**راهنمای نصب و راه اندازی درگاه امضای دیجیتال (ISG)** 

前州而州、瓦公长而(前州、 而人们ヨー川トー「「「「「「「「「「「」」」 卡(公下面)公司公司长面 小公下面、国人间、订长雨 ヨーハインドアーゴノアーズアー

شركت يندار كوشك ايمن

واحد امنيت اطلاعات و زيرساخت كليد عمومي

| نسخه:     | 1,+                     |
|-----------|-------------------------|
| تاريخ:    | شهریور ۱۴۰۰             |
| شناسه:    | KI-ISG-Deployment-Guide |
| طبقەبندى: | عمومى                   |

راهنمای نصب و راه اندازی ISG شرکت پندار کوشک ایمن



## تاريخچه گزارش

| توضيحات        | مرور کننده/گان | تهيه کننده /گان          | تاريخ    | نسخه |
|----------------|----------------|--------------------------|----------|------|
| آماده سازی سند | مدیر فنی       | کارشناس نصب و راه اندازی | 14/.8/77 | ١,٠  |





## فهرست مطالب

| ٩                                 | مقدم   | ۱. |
|-----------------------------------|--------|----|
| ندیهای نرم افزاری                 | نيازمن | ۲. |
| نیازمندیها                        | . ساير | ۳. |
| گام به گام                        | نصب    | ۴. |
| پیش نیازهای نصب۴                  | ۴,۱    |    |
| نصب پایگاه داده۴                  | F,T    |    |
| تنظیمات دسترسی به پایگاه داده۷    | ۴,۳    |    |
| ایجاد سامانه جدید در IIS          | 1 4,4  |    |
| ایجاد برنامه کاربردی در یک سامانه | ۴,۵    |    |
| اعمال تنظيمات سامانهها            | 1 4,9  |    |

PKI-ISG-Deployment-Guide



#### ۱. مقدمه

این مستند به صورت اختصاصی برای کارشناسان نصب و راه اندازی سامانههای تحت IIS تهیه شده است و قدر مسلم نیاز به دانش اولیه مرتبط با نصب و راه اندازی سامانههای تحت وب دارد.

در این مستند مراحل انتقال برنامه نصب به IIS و اعمال تنظیمات مربوط، به صوررت گام به گام توضیح داده شده است. درگاه امضای دیجیتال شامل ۴ سامانه مستقل است:

- ۱. سامانه درگاه امضای دیجیتال (ISG UI)
- ۲. سرویس REST در گاه امضا (ISG REST)
- ۳. سرویس SOAP درگاه امضا (ISG SOAP)
- ۴. سامانه مدیریت درگاه امضا (ISG Admin)

**نکته**: سرویسهای در گاه امضا میتوانند به صورت سامانهای مستقل یا به صورت یک برنامه کاربردی درون سامانه در گاه امضا نصب شوند. تصمیم گیری در این مورد وابسته به سیاستهای سازمانی بهره بردار است.

# ۲. نیازمندیهای نرم افزاری

|                | OS   |  | Web Server  |  |
|----------------|--|--|---|--|
| Windows Server | 2016 or upper (64-bit)   | <ul> <li>Server Roles: IIS</li> <li>Features: <ul> <li>.NET Framework 4.6.1 (or higher features, depend on OS version)</li> </ul> </li> <li>WCF Services <ul> <li>HTTP Activation</li> <li>Named Pipe Activation</li> <li>TCP Activation</li> <li>TCP Port Sharing</li> </ul> </li> <li>IIS Hostable Web Core</li> </ul> |   |  |
|                |  | مشخصات پایگاه داده   |   |  |
| DB Engine      | F  | eatures  | User  |  |
| MS SQL 2019    | Instance Features:<br>• Database Eng<br>• Full-Text an<br>Search<br>Shared Features:<br>• Client Tools<br>• SQL Client C | gine Services<br>d Semantic Extractions for<br>Connectivity<br>Conectivity SDK   | A login to a database called ISG, that<br>has:<br>Owned Schemas: db_owner<br>Membership: db_owner |  |

PKI-ISG-Deployment-Guide



| سایر نرم افزارهای مورد نیاز  |                                  |  |  |  |  |
|------------------------------|----------------------------------|--|--|--|--|
| Softwate                     | Version                          |  |  |  |  |
| SQL Server Management Studio | 18 or Upper                      |  |  |  |  |
| Notepad++                    | Any version with Compare Plugins |  |  |  |  |

