



جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

مرکز توسعه تجارت الکترونیکی

مرکز صدور گواهی الکترونیکی میانی عام

General Intermediate Certification Authority

راهنمای ساخت CSR بر اساس پروفایل گواهی

طبقه بندی: عادی

شناسه سند: GICA.SW.User.CertProfilev1.0

شماره بازنگری: ۱.۰

تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵

فهرست مطالب

۲.....	مقدمه.
۳.....	۱- نصب برنامه openssl
۴.....	۲- ایجاد درخواست گواهی (CSR)
۸.....	۳- تولید فایل . pfx
۱۰.....	پیوست ها: نامگذاری گواهی موجودیت نهایی
۱۰.....	پیوست ۱: نامگذاری گواهی الکترونیکی امضا شخص حقیقی
۱۱.....	پیوست ۲: نامگذاری گواهی الکترونیکی امضا شخص حقوقی
۱۲.....	پیوست ۳: نامگذاری گواهی الکترونیکی دفتر ثبت نام

راهنمای ساخت CSR بر اساس پروفایل گواهی			
تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵	شماره بازنگری: ۱.۰	شناسه سند: GICA.SW.User.CertProfilev1.0	
طبقه‌بندی: عادی			

مقدمه

این سند به تشریح فرایند تولید درخواست گواهی (Certificate Signing Request (CSR و الزامات فنی مرتبط با ایجاد کلید می پردازد.

لازم است فایل درخواست گواهی (CSR) بر حسب نوع در خواست گواهی مورد نیاز بر اساس پیوست مقداردهی شود.

مراحل اجرا برای تولید فایل csr به ترتیب زیر می باشد:

۱. نصب برنامه OpenSSL
۲. ایجاد درخواست گواهی (CSR)
 - a. ایجاد فایل پیکربندی
 - b. اجرای دستورات openssl
 - c. تولید CSR
۳. تولید فایل pfx

۱- نصب برنامه openssl

۲- برنامه OpenSSL را از آدرس www.gica.ir، صفحه دانلود، دریافت نمایید.

۳- فایل دریافتی را به مسیر درایو C: منتقل نمایید.

۴- فایل فشرده را از حالت زیپ خارج نمایید.





۲-

ایجاد درخواست گواهی (CSR)

a. ایجاد فایل پیکربندی

۱. در محل نصب نرم افزار OpenSSL برای مثال پوشه (C:\openssl) یک فایل متنی جدید ایجاد نمایید.

۲. محتوای زیر مربوط به درخواست گواهی مهر سازمانی وابسته به غیر دولت می باشد آن را در یک فایل متنی (notepad) قرار داده و اطلاعات مربوط به سازمان خود را در بخش های مشخص شده (موارد قرمز رنگ) ویرایش نمایید.

```
[req]
prompt = no
distinguished_name = dn
[dn]
CN = MyCompany [Stamp]      نام سازمان به انگلیسی
serialNumber = shenase      شناسه ملی ۱۱ رقمی سازمان
O = Non-Governmental          برای شرکت های دولتی #Governmental
3.OU = company department    واحد سازمانی
2.OU = company department    واحد سازمانی
1.OU = company department    نام سازمان به فارسی
L= Tehran                    نام شهر به فارسی
ST= Tehran                  نام استان به فارسی
C = IR
```

تذکر: فیلدهایی مثل 2.OU و 3.OU اختیاری بوده و میتوانید در صورتی که واحد سازمانی ندارید خط مربوطه را حذف نمایید.

نمونه محتوای فایل csr با استفاده از دستور بالا:

```
[req]
prompt = no
distinguished_name = dn
[dn]
CN = Iran Center for Ecommerce Development [Stamp]
serialNumber = 14000405500
```

