«بسمه تعالی»

خلاصه ای ازپروژه ی معماری وضع مطلوب

سند معماری کلان پروژه‌ی" کارت هوشمند ملی"

- **مقدمه :**

سازمان ثبت احوال کشور به دلیل دراختیار داشتن اسناد هویت و تابعیت فردی و آمارهای حیاتی یکی از ارکان مهم حکومت تلقی می‌شود. ارائه خدمات عمومی به آحاد مردم و اطلاعات ویژه جمعیتی به ارکان حکومت از ویژگی‌های اختصاصی و انحصاری این سازمان است. در قوانین جدید، از جمله وظایف سازمان ثبت احوال کشور ثبت وقایع حیاتی نظیر ثبت ولادت و صدور شناسنامه، ثبت وفات و صدور گواهی می‌باشد. وظایفی مانند ایجاد پایگاه مکانیزه اطلاعات جمعیت کشور و صدور کارت شناسایی ملی به منظور جمع‌آوری و تهیه آمار انسانی سراسر کشور و انتشار آن از مهم‌ترین وظایف سازمان ثبت احوال است. بدین‌منظور سازمان مذکور علاوه بر صدور شناسنامه، با صدور کارت شناسایی ملی بخشی از نیازهای اطلاعاتی کشور را برطرف نموده است.

- **هدف :**

لذا به منظور ایجاد بستری برای ارائه خدمات شهروندی در زمینه ثبت‌نام، درخواست صدور و خدمات پس از تحویل در زمینه کارت هوشمند ملی و امکان رهگیری و خدمات ارتباطی با شهروندان و به منظور " تدوین سند معماری مطلوب پروژه کارت هوشمند ملی" و نیز اجرای مرحله ای آزمایشی" ، این پروژه شکل گرفت .

سامانه های خدمات شهروندی، مدیریت کارت ، زیرساخت کلید عمومی، مدیریت کلید، زیست سنجی، کارت و مسائل امنیتی مورد بررسی قرار گرفتند . هدف ایجاد سامه نه ای بودکه با استفاده از سه سیستم اصلی شامل پورتال، دفتر پیشخوان و مدیریت ، اهداف را به تحقق برساند.

- **ساختار پروژه :**

ساختار سند معماری مطلوب ، در چهار سرفصل اصلی "فازها و مراحل پروژه کارت هوشمند ملی"، "دیدگاه کلان معماری" و "سامانه ها و اجزاء معماری"، "معماری امنیت" تهیه گردید.

- **معماری کلان پروژه:**

معماری کلان پروژه بر حسب لایه های خدمات، فرایند ها ، داده ها، نرم افزارها ، مرکز داده و زیرساخت شبکه مورد نیاز انجام شد.

- **اجرا ی پروژه و روش های اجرایی :**

یکی از مهم‌ترین موارد مطرح شده در مسیر توسعه پروژه کارت هوشمند ملی، بحث انتخاب خدمات(کاربردهای) کارت می بود. در این خصوص، اهداف مورد انتظار از برنامه چهارم توسعه، اهداف سند چشم انداز فناوری اطلاعات کشور و طرح ملی دولت الکترونیک، مراجع مناسب برای انتخاب خدمات بودند؛ با توجه به اینکه بیانیه چشم‌انداز و هدف کلی پروژه کارت هوشمند ملی نیز تهیه و تصویب شده بود، لذا اسناد مبنای تعیین کاربردها و خدمات ارائه شده توسط کارت قرار داده شدند.

بطورکلی و در سطح بالا خدمات قابل ارائه بواسطه کارت هوشمند ملی، در دو دسته‌ی کلی قرار داده شدند: خدمات فیزیکی (چشمی)، و خدمات الکترونیکی. خدمات فیزیکی یا چشمی خدماتی هستند که به صِرف دارا بودنِ کارت به دارنده ارائه می گردند. هویت ملی ایرانی دارنده‌ی کارت، بواسطه دارا بودن این کارت منجر به دریافت برخی خدمات می گردد که تنها با شناسایی قابل ارائه می‌باشند.

