Una	اجباری	Unaffiliated	En
۳	OU	Gov NGO	اجباری	نام سازمان	Fa
۴	OU	Gov NGO	اختیاری	نام واحد سازمانی ۱	All
۵	OU	Gov NGO	اختیاری	نام واحد سازمانی ۲	All
۶	OU	Gov NGO	اختیاری	نام واحد سازمانی ۳	All
۷	CN	Gov NGO Una	اجباری	Name Family [Sign]	En
۸	E	Gov NGO Una	اختیاری	Email Address	-
۹	SERIALNUMBER	Gov NGO Una	اجباری	کد (شناسه) ملی متقاضی	All
۱۰	SN	Gov NGO Una	اجباری	نام خانوادگی متقاضی	Fa
۱۱	G	Gov NGO Una	اجباری	نام متقاضی	Fa
۱۲	T	Gov NGO	اجباری	نقش یا سمت متقاضی در سازمان	All
۱۳	S	Gov NGO Una	اجباری	نام استان	Fa
۱۴	L	Gov NGO Una	اجباری	نام شهرستان	Fa
۱۵	OrganizationIdentifier ^۲	Gov NGO	اجباری	شناسه سازمان	All

^۱ در ستون Type منظور از Una (شخص حقیقی مستقل Unaffiliated)، NGO (شخص حقیقی وابسته به غیر دولت) و Gov (شخص حقیقی وابسته به دولت) می‌باشد. اگر برای یکی از فیلدها ذکر نشد به معنای عدم وجود فیلد مذکور در آن نوع گواهی می‌باشد.

^۲ در تولید فایل CSR بجای نام فیلد OrganizationIdentifier باید از شناسه ۲,۵,۴,۹۷ استفاده گردد و مقدار آن برابر با شناسه سازمان باشد.



نامگذاری گواهی الکترونیکی امضا شخص حقوقی

Row	Field	Type ^۳	Status	Value	Language
۱	C	Gov NGO	اجباری	IR	En
۲	O	Gov	اجباری	Governmental	En
		NGO	اجباری	Non-Governmental	En
۳	OU	Gov NGO	اجباری	نام سازمان	Fa
۴	OU	Gov NGO	اختیاری	نام واحد سازمانی ۱	All
۵	OU	Gov NGO	اختیاری	نام واحد سازمانی ۲	All
۶	OU	Gov NGO	اختیاری	نام واحد سازمانی ۳	All
۷	CN	Gov NGO	اجباری	Organization Unit [Stamp] نام کامل سازمان	En
۸	E	Gov NGO	اختیاری	پست الکترونیکی شخص حقوقی	All
۹	SERIALNUMBER	Gov NGO	اجباری	شناسه ملی شخص حقوقی (شناسه ملی شرکت)	All

^۳ در ستون Type منظور از Una (شخص حقیقی مستقل Unaffiliated)، NGO (شخص حقیقی وابسته به غیر دولت) و Gov (شخص حقیقی وابسته به دولت) می‌باشد. اگر برای یکی از فیلدها ذکر نشد به معنای عدم وجود فیلد مذکور در آن نوع گواهی می‌باشد.



نامگذاری گواهی الکترونیکی دفتر ثبت نام

Row	Field	Type ^۴	Status	Value	Language
۱	C	Gov NGO	اجباری	IR	En
۲	O	Gov	اجباری	Governmental	En
		NGO	اجباری	Non-Governmental	En
۳	OU	Gov NGO	اجباری	نام دفتر ثبت نام	Fa
۴	OU	Gov NGO	اختیاری	نام واحد سازمانی ۱	All
۵	OU	Gov NGO	اختیاری	نام واحد سازمانی ۲	All
۶	OU	Gov NGO	اختیاری	نام واحد سازمانی ۳	All
۷	CN	Gov NGO	اجباری	RaName. RA [National Code] نام دفتر ثبت نام [کد ملی]	En
۸	SERIALNUMBER	Gov NGO	اجباری	شناسه دفتر ثبت نام	En
۹	S	Gov NGO	اجباری	نام استان	Fa
۱۰	L	Gov NGO	اجباری	نام شهرستان	Fa
۱۱	Surname	Gov NGO	اجباری	نام خانوادگی	Fa
۱۲	GivenName	Gov NGO	اجباری	نام	Fa

^۴ در ستون Type منظور از Una (شخص حقیقی مستقل Unaffiliated)، NGO (شخص حقیقی وابسته به غیر دولت) و Gov (شخص حقیقی وابسته به دولت) می‌باشد. اگر برای یکی از فیلدها ذکر نشد به معنای عدم وجود فیلد مذکور در آن نوع گواهی می‌باشد.