O = Non-Governmental

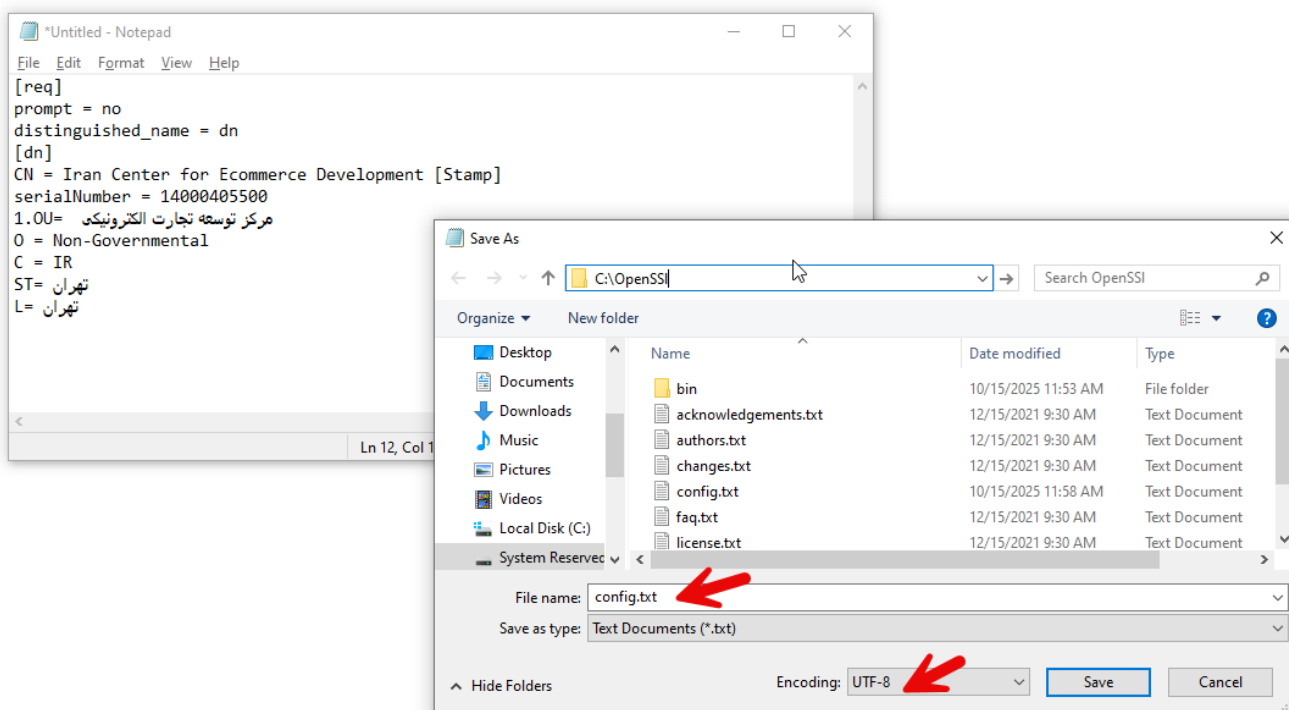
1.OU= مرکز توسعه تجارت الکترونیکی

L= تهران

ST= تهران

C = IR

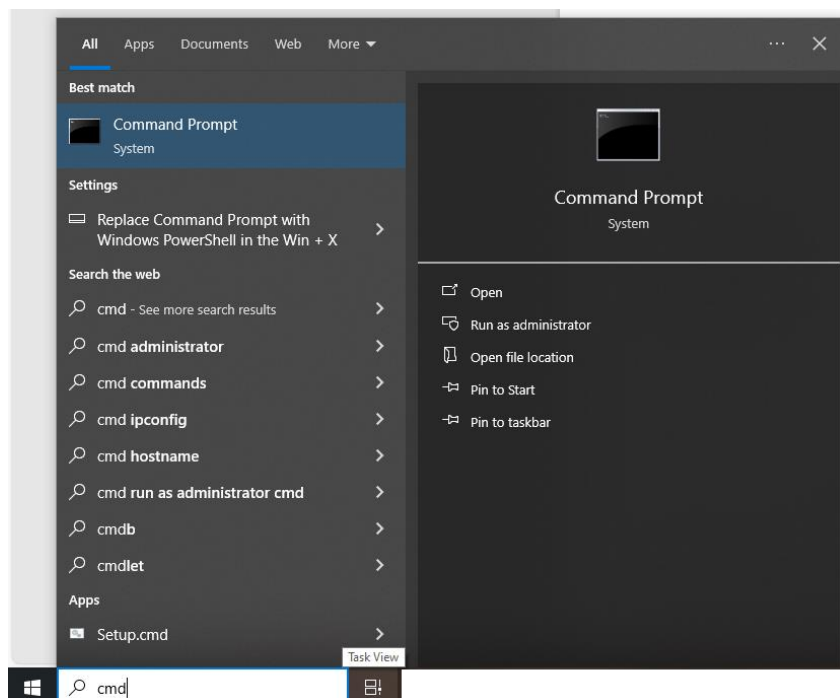
۱. فایل را به صورت utf8 و با نام config.txt ذخیره نمایید.



b. اجرای دستورات Openssl

۱. باز کردن CMD یا PowerShell

- روی پنجره ویندوز کلیک نموده و «cmd» را جستجو و اجرا نمایید.