دسته‌ی خدمات الکترونیکی که قابل ارائه بواسطه‌ی کارت می باشند، به دو دسته‌ی داخل کارت و خارج کارت تقسیم شدند. نقش اصلی این کارت، تامین زیرساخت استقرار دولت الکترونیکی بوده و اساس کارآن ، ارائه‌ی خدمات الکترونیکی به دارنده‌ی کارت است. خدمات الکترونیکی داخل کارت، خدماتی هستند که بواسطه‌ی ساختار و نرم‌افزارهای تعبیه شده درون کارت، به دارنده‌ی کارت ارائه می گردند. این خدمات نیز به دو دسته‌ی خدمات هویتی و خدمات شهروندی درون کارت تقسیم گشتند.

خدمات هویتی معادل خدمات IAS می باشد؛ همچنین خدمات شهروندی درون کارت شامل رای گیری، یارانه، سلامت و پرداخت می باشد. خدمات الکترونیکی خارج کارت، شامل کلیه‌ی کاربردها و خدمات دولت الکترونیک می‌باشد که بر اساس سه خدمت پایه‌ی IAS ارائه شدند.

نکته‌ای که همواره در نظر گرفته شد ، کاربردهای آینده و قابلیت افزایش کاربردهای کارت هوشمند ملی بود.لذا این کارت قابلیت توسعه و افزایش خدمات را بر حسب نیاز و آمادگی دریافت خدمت توسط شهروندان، دارا می باشد.

- **معماری پروژه ی کارت هوشمند:**

از آنجایی که یکی از مهمترین اهداف پروژه کارت ملی هوشمند ایجاد دروازه خدمات دولت الکترونیک می بود، این خدمات به تعداد زیاد و غیر قابل پیش بینی در نظر گرفته شدندو معماری پروژه کارت ملی هوشمند بر اساس نگرشی قائل به وجود یک ساختار مناسب روی کارت هوشمند به نحوی که بدون نیاز به وجود کاربردهای فراوان امکان ارائه تعداد حداکثری از کاربردها وجود داشته باشد، انجام شد. بر این اساس دو مدل ارائه خدمت در زمان بهره‌برداری از کارت ملی هوشمند ارائه گردیدند : ارائه خدمات On Card و ارائه خدمات Off Card.

خدمات on Card، خدماتی هستند که بر اساس «کاربردهای روی کارت » کارت ملی هوشمند ارائه می گردند. در این مدل نرم افزارهای مربوطه با داشتن مجوز های لازم، که توسط ثبت احوال در اختیار سازمان های خدمتگزار قرار داده شدهه است، انجام عملیاتی خاص را از کارت درخواست می کنند ویا داده ای را از بخش مربوطه خوانده و یا در آن می نویسند. داده‌های مربوط به هر خدمت On-Card که در فضای اختصاصی آن ذخیره و بازیابی می گردند به طور کلی به دو دسته «داده‌های اختصاصی کاربرد» مربوط به دارنده کارت که برای ارائه خدمت On-Card لازم است، مانند اطلاعات هویتی برای «تصدیق هویت» و یا اطلاعات پایه پزشکی برای «سلامت» ، به علاوه «سوابق دریافت خدمت» که جزییات ارائه خدمت به دارنده کارت را نگهداری می کند تشکیل شده است.برای نگهداری این داده‌ها ساختار File و Directory بروی کارت در نظر گرفته شده است که متولی ارائه هر خدمت تنها به بخش مربوط به خود دسترسی خواهد داشت.

