



دانشگاه قم  
دانشکده مهندسی کامپیوتر  
پایان نامه دوره کارشناسی ارشد  
رشته فناوری اطلاعات  
گرایش تجارت الکترونیک

**عنوان:**

**بررسی انواع معماری های زیر ساخت کلید عمومی و  
ارائه یک معماری زیر ساخت کلید عمومی مناسب و  
منطبق با زیر ساخت های ایران**

**استاد راهنما:**

**دکتر علی اصغر عمیدیان**

**استاد مشاور:**

**دکتر حمیدرضا ربیعی**

**نگارنده:**

**امینه مقصودی خسروشاهی**

**پاییز 90**

تقدیم به

پدر و مادر عزیزم،

که یار و یاور همیشگی من بوده‌اند و

همسرم که همیشه حمایتم کرده است.

## تشکر و قدردانی

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود. در اینجا برخود لازم می‌دانم از تمامی اساتید بزرگوار، به ویژه اساتید دوره کارشناسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت و فضائل اخلاقی یاری نموده‌اند تقدیر و تشکر نمایم.

از استاد گرامی و بزرگوار جناب آقای دکتر علی‌اصغر عمیدیان که راهنمایی اینجانب را در انجام تحقیق، پژوهش و نگارش این پایان نامه تقبل نموده‌اند نهایت تشکر و سپاسگزاری را دارم.

از جناب آقای دکتر حمیدرضا ربیعی به عنوان مشاور که با راهنمایی خود مرا مورد لطف قرار داده‌اند کمال تشکر را دارم.

## چکیده

با رشد فناوری اطلاعات و ارتباطات و پیچیده‌تر شدن زندگی بشر، برای پاسخ به این پیچیدگی، دولت‌ها ناگزیر به ایجاد دولت الکترونیک می‌باشند. در حال حاضر کشور ما نیز نیازمند ورود به عرصه دولت الکترونیک است، برای ورود کشور به این عرصه صدور گواهینامه‌های الکترونیکی برای کاربران دولت الکترونیک امری ضروری است. از این رو برای صدور گواهینامه‌های الکترونیکی در کشور اقدام به ایجاد مراکز موسوم به مراجع صدور گواهینامه الکترونیکی شده است. به دلیل وجود ارتباطات مختلف مابین عناصر دولت الکترونیک جهت حفظ یکپارچگی و سهولت در این ارتباطات، ایجاد و افزایش چنین مراکزی باید به صورت یکپارچه و تحت یک مدیریت مرکزی و سیاست‌های یکسان انجام شود. برای این امر نیازمند وجود یک معماری مناسب (مدل اعتماد) برای زیرساخت کلید عمومی کشور هستیم. در این پروژه سعی شده است با غلبه بر چالش‌های موجود در این مسأله و ارزیابی مدل‌های اعتماد مختلف بر اساس پارامترهای مهم ارزیابی، یک مدل اعتماد تکاملی برای زیرساخت کلید عمومی کشور ارائه گردد. مدل ارائه شده منطبق بر زیرساخت‌های قانونی و فنی موجود در کشور بوده و ضعف‌های معماری موجود را پوشش می‌دهد. از سوی دیگر با توجه به اینکه با گذر زمان و افزایش کاربردهای فناوری اطلاعات و ارتباطات در کشور نیازمندی‌های جدیدی ایجاد خواهد شد، مدل ارائه شده به جهت حالت تکاملی خود امکان گسترش بهینه زیرساخت کلید عمومی در کشور را فراهم می‌کند. حالت تکاملی مدل باعث سهولت در گسترش کاربردهای زیرساخت کلید عمومی و افزایش زیرساخت‌های کلید عمومی جدید در کشور خواهد شد.

**کلمات کلیدی:** زیرساخت کلید عمومی، گواهینامه الکترونیکی، معماری (مدل اعتماد)،

مرکز صدور گواهی‌نامه الکترونیکی

## فهرست مطالب

چکیده.....	و
1-مقدمه.....	2
1-1 مفاهیم اولیه زیر ساخت کلید عمومی.....	4
1-1-1 امضای دیجیتال.....	4
2-1-1 زیرساخت کلید عمومی.....	8
3-1-1 گواهینامه‌های الکترونیکی.....	10
4-1-1 اجزای زیرساخت کلید عمومی.....	14
5-1-1 عملکردهای اصلی زیرساخت کلید عمومی.....	18
6-1-1 مدل اعتماد زیرساخت کلید عمومی.....	28
2-1 بیان مسئله.....	29
3-1 ساختار پایان‌نامه.....	30
2- مدل‌های اعتماد موجود و اقدامات انجام شده در کشور.....	32
1-2مقدمه.....	32
2-2 انواع مدل‌های اعتماد زیرساخت کلید عمومی.....	32