فایل تنظیمات ایجاد درخواست گواهی

مثال: گواهی مهر سازمانی

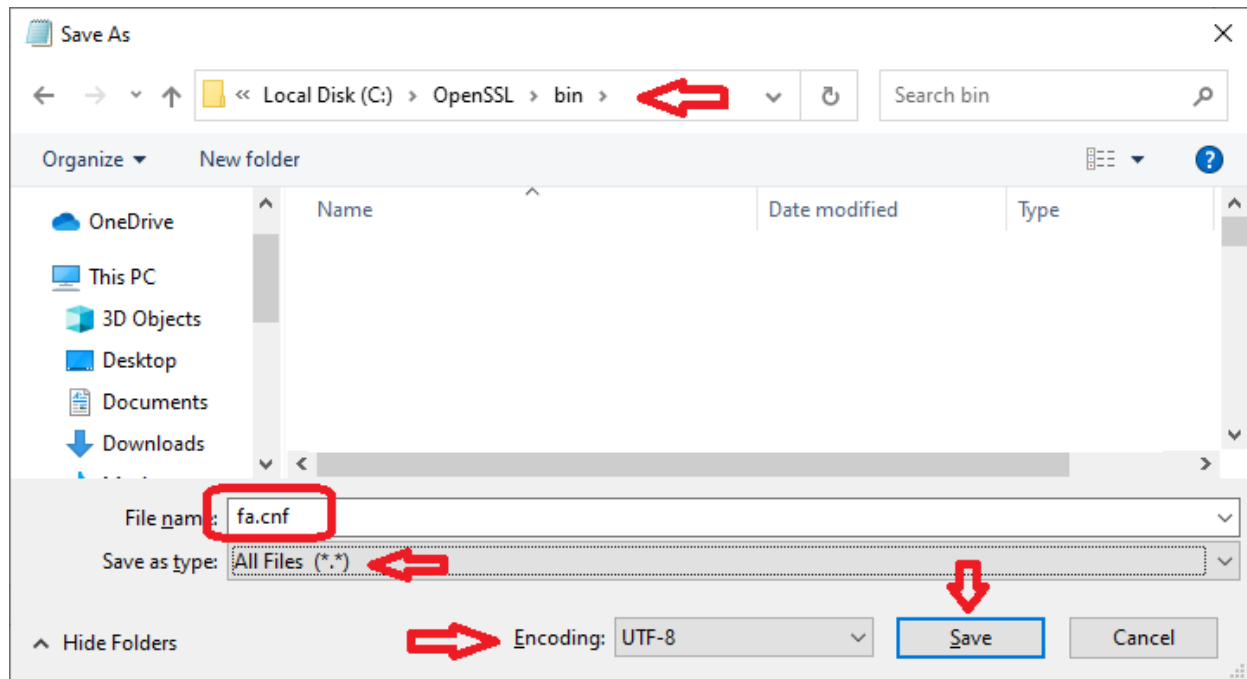
برای ایجاد فایل درخواست گواهی، یک فایل به نام fa.cnf با استفاده از نرم افزار Notpad با مشخصات زیر ایجاد نمایید:

Path: C:\OpenSSL\bin

File Name: fa.cnf

Save as type: All Files (*.*)

Encoding: UTF-8



سپس فایل ایجاد شده را با نرم افزار Notpad باز نموده و مقادیر مشخص شده را با مشخصات سازمان/شرکت خود مطابق جدول تکمیل نمایید.



```
[req]
prompt = no
distinguished_name = dn
```


```
[dn]
CN = Value1 [Stamp]
serialNumber = Value2
O = Value3
3.OU = Value4
2.OU = Value5
1.OU = Value6
C = Value7
```

Field	Type ^a	Status	Value	Language
Value1	Gov NGO	اجباری	نام سازمان به انگلیسی	En
Value2	Gov NGO	اجباری	شناسه 11 رقمی سازمان	En
Value3	Gov	اجباری	Governmental	En
	NGO	اجباری	Non-Governmental	En
Value4	Gov NGO	اختیاری	نام واحد سازمانی ۲	All
Value5	Gov NGO	اختیاری	نام واحد سازمانی ۱	All
Value6	Gov NGO	اختیاری	نام سازمان	Fa
Value7	Gov NGO	اجباری	IR	En

دکمه های **R +** را با هم فشار دهید تا پنجره Run باز شود سپس دستور CMD را تایپ نموده و دکمه Enter را فشار دهید تا صفحه فرمان باز شود. سپس با دستورات زیر خط فرمان را در شاخه نصبی openssl قرار دهید:

```
CD \
CD Openssl\bin
```

^a در ستون Type منظور از Una (شخص حقیقی مستقل Unaffiliated)، NGO (شخص حقیقی وابسته به غیر دولت) و Gov (شخص حقیقی وابسته به دولت) می‌باشد. اگر برای یکی از فیلدها ذکر نشد به معنای عدم وجود فیلد مذکور در آن نوع گواهی می‌باشد.

راهنمای پروفایل گواهی در تولید CSR			
طبقه‌بندی: عادی	شناسه سند: ICA.SW.User.CertProfilev0.4	شماره بازنگری: ۰,۴	تاریخ بازنگری: ۱۴۰۰/۰۴/۱۶

در خط فرمان دستور زیر را اجرا نمایید.

```
openssl req -new -utf8 -nameopt multiline,utf8 -config fa.cnf -newkey rsa:2048 -nodes -keyout fa.key -out fa.csr
```

با اجرای این دستور یک فایل به نام **fa.csr** و یک فایل به نام **fa.key** ایجاد می شود که به ترتیب فایل درخواست گواهی و کلید گواهی می باشد.
فایل **fa.csr** را در اختیار مرکز صدور گواهی الکترونیکی قرار دهید تا گواهی شما مطابق با فایل **config** صادر شود.

ایجاد فایل **pfx** یا **p12** از گواهی صادر شده

بعد از گرفتن گواهی صادر شده، آن را به **fa.cer** تغییر نام دهید و سپس در مسیر **C:\OpenSSL\bin** کپی نمایید.
توجه: گواهی باید به فرمت **base 64 encoded X.509(.cer)** ذخیره شده باشد.
وارد خط فرمان **openssl** شاخه **bin** شوید و دستور زیر را اجرا نمایید:

```
openssl pkcs12 -export -out fa.pfx -inkey fa.key -in fa.cer
```

یا

```
openssl pkcs12 -export -out fa.p12 -inkey fa.key -in fa.cer
```

با اجرای دستور، برای دسترسی به کلید از شما درخواست رمز می شود. بعد از تکرار رمز فایل خروجی **fa.pfx** یا **fa.p12** می باشد.