۲. تغییر مسیر اجرای دستورات

مسیر کامل فایل openssl.exe در پوشه نصب نرم افزار (C:\openssl\bin\openssl.exe) قرار دارد. در CMD (یا PowerShell)، دستور زیر را اجرا نمایید.

```
cd /d "C:\Openssl\bin"
```

۳. تولید CSR

جهت ایجاد فایل CSR، دستور زیر را وارد نمایید در این دستور فایل کلید خصوصی و CSR ایجاد می گردد.

```
openssl req -new -utf8 -config "C:\openssl\config.txt" -newkey rsa:2048 -keyout mykey.key -out mycsr.txt
```

ورودی	"C:\openssl\config.txt"	آدرس فایل تنظیمات
خروجی	mykey.key	کلید خصوصی
خروجی	mycsr.txt	فایل درخواست گواهی CSR

با اجرای این دستور، رمز کلید خصوصی از کاربر دریافت می گردد.

جهت تولید کلید عمومی از کلید خصوصی در دستور قبل، دستور زیر اجرا گردد

راهنمای ساخت CSR بر اساس پروفایل گواهی



مرکز واسطه‌سازی گواهی
General Intermediary Certification Authority

طبقه‌بندی: عادی

شناسه سند GICA.SW.User.CertProfilev1.0

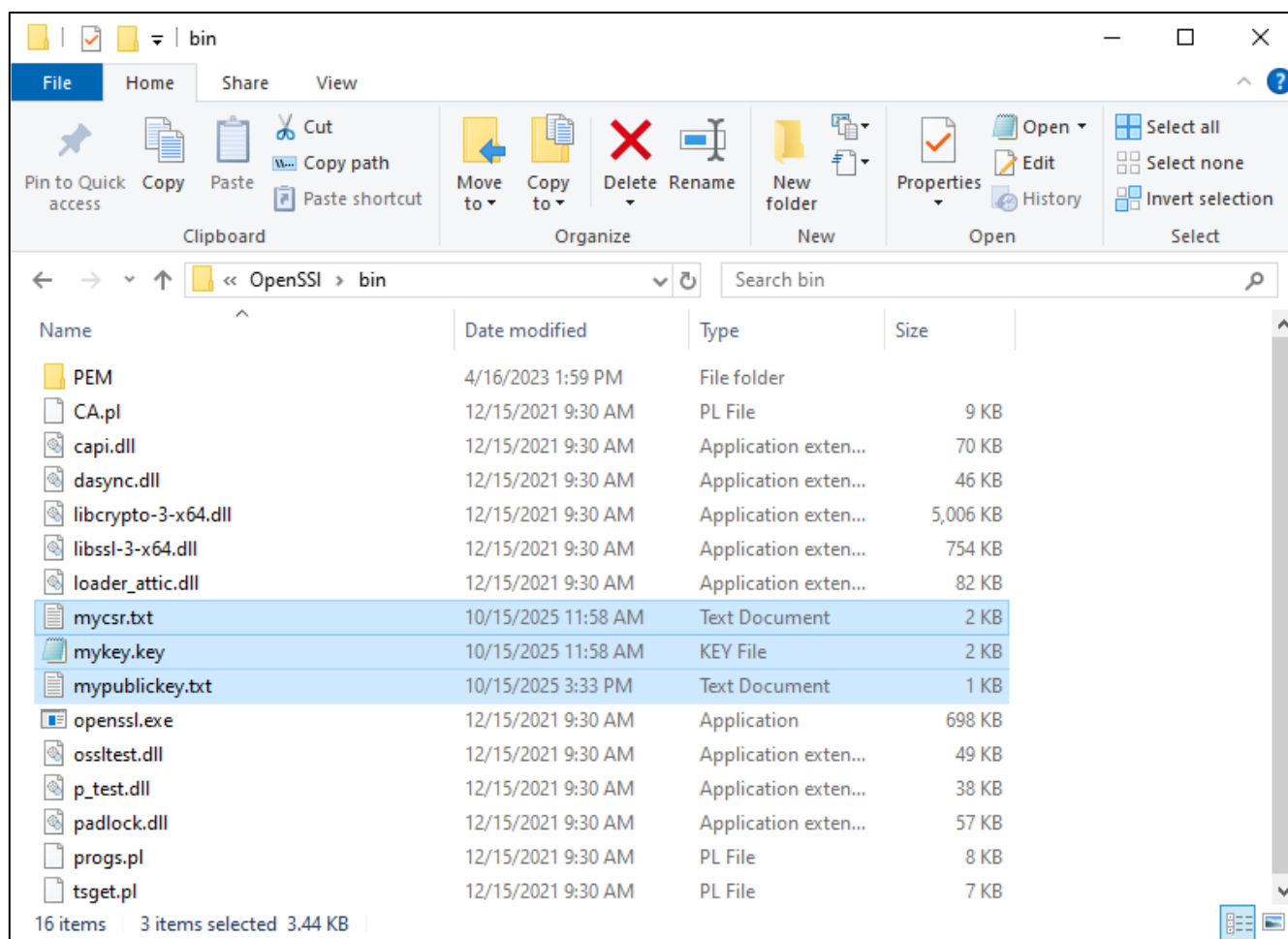
شماره بازنگری: ۱.۰

تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵

openssl rsa -in mykey.key -pubout -out mypublickey.txt		
ورودی	mykey.key	کلید خصوصی
خروجی	mypublickey.txt	کلید عمومی

در این مرحله رمز وارد شده در مرحله قبل از کاربر درخواست می‌گردد.

تذکر: فایل های خروجی دستور در مسیر پوشه C:\openssl\bin ایجاد می شوند.



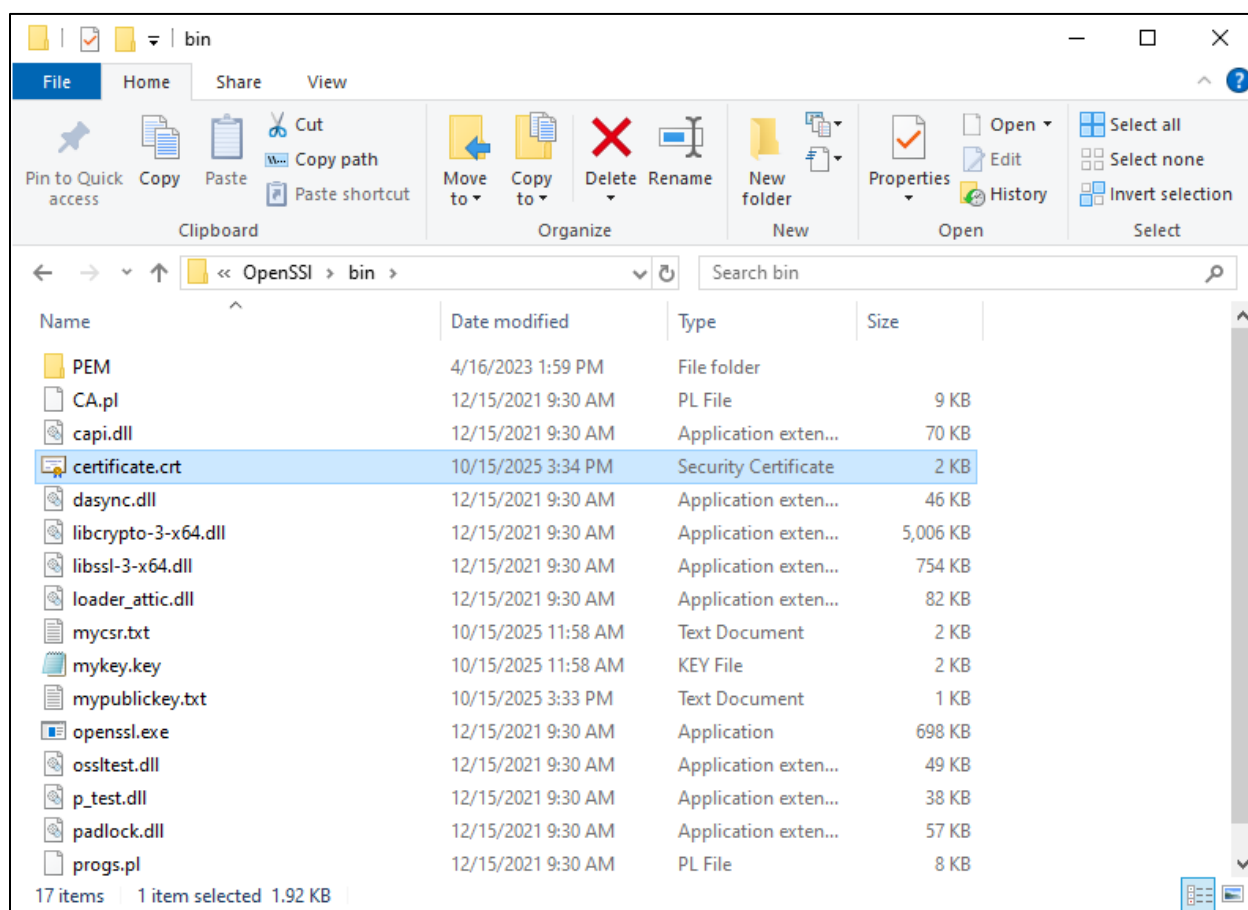
- فایل mycsr.txt فایل csr می باشد.
- فایل mykey.key همان کلید خصوصی است که باید محرمانه بماند.
- فایل mypublickey.pem شامل کلید عمومی خواهد بود.