### ۳. سایر نیازمندیها

| توضيحات                                    | پورتھا | به مقصد  | از مبدا                 |
|--|--------|--|-------------------------|
| سرور مقصد متعلق به شرکت پندار بوده و ارایه | ٨٠     | ۲۱۲,۱۶,۷۰,۲۱                                   | آی پی سرور ISG          |
| دهنده خدمات اطلاع رساني توسط تلفن همراه    | 444    |  |                         |
| است.                                       |        |  |                         |
| جهت مراجعه امضا کنندگان به درگاه امضا      | ٨٠     | آی پی سرور ISG                                 | از هر نشانی اینترنتی    |
|  | 444    |  |                         |
| جهت مراجعه مدیر درگاه امضا                 | ٨٠٨٠   | آی پی سرور ISG                                 | از هر نشانی اینترنتی یا |
|  | ٨٠٨١   |  | نشانی شبکه داخلی        |
| Google Auth                                |        | https://accounts.google.com<br>/o/oauth2/auth  | آی پی سرور ISG *        |
| Google Ttoken                              |        | https://oauth2.googleapis.co<br>m/token        | آی پی سرور ISG *        |
| Google Auth Provider X509 Cert             |        | https://www.googleapis.co<br>m/oauth2/v1/certs | آی پی سرور ISG *        |
|  |        | https://www.googleapis.co                      | آی پی سرور ISG *        |
| Google Client X509 Cert                    |        | m/robot/v1/metadata/x509/f                     |                         |
| Google Chent A507 Cert                     |        | zn8t9%40pendarnotificatio                      |                         |
|  |        | n.iam.gserviceaccount.com                      |                         |

• دسترسیهای دایم اینترنت

\* سرویس های گوگل به منظور پیام رسانی به تلفن های همراه اندروید استفاده می شود. در ارتباط با این سرویس ها ۳ رویکرد امکان پذیر است:

- I ایجاد حساب کاربری بهره بردار در مجموعه سرویسهای Firebase برای بهره بردارانی که امکان دسترسی به این سرویسها را دارند. مالک این حساب کاربری، بهره بردار خواهد بود.
- II. استفاده از حساب کاربری شرکت پندار کوشک ایمن برای بهره بردارانی که امکان دسترسی به این سرویسها را دارند اما مایل به داشتن حساب کاربری در Firebase نمی باشند. مالک این حساب کاربری، شرکت پندار است.

PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir



- III. استفاده از سرویس ویژه شرکت پندار کوشک ایمن برای بهره بردارانی که در دسترسی به این سرویسها با مانع مواجه هستند.
  - مشخصات binding سامانهها

درگاه امضای دیجیتال در sub-domain های مجزایی برای ارایه سرویسها، رابط کاربری و دسترسی مدیر درگاه میزبانی میشود. به عنوان مثال:

isg.Your\_Organization.ir isgREST. Your\_Organization.ir or isgREST.Your\_Organization.Local isgSOAP. Your\_Organization.ir or isgSOAP.Your\_Organization.Local isgAdmin.Your\_Organization.ir or isgAdmin.Your\_Organization.Local

به صورت پیش فرض، سرویسهای ISG در همان درگاه امضای دیجیتال نصب می شوند. در صورت تمایل بهره بردار به نصب هر یک از سرویسها در سامانه ای مجزا، با ارایه مشخصات رکورد DNS آن سامانه، تفکیک سرویسها امکان پذیر است. لذا می بایست رکوردهای DNS مربوط به تمامی sub-domain ایجاد و اعلام گردند. همچنین لازم است گواهینامه SSL هر سامانه بر روی سرور نصب و مشخصات آن ارایه شود.

مدیریت درگاه امضا

دسترسی به سامانه مدیریت درگاه، مبتنی بر SSL دوطرفه می باشد. توصیه اکید می شود به منظور حفظ امنیت بیشتر، گواهینامه سمت کلاینت (ISG Admin) بر روی توکن سخت افزاری نگهداری شود. برای شناسایی کاربر مجاز (مدیر درگاه)، ارایه فایل cer (کلید عمومی) به همراه زنجیره این گواهینامه الزامی است.



### ۴. نصب گام به گام

### ۴,۱ پیش نیازهای نصب

با توجه به مطالب ذکر شده، پیش از آغاز فرآیند نصب، می بایست اطمینان حاصل کنید که نیازمندی های لازم فراهم شدهاند:

- SQL Server طبق مشخصات ذکر شده در بند ۲ نصب شده است.
- و حساب کاربری لازم برای دسترسی به SQL Server ایجاد شده است.
  - فایل backup پایگاه داده ISG دریافت شده است.
  - IIS طبق مشخصات ذکر شده در بند ۲ نصب شده است.
    - برنامه نصب هر یک از درگاهها دریافت شده است.
    - دسترسیهای اینترنتی مطابق جدول بند ۳ وجود دارد.
  - حساب کاربری Firebase ایجاد و فایل json آن دریافت شده است.
  - رکوردهای DNS به تعداد سامانههای مورد نیاز ساخته شده است.
- گواهینامه مدیر درگاه صادر شده و فایل cer (کلید عمومی) آن به همراه زنجیره این گواهی دریافت شده است.
- زنجیره انواع گواهینامههایی که امضا کنندگان استفاده خواهند کرد، موجود است. به عنوان مثال اگر امضا کنندگان میبایست از گواهینامههای سطوح برنزی تا پلاتینیم مرکز توسعه استفاده نمایند، میبایست زنجیره این نوع گواهینامهها موجود باشد.