خدمات Off-Card خدمات الکترونیکی قابل ارائه به دارندگان کارت ملی هوشمند است که تمامی این خدمات از دو خدمت Identification و Authentication که برروی کارت ملی هوشمند وجوددارند به ترتیب برای شناسایی خدمت گیرنده

(شهروند) و تصدیق هویت آن استفاده می نمایند. همچنین Digital Signature نیز برای این خدمات قابل ارائه است. تمامی داده‌ها و فرآیندهای لازم برای ارائه خدمت، در سیستم آماده شده توسط ارائه دهنده قراردارند و هیچ فضای اختصاصی برای این نوع خدمات بروی کارت وجود ندارد.

در این حالت Special Data و Transaction Logs در بانک اطلاعاتی که توسط خدمتگزار طراحی گردیده است ذخیره و بازیابی می‌گردند و بنابراین محدودیتی برای تعداد اقلام اطلاعاتی و همچنین حجم داده‌ها وجود نخواهد داشت. اما بدیهی است که Access Condition لازم برای استفاده از خدمات IAS باید در اختیار خدمتگزار قرارداده شود.

کارت هوشمند ملی، اساسی‌ترین زیرساخت دریافت خدمات دولت الکترونیکی می باشد؛ در این راستا جامعه خدمت گیرندگان کارت هوشمند ملی ایران سه گروه می باشند: : دولت، بخش خصوصی (بنگاه‌ها) و شهروندان.

زیرساخت ارتباط الکترونیکی این سه گروه با هدف ارائه خدمات الکترونیک، کارت هوشمند ملی می باشد . در نتیجه نُه نوع ارتباط می تواند حاصل گردد که کاربران بر اساس این ارتباطات از کارت هوشمند ملی بهره‌مند خواهند شد:

ارتباط بین موجودیت های مرتبط در ارائه خدمات الکترونیکی

	دولت	بنگاه	شهروند
دولت	دولت-دولت	دولت-بنگاه	دولت-شهروند
بنگاه	بنگاه-دولت	بنگاه-بنگاه	بنگاه-شهروند
شهروند	شهروند-دولت	شهروند-بنگاه	شهروند-شهروند

از دیدگاه دیگر، کارت هوشمند ملی، دو گروه کاربر اصلی را تحت تاثیر قرار می دهد؛ از یک سو فرایندهای سازمان‌های ارائه دهنده خدمات را تسهیل و بهبود می‌بخشد و از سوی دیگر برای عموم شهروندان ایرانی، زیرساخت دریافتِ خدمات را فراهم می‌نماید.

در کارت ملی هوشمند برای اینکه مالکیت هر موجودیت با چه سازمانی است و عملیات مربوط به هر کاربرد را چه نهادی انجام می‌دهد سناریوهای مختلفی قابل انجام است.

- **معماری فرآیند ها :**

فهرست فرایندهای یکپارچه مطلوب به قرار زیر تهیه گردیدند :

- فرآیند کسب‌وکار پیش ثبت نام متقاضی
- فرآیند کسب‌وکار ثبت نام متقاضی
- فرآیند کسب‌وکار رهگیری
- فرآیند خدمات پس از تحویل کارت هوشمند ملی بدون استفاده از کارت
- فرآیند خدمات پس از تحویل کارت هوشمند ملی با استفاده از کارت
- فرآیند Unblock کردن کارت
- فرآیند کسب‌وکار برنامه ریزی تولید کارت هوشمند ملی

- فرآیند کسب‌وکار صدور کارت هوشمند ملی
- فرآیند کسب‌وکار کنترل کیفیت
- فرآیند کسب‌وکار میلینگ کارت هوشمند ملی

در ادامه برای هر فرایند، شناسنامه و نمودار مربوطه تهیه گردید.