< توجه: فایل کلید خصوصی باید به صورت محرمانه نگهداری شده و در اختیار اشخاص غیرمجاز قرار نگیرد.

تولید فایل pfx

بعد از اخذ گواهی از یکی از مراکز صدور گواهی، فایل گواهی را کنار کلیدها در مسیر نصب قرار دهید.



- فرمان زیر را در مسیر نصب openssl اجرا نمایید.

openssl pkcs12 -export -inkey mykey.key -in certificate.crt -out keystore.pfx		
ورودی	certificate.crt	فایل گواهی صادر شده
ورودی	mykey.key	کلید خصوصی
خروجی	keystore.pfx	حاوی کلید خصوصی و گواهی

توجه: برای ایجاد فایل pfx از رمز عبور قوی استفاده نموده و آن را امن نگه دارید.

 Command Prompt

(c) Microsoft Corporation. All rights reserved.

```
C:\OpenSSL\bin>openssl req -new -utf8 -config "C:\openssl\config.txt" -newkey rsa:2048 -keyout mykey.key -out mycsr.txt
```

[illegible]

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

```
C:\OpenSSL\bin>openssl rsa -in mykey.key -pubout -out mypublickey.txt
```

Enter pass phrase for mykey.key:

writing RSA key

```
C:\OpenSSL\bin>openssl pkcs12 -export -inkey mykey.key -in certificate.crt -out keystore.pfx
```

Enter Export Password:

Verifying - Enter Export Password:

```
C:\OpenSSL\bin>
```

راهنمای ساخت CSR بر اساس پروفایل گواهی



مرکز واسطه‌سازی گواهی‌های عمومی
General Intermediary Certification Authority

طبقه‌بندی: عادی

شناسه سند GICA.SW.User.CertProfilev1.0

شماره بازنگری: ۱.۰

تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵

پیوست ها: نامگذاری گواهی موجودیت نهایی

پیوست ۱: نامگذاری گواهی الکترونیکی امضا شخص حقیقی

Row	Field	Type ¹	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 ²	Gov NGO	اجباری	شناسه سازمان	All

¹ در ستون Type منظور از Una (شخص حقیقی مستقل)، 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.

2 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.

راهنمای ساخت CSR بر اساس پروفایل گواهی



مرکز واسطه‌گری گواهی‌های دیجیتال
General Intermediary Certification Authority

طبقه‌بندی: عادی

شناسه سند GICA.SW.User.CertProfilev1.0

شماره بازنگری: ۱.۰

تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵

پیوست ۲: نامگذاری گواهی الکترونیکی امضا شخص حقوقی

Row	Field	Type ³	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
۱۰	S	Gov NGO	اجباری	نام استان	Fa
۱۱	L	Gov NGO	اجباری	نام شهرستان	Fa

³ 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 ساخت CSR بر اساس پروفایل گواهی



مرکز واسطه‌سازی گواهی‌های دیجیتال
General Intermediary Certification Authority

طبقه‌بندی: عادی

شناسه سند GICA.SW.User.CertProfilev1.0

شماره بازنگری: ۱.۰

تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵

پیوست ۳: نامگذاری گواهی الکترونیکی دفتر ثبت نام

Row	Field	Type ⁴	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

⁴ در ستون Type منظور از Una (شخص حقیقی مستقل)، 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.