#### ۴,۲ نصب یایگاه داده

۱. فایل backup را به مسیر پیش فرض SQL Server منتقل کنید.

 $C:\Program Files\Microsoft SQL Server\<INSTANCE NAME>\Microsoft SQL\Backup$ 

۲. در محیط Management Studio در بخش Databases، آیتم Restore Database را انتخاب کنید.

| New Database                 |   |
|------------------------------|---|
| Attach                       |   |
| Restore Database             |   |
| Restore Files and Filegroups |   |
| Filter                       | , |
| Deploy Data-tier Application |   |
| Import Data-tier Application |   |
| Start PowerShell             |   |
| Reports                      | • |
| Refresh                      | _ |

PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir





۳. در پنجره Restore Database گزینه Device را انتخاب کرده، روی دکمه مقابل (...) کلیک کنید تا پنجره Select backup را انتخاب کرده، روی دکمه مقابل (...) کلیک کنید تا پنجره devices

| 🕵 Restore Database -   | - 🗆  | $\times$             |
|--|--|----------------------|
| 🐼 No backupset selected to be restored   | d.   |                      |
| <ul> <li>No backupset selected to be restored</li> <li>Select a page</li> <li>General</li> <li>Files</li> <li>Options</li> </ul> | J.         Script ✓           Source         Obtabase:         Database:         Database:         Database:         Database:         Database:         Database:         Database:         Database:         Database:         Destination         Restore         Specify the backup media and its location for your restore operation.         Backup media type:         File         Backup media: | v<br>eline           |
| Connection   | Restore Add t LSN<br>Remove<br>Contents  | Full LS              |
| ₩ \MSSQL2019<br>[DESKTOP-E5CDRVH\PKI]  | OK Cancel Help   |                      |
| Progress   |  |                      |
| Ready  | <  | <b>&gt;</b><br>Media |
|  | OK Cancel  | Help                 |

۲. روی دکمه Add در تصویر قبل کلیک کنید تا پنجره Locate Backup File گشوده شود. سپس فایل پشتیبان پایگاه داده ISG
 ۹. را انتخاب کنید.

| ■ Locate Backup File - DESKTOP-E5CE   | RVH\MSSQL2019               | —                      | < |
|---|-----------------------------|------------------------|---|
| Backup File location:   | QL15.MSSQL2019\MSSQL\Backup | 1                      | ρ |
| Microsoft MPI     Microsoft SQL Server     Microsoft SQL     Microsoft SQL Server     Microsoft SQL     Mi | > ISG bak                   |                        |   |
| File name:  | Backup Fil                  | es(*.bak;*.tm;*.log) ~ |   |
|   | OK                          | Cancel                 |   |

PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir

صفحه ۵





| 💀 Restore Database - ISG                           |  |                          |             |                 |           |                     |            |           | —          |        | $\times$  |
|--|--|--------------------------|-------------|-----------------|-----------|---------------------|------------|-----------|------------|--------|-----------|
| A tail-log backup of the source datab              | ase will be taken  | . View this setting o    | n the Optio | ns page.        |           |                     |            |           |            |        |           |
| Select a page<br>& General<br># Files<br># Options | Script Source Source Data O Data Destination   | Help base: ce: Database: | C:\Progra   | m Files\Microso | oft SQL S | Server\MSSQL15.MSSQ | L2019\MSSC | QL\Backup | \ISG.bak   |        | >         |
| Connection   | Databas  | se:                      | ISG         |                 |           |                     |            |           |            |        | ~         |
| ₩ .\MSSQL2019<br>[DESKTOP-E5CDRVH\PKI]             | Restore to: The last backup taken (Saturday, May 15, 2021 12:05:12) Restore plan Backup sets to restore: |                          |             |                 |           |                     |            | Timeline  |            |        |           |
| View connection properties                         | Restore  | Name                     |             | Component       | Туре      | Server              | Database   | Position  | First LSN  |        |           |
| Progress   | <  | ISG-Full Database        | Backup      | Database        | Full      | DESKTOP-REH3V53     | ISG        | 1         | 1064000    | 000130 | 600(<br>> |
| Une Done   |  |                          |             |                 |           |                     |            | [         | Verify Bac | kup Me | dia       |
|  |  |                          |             |                 |           |                     | ОК         | Car       | ncel       | Help   |           |

۵. با کلیک روی دکمه OK در پنجرههای گشوده شده به پنجره Restore Database باز گردید.