• معماری نرم افزارها:

سامانه های پروژه کارت هوشمند ملی به قرار زیر می باشند:

- سامانه خدمات شهروندی
- سامانه مدیریت کارت
- سامانه زیرساخت کلید عمومی
- سامانه مدیریت کلید
- سامانه زیست سنجی
- سامانه کارت

از میان این موارد، بجز "کارت" که ماهیتا نرم افزار نیست، برای سایر سامانه ها یک نمودار یکپارچه در سه لایه نرم افزار ی با ماژول های خاص هر لایه به شرح زیر در نظر گرفته شدند :

لایه واسط: چگونگی ارتباط بین نرم افزارها با کاربران(انسانی، سیستمی) را مشخص می کند و شامل سرویس پیام کوتاه، پست الکترونیک، وب سرویس، واسط مبتنی بر وب، واسط مبتنی بر ویندوز می باشد.

لایه نرم افزارها: در این لایه مجموعه نرم افزارهای پروژه کارت هوشمند ملی آورده شده است. از جمله: CSC, CMS, KMS,AFIS,PKI .

لایه زیرساخت و سکو: در این لایه سکوها و زیرساختهایی که نرم افزارهای پروژه کارت هوشمند ملی از انها استفاده می کنند وجود دارند. از جمله:

- واسط یکپارچه سازی نرم افزارها[1]: ابزار یا میان افزاری است که نرم افزارهای مختلف را از طریق استانداردهای وب سرویس یاسایر متدهای ارتباطی با هم یکپارچه می کند.
- سیستم مدیریت بانک های اطلاعاتی[2]: ابزار یا سیستمی که داده های نرم افزارها در آن نگهداری و مدیریت میشود، از جمله معرفترین محصولات این مورد میتوان به Oracle, SQL, DB2 اشاره نمود.
- سیستم مدیریت هویت[3]: سیستم یا واسط ارتباطی با مرکز داده هویتی کشوری سازمان ثبت احوال که جهت استعلام هویت شهروندان مورد استفاده قرار میگیرد.

[1] Enterprise Applicatin Integration (EAI)
[2] Data Base Management System
3 Identity Management System(IMS)

- پلتفرم جاوا[4] : مجموعه اجزاء و ابزارها که در پلتفرم جاوا وجود دارد و نرم افزارها از آن استفاده میکنند.

- **معماری مرکز داده**

مرکز داده کارت هوشمند ملی یکی از بخش های مهم ارائه سرویس به شهروندان و مخاطبان سرویس محسوب می‌گردد، مرکز داده کارت هوشمند ملی، گرچه از لحاظ وجود اطلاعات وپردازش آن حائز اهمیت است، لیکن یکی از مهترین دلایل اهمیت آن ارائه سرویس بدون وقفه وامن به شهروندان است، سرویسی که در نوع خود و با توجه به حجم و تعداد زیر سیستم های درگیر در ارائه سرویس منحصر به فرد به شمار می رود. به طور کلی برای مرکز داده معیارهای زیر باید مد نظر قرار گیرد:

- قابلیت دسترسی بالا(High Availability)
- توسعه پذیری(Scalability)
- امنیت (Security)
- قابلیت مدیریت(Manageability)

همچنین در انجام کلیه مراحل رعایت الزامات مرتبط در ISO 27001 توصیه می شود.

در جهت نیل به یک مرکز داده استاندارد و متناسب با نیازمندیهای لایه تجاری و سرویس، گام های ذیل به ترتیب و به دقت انجام شدند:

- طراحی کلان مرکز داده مبتنی بر نیازمندیهای لایه تجاری
- طراحی مفهومی مرکز داده مبتنی بر نیازمندیهای لایه تجاری و طراحی کلان
- طراحی جزیی براساس خروجی های طراحی مفهومی

هدف این بخش مستند، تعریف بستر لازم در جهت تهیه طراحی مفهومی مرکز داده کارت هوشمند ملی بود, در این مستند به صورت کلان به ساختار طراحی مرکز داده کارت هوشمند ملی پرداختیم . بطور کلی مرکز داده کارت هوشمند ملی به صورت کلان از بخش های ذیل تشکیل می گردد:

- بخش فیزیکی مرکز داده
- بخش شبکه مرکزداده
- بخش امنیت مرکزداده
- بخش منابع پردازشی مرکزداده
- بخش منابع ذخیره سازی مرکزداده
- بخش تهیه نسخه پیشتیان مرکزداده
- بخش سرویس دهندگان مرکزداده

[4] Java Platform

- بخش سرویسهای زیرساختی مرکزداده
  - **معماری شبکه مطلوب**

با توجه به بررسی‌ها و جلسات مختلف با کارفرما، نیازمندی‌های شبکه خصوصا در بخش ارتباط با دفاتر خدمات شهروندی به شرح زیر تدوین گردید:

۱. **نیازمندی‌های شبکه دفاتر پیشخوان** به شرح زیر تعیین گردید:
   - حداقل ارتباط موردنیاز دفاتر پیشخوان: ارتباط با اینترانت با حداقل پهنای باند ۲۵۶Kbps همزمان (synchron)
   - سوئیچ با قابلیت مدیریت کارکردهای لایه ۲ شبکه مانند VLAN , MAC filter , port security , SSH CLI
   - وجود لینک افزونه برای ارتباط با سازمان ثبت احوال مانند dial-up
   - وجود یک رایانه اختصاصی با حداقل ۱ CPU (x86 2GHz) – 2GB Memory - 100 GB H.D.D – 1 NIC
   - امکان احراز هویت رایانه با توجه به پروتکل X۸۰۲,۱ و هر کاربر برا اساس مکانیزم‌های احراز هویت چندگانه
   - امکان برقراری سرویس VPN IPSec Site-to-Site در هر دفتر پیشخوان
   - وجود برق بی وقفه (UPS) با زمان پشتیبان حداقل ۲ ساعت

۲. **نیازمندهای شبکه ثبت احوال** چنین تعیین گردید:
   - حداقل ارتباط موردنیاز ارتباط با اینترانت کشور با حداقل پهنای باند ۶۰ Mbpsهمزمان است.
   - زیرساخت فیزیکی براساس نیازمندی‌های Tier3 استاندارد TIA-942
   - وجود برق بی وقفه (UPS) با زمان پشتیبان حداقل ۱ ساعت و همچنین ژنراتور در جهت تأمین برق برای زمان بیشتر
   - امکان برقراری سرویس VPN IPSec Site-to-Site با دفاتر پیشخوان

در طراحی شبکه‌های گسترده و ملاحظات امنیتی پروژه، سه راه‌حل کلی برای ارتباطات دفاتر پیشخوان به ثبت احوال در دو سطح " مرکزداده تا دفاتر پیشخوان" و "ارتباط داخلی دفاتر پیشخوان"، به دقت بررسی گردیدند :

سناریوی اول: استفاده از فناوری DMVPN – VRF_VLAN و پروتکل ارتباطی HTTPS

سناریوی دوم: استفاده از فناوری DMVPN – VRF_VLAN و پروتکل ارتباطی HTTP

سناریوی سوم: استفاده از فناوری Remote VPN و پروتکل HTTP

راه‌حل اول، راه‌حل برگزیده و سپس راه‌حل دوم و سوم به ترتیب راه‌حل‌های جایگزین انتخاب شدند.

- **سیاست‌های کلان امنیتی**

امنیت در سیستم کارت هوشمند ملی تابع مجموعه‌ای از اصول و خط‌مشی‌ها است. این اصول در کلیه مراحل و سطوح جاری خواهد بود و بر اساس اقتضای هر بخش نمود متناسب با آن بخش را خواهد داشت. یکی از مهمترین اصول

حاکم بر فعالیتهای امنیتی که در هر شأنی و در هر مرحله‌ای بصورت یکپارچه پیگیری می‌گردد نگاه منسجم و یکپارچه به راه‌حلهای امنیتی در کل سیستم است. شئون مختلف عبارتند از: راه حل امنیتی، پیکربندی ، نقشها، پرسنل ، واسط کاربری و مراحل کلی عبارتند از: طرح نیازمندی ، تحلیل مخاطرات ، طراحی راه‌حل ، پیاده‌سازی راه حل ، بهره‌برداری از سیستم.