- 33 ..... 1-2-2 مدل مرجع صدور گواهی واحد
- 34 ..... 2-2-2 مدل سلسله مراتبی
- 36 ..... 3-2-2 مدل مش (گواهی متقابل)
- 38 ..... 4-2-2 مدل پل
- 40 ..... 5-2-2 مدل ترکیبی
- 41 ..... 6-2-2 مدل وب (لیستهای اعتماد)
- 44 ..... 7-2-2 مدل کاربر محور
- 45 ..... 8-2-2 مدل به رسمیت‌شناسی متقابل
- 47 ..... 9-2-2 مدل اعتماد مبتنی بر مراجع صدور گواهینامه دروازه
- 3-2 مدل‌های زیرساخت کلید عمومی دولتی کشورهای مختلف پیشرو در زمینه زیرساخت  
49 ..... کلید عمومی
- 49 ..... 1-3-2 ایالات متحده آمریکا
- 53 ..... 2-3-2 کانادا
- 54 ..... 3-3-2 انگلستان
- 56 ..... 4-3-2 فنلاند

57	..... 5-3-2 سنگاپور
58	..... 6-3-2 ژاپن
61	..... 7-3-2 بلژیک
62	..... 8-3-2 استونی
64	..... 9-3-2 پر تغال
66	..... 10-3-2 کره جنوبي
67	..... 4-2 تحليل مقايسه‌اي انواع مدل‌ها بر اساس پارامترهاي آريزايي
72	..... 5-2 اقدامات انجام شده در کشور
72	..... 1-5-2 اقدامات قانونی
80	..... 2-5-2 اقدامات فنی
86	..... 6-2 مدل اعتماد موجود در کشور
86	..... 1-6-2 نقاط ضعف مدل موجود
87	..... 7-2 جمع‌بندی و نتیجه‌گیری
91	..... 3- مدل پیشنهادی
91	..... 1-3 مقدمه



91	2-3 نکات کلیدی برای آغاز ایجاد زیرساخت کلید عمومی دولتی
95	3-3 ویژگی‌های کلی زیرساخت کلید عمومی دولتی
97	4-3 پارامترهای مهم در انتخاب مدل اعتماد در کشور
101	1-4-3 ارزیابی مدلها بر اساس پارامترهای مهم در کشور
104	5-3 ارائه مدل اعتماد مناسب و تعیین سازمان‌های متولی مراجع صدور گواهینامه
106	1-5-3 مرحله اول
117	2-5-3 مرحله دوم
120	3-5-3 مرحله سوم
123	4-5-3 مرحله چهارم
123	6-3 مسائل مربوط به طرح پیشنهادی
128	4- نتیجه‌گیری و کارهای آتی
128	1-4 جمع‌بندی
131	2-4 کارهای آتی
132	مراجع
137	واژه‌نامه

## فهرست شکل‌ها

- شکل 1-1 الگوی مفهومی امضای دیجیتالی مبتنی بر چکیده پیام.....6
- شکل 2-1 گواهینامه الکترونیکی.....11
- شکل 3-1 ساختار کلی ورژنهای مختلف یک گواهینامه دیجیتالی x.509.....14
- شکل 4-1 موجودیت‌های زیرساخت کلید عمومی.....15
- شکل 5-1 مثالی از مسیر اعتباردهی گواهینامه.....20
- شکل 6-1 لیست ابطال گواهینامه X.509.....27
- شکل 1-2 ساختار مفهومی مدل مرجع صدور گواهینامه واحد.....33
- شکل 2-2 مدل سلسله مراتبی.....35
- شکل 3-2 مدل مش کامل.....37
- شکل 4-2 شکل دیگری از مدل مش.....37
- شکل 5-2 مدل پل.....39
- شکل 6-2 مدل ترکیبی مدل‌های دیگر با مدل پل.....40
- شکل 7-2 لیست مراجع صدور گواهینامه مورد اعتماد در مرورگر Netscape.....42
- شکل 8-2 مراجع صدور گواهینامه مورد اعتماد در مرورگر Microsoft Explorer.....42