۶. در پانل سمت چپ پنجره فوق، گزینه Options را انتخاب نموده و تیک مربوط به Take tail-log backup before restore را

|   |   |  | رداريد. | بر     |
|---|---|--|---------|--------|
| 💀 Restore Database - ISG  |   | _  |         | ×      |
| 🕕 Ready   |   |  |         |        |
| Select a page<br>General<br>Files<br>P Options                                      | Script  General Help  Restore options  Overwrite the existing databas  Preserve the replication setting Restrict access to the restored | e (WITH REPLACE)<br>gs (WITH KEEP_REPLICATION)<br>d database (WITH RESTRICTED_USER)    |         |        |
|   | Recovery state:   | RESTORE WITH RECOVERY  |         | $\sim$ |
|   | Standby file:   | C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQL2019\MSSQL\Backu                    | .p∖     |        |
| Connection           y         ✓         .MSSQL2019           [DESKTOP-E5CDRVH\PKI] | Leave the database ready to use<br>Tail-Log backup  | by rolling back uncommitted transactions. Additional transaction logs cannot be restor | ed.     |        |
| View connection properties  | (WITH NORECOVERY  | ) (in the restoring state  |         |        |
| Progress<br>Done  | Backup file:<br>Server connections<br>Close existing connections to   | C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQL2019\MSSQL\Backu                    | /qı     |        |
|   |   | OK Cancel  | Hel     | р      |

۷. بر روی دکمه OK کلیک کنید و تا پایان مرحله ساخت پایگاه داده از روی فایل backup و دریافت پیام success تامل نمایید.



### ۴,۳ تنظیمات دسترسی به پایگاه داده

 ۱۶. اگر لاگین مربوط به دسترسی به پایگاه داده ISG وجود دارد، میتوانید از این قسمت صرفنظر کنید. در غیر این صورت در پنجره Object Explorer قسمت مربوط به Security را بازکرده و برای ساخت یک لاگین جدید اقدام نمایید.



۲. یک login به نام ISG تعریف کرده، گذرواژه آن را تعیین کنید. سپس پایگاه داده پیش فرض را ISG قرار دهید.

| 🗄 Login - New                       |  |                     | _        |        |   |
|-------------------------------------|--|---------------------|----------|--------|---|
| Select a page                       | 🖵 Script 🔻 😯 Help                          |                     |          |        |   |
| <ul> <li>Server Roles</li> </ul>    |  |                     |          | -      |   |
| User Mapping                        | Login name:                                | ISG                 |          | Search |   |
| Status                              | <ul> <li>Windows authentication</li> </ul> |                     |          |        |   |
|                                     | SQL Server authentication                  |                     |          |        |   |
|                                     | Password:                                  | •••••               |          |        |   |
|                                     | Confirm password:                          | •••••               |          |        |   |
|                                     | Specify old password                       |                     |          |        |   |
|                                     | Old password:                              |                     |          |        |   |
|                                     | Enforce password policy                    |                     |          |        |   |
|                                     | Enforce password expiration                | tion                |          |        |   |
|                                     | User must change passw                     | vord at next login  |          |        |   |
|                                     | <ul> <li>Mapped to certificate</li> </ul>  |                     |          | ~      |   |
|                                     | O Mapped to asymmetric key                 |                     |          | ~      |   |
| Connection                          | Map to Credential                          |                     | ```      | ~ Add  |   |
| Server:<br>DESKTOP-E5CDRVH\MSSQL201 | Mapped Credentials                         | Credential          | Provider |        |   |
| Connection:<br>DESKTOP-E5CDRVH\PKI  |  |                     |          |        |   |
| View connection properties          |  |                     |          |        |   |
|                                     |  |                     |          |        |   |
| Progress                            |  |                     |          | Remove |   |
| Ready                               | Default database:                          | ISG                 |          | ~      |   |
| A <sup>d b</sup> A                  | Default language:                          | <default></default> |          | ~      |   |
|                                     |  |                     | ОК       | Cancel | ] |



۳. سپس به قسمت User Mapping رفته، در قسمت Users mapped to this login پایگاه داده ISG را انتخاب کنید و در قسمت ۳. سپس به قسمت Database role membership و bb\_owner را برگزینید.

| Login - New                        |   |              | _              |        |
|------------------------------------|---|--------------|----------------|--------|
| Select a page                      | Script ▼ ? Help   |              |                |        |
| Securables<br>Status               | Users mapped to this login:<br>Map Database<br>ISG<br>master<br>model<br>tempdb | User         | Default Schema |        |
| Connection                         | Guest account enabled for:  | ActivationDB |                | ~      |
| DESKTOP-E5CDRVH\MSSQL20            | Database role membership for:   | ISG          |                |        |
| Connection:<br>DESKTOP-E5CDRVH\PKI | db_accessadmin<br>db_backupoperator   |              |                |        |
| YT view connection properties      | db_datawriter<br>db_ddladmin<br>db_denydatareader<br>db_denydatawriter          |              |                |        |
| Progress                           | db_owner  |              |                |        |
| Ready                              | ☐ db_securityadmin<br>☑ public  |              |                |        |
|                                    |   |              | ОК             | Cancel |

۹. روی دکمه OK کلیک کنید تا login مربوط به ISG ایجاد شود.