لازم است مدیریت امنیت در پروژه کارت هوشمند ملی سه حوزه مشخص مدیریت، عملیات و فناوری را پوشش دهد. بر این اساس در هر یک از این سه حوزه، معیارهای امنیتی مشخصی باید مبنای عمل قرار گیرد. این معیارها مطابق جدول زیر است:

حوزه	معیارهای امنیتی
امنیت در حوزه مدیریت	انتصاب مسؤولیتها استمرار پشتیبانی ظرفیت پاسخ به رخداد بازنگری و مرور کنترلهای امنیتی تأیید صلاحیت پرسنل و بررسی پیشینه آنها ارزیابی مخاطرات آموزشهای امنیتی و فنی تفکیک وظایف تأیید سطح اختیارات سیستمی و بازنگری آنها[5] طرح امنیت سیستم و کاربرد
امنیت در حوزه عملیات	حفاظت فیزیکی از امکانات توزیع و برچسب‌گذاری داده‌های خارجی کنترل شرایط زیست محیطی محیط کنترل جهت اطمینان از کیفیت منابع تغذیه برق مهیا بودن و دسترسی به رسانه حاوی داده
امنیت در حوزه فنی	حفاظت از ارتباطات رمزنگاری بنا بر نیاز کنترل دسترسی شناسایی و تأیید هویت کشف نفوذ استفاده مجدد از اشیاء ممیزی سیستمی

- **استقرار سامانه خدمات شهروندی**

سامانه خدمات شهروندی با معماری مبتنی بر وب و با توجه به لایه های معماری راه اندازی شد.

شهروندان برای استفاده از خدمات پورتال سامانه خدمات شهروندی کافی است دارای یک کامپیوتر خانگی باشند که به شبکه اینترنت متصل و دارای مرورگر باشد. در دفاتر پیشخوان و ادارات ثبت احوال نیز اپراتورها برای دسترسی به سیستم های CCOS و S۳ کافی است که برروی ایستگاههای کاری خود مرورگر داشته باشند. البته تجهیزاتی مانند «کارت خوان » و «سنسور دریافت اثر انگشت » نیز باید به ایستگاههای کاری پیشخوان متصل گردند.

- **استانداردها و تکنولوژی ها**

استانداردها و تکنولوژی های مورد استفاده در سامانه خدمات شهروندی به قرار زیر می باشند:

عنوان	استاندارد/تکنولوژی
متد طراحی	Object Oriented
متدولوژی توسعه نرم افزار	RUP
نماد مدلسازی	UML 2.0
مدیریت امنیت	ISO 27002
لایه بندی	3-Layer
سبک	Web-Base
پایگاه داده	Oracle 11g
سکوی نرم افزار	J2EE
فناوری واسط کاربری	Java Activex
کدینگ زبان فارسی	UTF-8
مرورگر اینترنت	IE/Firefox/ Chrome
پروتکل شبکه	TCP/IP
سیستم عامل سمت سرور	Linux
سیستم عامل سمت کاربر	Win XP/ 7
تصویر چهره	ISO/IEC FCD 19794-5
کیفیت و فرمت اثرانگشت	FBI IAFIS IQS CJIS-RS-0010(V7) Appendix F Compliance NFIQ ANSI/NIST-ITL 1-2007 ISO/IEC FCD 19794-4 ANSI/NIST-ITL 1-2000 ANSI/NIST-ITL 1-2000 Interpol Implementation
فشرده سازی تصویر	IS 10918-1 Joint Photographic Experts Group (JPEG) ISO 15444-1 JPEG 2000 IAFIS-IC-0110 (v3) Wavelet Scalar Quantization