#### ۴,۴ ایجاد سامانه جدید در IIS

در این بخش مراحل ایجاد یک سامانه در IIS توضیح داده می شود. از سامانه ISG به عنوان یک سامانه نمونه استفاده شده است اما مراحل شرح داده شده، برای ایجاد هر سامانه دیگری کاربرد دارد.

۰. پوشهای برای دسترسی سامانه مورد نظر به نرم افزار مربوط ایجاد کنید. پیشنهاد می شود پوشه مذکور در این مسیر باشد: C:\inetpub\wwwroot\ISG

سپس نرم افزار ISG را که در فایل ISG\_UI\_Vx.x.x.exe فشرده شده است، در مسیر پوشه ایجاد شده بازگشایی کنید.

| 😨 WinRAR self-extracting archive — 🗌 🗙 |   | ×                                    |  |
|--|---|--------------------------------------|--|
|  | <ul> <li>Press Extract button to start extraction.</li> <li>Use Browse button to select the destination from the folders tree. It can be also entere manually.</li> <li>If the destination folder does not exist, it we created automatically before extraction.</li> </ul> | on folder<br>d<br>vill be<br>Browse. |  |
|  | Extract   | Cancel                               |  |

۲. کنسول IIS Manager را باز کرده و در قسمت Sites اقدام به ایجاد سامانه جدید نمایید.



عمومى

صفحه ۹



۳. در پنجره Add Website مشخصات سامانه را مطابق شکل زیر درج کنید.

| dd Website   |                                    | ?      | × |
|--|------------------------------------|--------|---|
| Site name:   | Application pool:                  |        |   |
| ISG  | ISG Select                         |        |   |
| Content Directory  |                                    |        |   |
| Physical path:   |                                    |        |   |
| C:\inetpub\wwwr  | pot\ISG                            |        |   |
| Pass-through auth  | entication                         |        |   |
|  | <b>T</b> 10 m                      |        |   |
| Connect as   | lest Settings                      |        |   |
| Binding  |                                    |        |   |
| Type:  | IP address: Port:                  |        |   |
| http   | ✓ All Unassigned ✓ 80              |        |   |
| Host name:   |                                    |        |   |
| isg. <your doma<="" td=""><td>IN NAME&gt;.ir</td><td></td><td></td></your> | IN NAME>.ir                        |        |   |
| Example: www.co  | ntoso.com or marketing.contoso.com |        |   |
|  | -                                  |        |   |
| Start Website imm  | nediately                          |        |   |
|  |                                    |        |   |
|  | ОК                                 | Cancel |   |
|  |                                    |        |   |

در قسمت Host name به جای عبارت isg.<YOUR DOMAIN NAME>.ir مشخصات رکورد DNS سامانه خود را وارد نمایید. سپس روی دکمه OK کلیک کنید تا سامانه جدید ایجاد و پنجره بسته شود.



- ۴. برای اعمال تنظیمات SSL باید از قبل گواهینامه SSL سایت مورد نظر بر روی سرور نصب شده باشد.
- ۴.۱. در بخش Sites در پانل سمت چپ، سایت ISG را انتخاب کنید.
  ۴.۲. در پانل سمت راست روی آیتم Bindings کلیک کنید تا پنجره Site Bindings گشوده شود.
  ۴.۳. در پنجره Bindings روی Add کلیک کنید تا پنجره Add Site Binding گشوده شود.
  ۴.۴. آیتم https را stat قرار دهید.
  ۴.۴. نشانی II را مطابق II سرور قرار داده یا به صورت پیش فرض در وضعیت All Unassigned رها کنید.
  ۴.۶. پورت پیش فرض Site Signed است. اگر پورت خاصی مد نظر شماست، شماره پورت را درج کنید.
  ۴.۶. در قسمت name روی ISS مشخصات رکورد OMA سامانه خود (۲۰۰۰ مشخصات رکورد State).
  - ۲٫۷. در قسمت Host name به جای عبارت Isg.< I OUR DOMAIN NAME>.if مشحصات ر تورد DNS سامانه -را وارد نمایید.
    - ۴,۸. گواهینامه SSL Certificate سامانه را از فهرست SSL Certificate انتخاب کنید.
      - ۴,۹. روی دکمه OK پنجرههای گشوده شده کلیک کنید تا بسته شوند.







- ۵. در این مرحله حساب کاربریای که Applicatin Pool تحت آن اجرا میشود را مطابق شکل بعد تغییر دهید. ۵٫۱. در پانل سمت چپ Application Pools را انتخاب کنید تا فهرست آن دیده شود.
  - ۵٫۲. از فهرست ISG را انتخاب کنید.
  - ۵٫۳. سپس در پانل سمت راست روی Advanced Settings کلیک کنید.
- Advanced Settings از قسمت Process Model ویژگی Identity را تغییر دهید. مقدار این ویژگی به صورت ۵٫۴. در پنجره Application Pool Identity گشوده پیش فرض ApplicationPoolIdentity است. روی آن کلیک کنید تا پنجره Application Pool Identity گشوده شود.
  - ۵٫۵. در قسمت Built-in account آیتم NetworkService را برگزینید.
  - ۵٫۶. سپس روی دکمه OK پنجرههای گشوده شده کلیک کنید تا بسته شوند.

| 🍋 Internet Information Services (IIS) Manager  |  | - 🗆 ×   |
|--|--|---|
| ← → 🔯 ► DESKTOP-E5CDRVH ► Applie   | ation Dools  | 🖸 🖂 🙆 🔹   |
| File View Help   | Application Pool Identity ? X  |   |
| Connections Connec | Built-in account:      ApplicationPoolIdentity      LocalService      ApplicationPoolIdentity      Event Key Set      OK Cancel      Processor Attinity Enabled     Plase     Processor Attinity Enabled     Processor Attinity Enable     Proce | Actions       Is are<br>ng different          • |
| Ready  |  | ۹ <u>۱.</u> :                                   |





- ۶. اکنون به پوشه محل نصب نرم افزار ISG بروید و اگر داخل آن پوشهای به نام logs وجود ندارد، آن را ایجاد کنید.
  - .۶٫۱ روی پوشه logs کلیک راست کنید و از منو Properties را انتخاب کنید.
    - ۶٫۲. در پنجره logs Properties به برگه Security بروید.
  - ۶٫۳. روی دکمه Edit کلیک کنید تا پنجره Permissions for logs گشوده شود.
- ۶٫۴. در پنجره Permissions for logs روی Add کلیک کنید و گروه NETWORK SERVICE را اضافه نمایید.
- ۶٫۵. در بخش Permissions for NETWORK SERVICE آیتم Full Control را در ستون Allow تیک بزنید.
  - ۶٫۶. روی دکمه OK پنجرههای گشوده شده کلیک کنید تا بسته شوند.

| PC → Local I  | 📜 logs Properties   | Permissions for logs X             |
|---|---|------------------------------------|
| Name  | General Sharing Security Previous Versions Customize  | Security                           |
| bin<br>1 pontent  | Object name: logs<br>Group or user names:   | Object name: D:\Publish\ISG\UINogs |
| onts<br>logs<br>Scripts<br>Views<br>↓ favicon.i<br>↓ libman.j<br>↓ package<br>PKTB.xm<br>↓ Precomp<br>Startup o<br>Web.cor<br>↓ Web.cor | Authenticated Users SYSTEM Administrators (DESKTOP-E5CDRVH\Administrators) Users (DESKTOP-E5CDRVH\Users) To change permissions, click Edit. Permissions for Authenticated Users Full control Modify Read & execute List folder contents Read Write For special permissions or advanced settings. Click Advanced. Advanced | Group or user names:               |
|   | OK Cancel App   |                                    |

راهنمای نصب و راه اندازی ISG شرکت پندار کوشک ایمن



### ۴,۵ ایجاد برنامه کاربردی در یک سامانه

در این بخش مراحل ایجاد یک Application در IIS توضیح داده می شود. از برنامه ISG.REST به عنوان یک Application در این بخش مراحل ایجاد یک Application در این بخش مده است اما مراحل شرح داده شده، برای ایجاد هر Application دیگری کاربرد دارد.

۱. پوشهای برای دسترسی Application مورد نظر به نرم افزار مربوط ایجاد کنید. پیشنهاد میشود پوشه مذکور در این مسیر باشد:

- ۲. سپس نرم افزار سرویس REST را که در فایل ISG\_REST\_Vx.x.x.exe فشرده شده است، در مسیر پوشه ایجاد شده بازگشایی کنید.
  - ۳. روی سایت مورد نظر در IIS Manager کلیک راست کرده و Add Application را برگزینید.



- ۴. اطلاعات لازم در پنجره Add Application را مطابق شکل بعد مشخص نمایید.
  - ۴,۱. نام Alias را درج کنید.
- با کلیک بر روی Select میتوانید Application Pool مختص به Application مورد نظر را معرفی کرده یا از ۴٫۲. با کلیک بر موی مورد نظر را معرفی کرده یا از Application Pool سایت اصلی استفاده نمایید.
  - ۴٫۳. در قسمت Physical path مسیری که فایلهای Application را قرار دادهاید، معرفی نمایید.

PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir

| ISG | راهنمای نصب و راه اندازی |
|-----|--------------------------|
|     | شركت پندار كوشك ايمن     |



| Add Application  | ?      | × |
|--|--------|---|
| Site name: Default Web Site Path: Alias: Application pool: REST Example: sales Physical path:            | Select |   |
| C:\inetpub\wwwroot\ISG_REST<br>Pass-through authentication<br>Connect as Test Settings<br>Enable Preload |        |   |
| ОК   | Cancel |   |

۵. با کلیک بر روی OK پنجره بسته شده و Application مورد نظر شما ساخته می شود.

#### ۴,۶ اعمال تنظيمات سامانهها

پس از تکرار مراحل ایجاد Site و Application برای ایجاد تمامی سامانههای مورد نیاز، می بایست هر سامانه را تنظیم کنید.

- . تنظیم سامانه ISG
- فایل web.config سامانه را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:



logToFile: در صورتی که مقدار logToFile برابر با true باشد، هنگام بروز خطا در برنامه، جزییات خطا در یک فایل متنی در پوشه logs بر اساس تاریخ رخداد خطا ذخیره خواهد شد.



CRLAndOCSPValidation: در صورت true بودن مقدار این تنظیم، گواهینامههای امضا کنندگان به صورت آنلاین بر اساس نشانیهای مندرج در گواهینامه با صادر کننده گواهینامه چک خواهد شد. اگر مقدار این تنظیم false باشد، فقط ویژگیهایی از گواهینامه اعتبار سنجی میشوند که نیاز به دسترسی آنلاین ندارند. مانند تاریخ انقضا و ...

ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

در فایل web.config به قسمت connectionStrings بروید و آیتم ISGConnectionString را مطابق بند ۴,۳
 (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. نام ISGConnectionString را ویرایش نکنید.

<add name="ISSConnectionString" connectionString="Integrated Security=SSPI;Initial Catalog=ISG;Data Source=(local)\VISSQL2019" providerName="System.Data.SqlClient" /
</pre>

۲. تنظیمات Site یا Application مربوط به سرویس REST

سرویس REST درگاه امضا را میتوانید هم به صورت یک Site و هم یک Application نصب نمایید. متناسب با نوع نصب انتخاب شده، تنظیمات دسترسی به پایگاه داده متفاوت خواهد بود که در ادامه توضیح داده میشود.

 فایل web.config مربوط را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:



logToFile: در صورتی که مقدار logToFile برابر با true باشد، هنگام بروز خطا در برنامه، جزییات خطا در یک فایل متنی در پوشه logs بر اساس تاریخ رخداد خطا ذخیره خواهد شد.

ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

homePage: تنظیم مقدار این آیتم اختیاری میباشد. هر نشانی اینترنتی که در این تنظیم درج شود، به عنوان صفحه اصلی نمایش داده خواهد شد.

gateway: نشانی اینترنتی سامانه ISG است. این نشانی را بدون کاراکتر / در آخر آن درج کنید.

PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir



pendarNotificationServiceURL: نشانی سرویس ویژه اطلاع رسانی شرکت پندار کوشک ایمن است. تغییر در این نشانی، موجب بروز خطا، در هنگام ارسال پیام اطلاع رسانی خواهد شد. بدون هماهنگی با شرکت پندار این نشانی را تغییر ندهید.

usePendarNotification اگر مقدار true تنظیم شود، پیامهای اطلاع رسانی از طریق سرویس ویژه شرکت پندار ارسال شده و در غیر این صورت، پیامها از طریق سرویس Firebase گوگل ارسال خواهند شد. نکته: پیامهای اطلاع رسانی فقط به تلفن همراه امضا کنندگانی ارسال خواهد شد که برنامه mKeyOne را روی گوشی هوشمند خود نصب و مراحل ثبت نام را طی کرده باشند.

اگر سرویس REST را به صورت یک Site نصب کردهاید، در فایل web.config به قسمت connectionStrings بروید
 و آیتم ISGConnectionString را مطابق بند ۴٫۳ (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. در این حالت
 می بایست قسمت defaultConnectionFactory از بخش entityFramework را مطابق شکل زیر کامنت کرده یا حذف
 نمایید.

unString" connectionString="Integrated Security=SSPI;Initial Catalog=ISG;Data Source=(local)\VISSQL2019" providerName="System.Data.SqlClient" /> rrameworkD <cdefaultConnectionFactory type="System.Data.Entity.Infrastructure.SqlConnectionFactory, EntityFramework"> <parameters) <parameter value="IS6ConnectionString" /> </parameters> </defaultConnectionFactory>--> (providers> cyrovider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" /> </providers>

• اگر سرویس REST را به صورت یک Application در سامانه ISG نصب کردهاید، می بایست تنظیمات مربوط به دسترسی به پایگاه داده را برعکس مورد قبل انجام دهید. یعنی بخش connectionStrings را کامنت نموده یا حذف کنید و قسمت entityFramework را به بخش defaultConnectionFactory بیافزایید.



**نکته**: استفاده از کلید واژه ISGConnectionString در هر دو حالت از تنظیمات فوق الزامی است. به هیچ عنوان این کلید واژه را تغییر ندهید.



۳. تنظیمات Site یا Application مربوط به سرویس SOAP

سرویس SOAP درگاه امضا را میتوانید مانند سرویس REST، هم به صورت یک Site و هم یک Application نصب نمایید. تمامی تنظیمات لازم برای سرویس SOAP همانند تنظیمات سرویس REST است. تنها تفاوت این است که در بخش appSettings به آیتم homePage نیازی نیست.



- ۴. تنظیم سامانه ISG Admin
- فایل web.config سامانه را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:

| <pre>cappSettir</pre>   | ngs>  |
|---|---|
| <add k<="" td=""><td><pre>key="webpages:Version" value="3.0.0.0" /&gt;</pre></td></add>                                       | <pre>key="webpages:Version" value="3.0.0.0" /&gt;</pre>                                       |
| <add k<="" td=""><td><pre>key="webpages:Enabled" value="false" /&gt;</pre></td></add>   | <pre>key="webpages:Enabled" value="false" /&gt;</pre>   |
| <add k<="" td=""><td><pre>key="ClientValidationEnabled" value="true" /&gt;</pre></td></add>                                   | <pre>key="ClientValidationEnabled" value="true" /&gt;</pre>                                   |
| <add k<="" td=""><td><pre>key="UnobtrusiveJavaScriptEnabled" value="true" /&gt;</pre></td></add>                              | <pre>key="UnobtrusiveJavaScriptEnabled" value="true" /&gt;</pre>                              |
| <add k<="" td=""><td><pre>key="daysBefore" value="30" /&gt;</pre></td></add>  | <pre>key="daysBefore" value="30" /&gt;</pre>  |
| <add k<="" td=""><td><pre>key="ServiceLogIsEnabled" value="true" /&gt;</pre></td></add>                                       | <pre>key="ServiceLogIsEnabled" value="true" /&gt;</pre>                                       |
| <add k<="" td=""><td><pre>key="TwoWaySslEnabled" value="true" /&gt;</pre></td></add>  | <pre>key="TwoWaySslEnabled" value="true" /&gt;</pre>  |
| <add k<="" td=""><td><pre>key="CertificateThumbprint" value="6c1aa690580f98212fe1523967fedd89e8192df3" /&gt;</pre></td></add> | <pre>key="CertificateThumbprint" value="6c1aa690580f98212fe1523967fedd89e8192df3" /&gt;</pre> |
| (/appSetti  | ings>   |

daysBefor: مقدار این تنظیم به صورت پیش فرض ۳۰ روز قرار داده شده است. با استفاده از این مقدار به مدیر درگاه پیام داده می شود که در صورت تمایل، لاگهای قدیمی تر سامانه از پایگاه داده حذف شوند.

ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

**TwoWaySslEnabled**: مقدار true، دسترسی به این سامانه از طریق کانال SSL را الزامی مینماید.

CertificateThumbprint: در صورتی که مقدار TwoWaySslEnabled برابر با true باشد، فقط گواهینامهای برای سمت کلاینت پذیرفته خواهد شد که مقدار thumbprint آن برابر با مقدار درج شده در این تنظیم است. برای درج مقدار صحیح این تنظیم میبایست فایل cer (کلید عمومی) گواهینامه مدیر سایت را در اختیار داشته باشید.

در فایل web.config به قسمت connectionStrings بروید و آیتم ISGConnectionString را مطابق بند ۴,۳
 (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. نام ISGConnectionString را ویرایش نکنید.



• در IIS Manager سایت ISGAdmin را انتخاب کرده و تنظیمات SSL را باز کنید.



• در بخش SSL Settings تنظیمات را مطابق شکل زیر اعمال کنید.



- ابتدا با تیک زدن Required SSL استفاده از کانال SSL را الزامی نمایید.
  - سپس در بخش Client certificates آیتم Require را انتخاب کنید.
    - در پایان با کلیک روی Apply، تغییرات را اعمال نمایید.

#### نكات عمومى:

- در صورت بهره برداری از امکان پیام رسانی به تلفن همراه، فایل json حساب کاربری Firebase را به سامانههای REST و SOAP در مسیری که فایل web.config وجود دارد، منتقل نمایید.
- زنجیرههای انواع گواهینامههایی که امضا کنندگان استفاده مینمایند، همچنین زنجیره گواهینامه مدیر درگاه امضا را در Certificate Store مربوط به Local Machine نصب کنید.
- پس از اعمال تنظیمات در هر Site یا Application، یکبار آن Site را Restart نموده و Application Pool مربوط را نیز Recycle کنید.

#### PKI-ISG-Deployment-Guide

تمامی حقوق نشر این سند متعلق به شرکت پندار کوشک ایمن میباشد www.pki.co.ir