- شکل 9-2 ساختار مفهومی مدل لیست‌های اعتماد..... 44
- شکل 10-2 ساختار مفهومی مدل رسمیت‌شناسی متقابل..... 46
- شکل 11-2 ساختار مفهومی مدل مرجع صدور گواهینامه دروازه ..... 48
- شکل 12-2: معماری زیرساخت کلید عمومی فدرال ..... 50
- شکل 13-2 : FPKIPA و گروه‌های کاری..... 51
- شکل 14-2: نمایی از FBCA..... 52
- شکل 15-2: مدل اعتماد زیرساخت کلید عمومی دولت کانادا..... 54
- شکل 16-2: ساختار زیرساخت کلید عمومی فنلاند..... 57
- شکل 17-2: ساختار زیرساخت کلید عمومی ژاپن..... 59
- شکل 18-2: مدل زیرساخت کلید عمومی ژاپن..... 59
- شکل 19-2: معماری زیرساخت کلید عمومی بلژیک..... 62
- شکل 20-2: ساختار زیرساخت کلید عمومی استونی..... 63
- شکل 21-2: ساختار زیرساخت کلید عمومی دولتی پرتغال..... 65
- شکل 22-2: ساختار زیرساخت کلید عمومی کره..... 67
- شکل 23-2 مدل اعتماد زیرساخت کلید عمومی کشور در حال حاضر..... 86

شکل 2-24 وضعیت کنونی زیرساخت‌های کلید عمومی با مقیاس بزرگ ..... 89

شکل 3-1 ساختار مربوط به گواهینامه‌های کاربر نهایی ..... 109

شکل 3-2: ساختار کلی زیرساخت کلید عمومی دولتی در انتهای مرحله اول ..... 116

شکل 3-3: ساختار کلی زیرساخت کلید عمومی دولتی در انتهای مرحله دوم ..... 119

شکل 3-4 ساختار کلی زیرساخت کلید عمومی کشور در انتهای مرحله سوم ..... 122

## فهرست جدول‌ها

جدول 2-1 مقایسه اولیه‌ای مابین انواع مدل‌های اعتماد بر حسب پارامترهای ارزیابی.....69

جدول 3-1 مقایسه مابین مدل‌های اعتماد پرکاربرد بر حسب پارامترهای ارزیابی مهم در کشور.....101

جدول 3-2 مسائل مهم مطرح در انتخاب مدل اعتماد مناسب در کشور.....102

جدول 3-3 معایب و مزایای هر کدام از مدل بر حسب پارامترهای ارزیابی و مسائل مطرح در کشور.....103

فصل اول

مفاهیم اولیه

رویکرد خاصی مانند تامین امنیت اطلاعات دیجیتالی، یکی از موانع و چالش‌های اصلی در به کارگیری فناوری اطلاعات در سطوح مختلف مصرف‌کنندگان به شمار می‌رود.

دولت الکترونیکی روشی برای فراهم کردن دسترسی آسان شهروندان به اطلاعات و خدمات دولت و همچنین برای انجام کسب‌وکار داخلی دولت از طریق اینترنت است. مشکلی که روند پیشرفت سرمایه‌گذاری دولت‌ها در این حوزه را مختل می‌کند، طراحی باز<sup>۱</sup> اینترنت است که باعث سهولت در استراق سمع، رهگیری، نظارت و جعل ارتباطات بر روی اینترنت است. این موارد دلیل بی‌میلی شهروندان و دولت‌ها در استفاده از اینترنت برای داده‌های حساس مالی و قانونی است.

مسائلی که کاربران اینترنت با آن روبرو هستند به دو دسته<sup>۲</sup> محرمانگی<sup>۲</sup> و احراز هویت<sup>۳</sup> تقسیم می‌شوند. رمزنگاری<sup>۴</sup>، امضای دیجیتال<sup>۵</sup> و گواهی دیجیتال<sup>۶</sup> مکانیزم‌های مختلف پوشش دهنده<sup>۷</sup> سرویس‌های محرمانگی اطلاعات، احراز هویت، جامعیت داده<sup>۷</sup> و انکارناپذیری<sup>۸</sup> هستند.

رمزنگاری روشی امن برای حفاظت داده‌های دیجیتال در محیط‌های ناامن از دسترسی‌های غیرمجاز می‌باشد. ولی این روش‌ها هیچ اقدامی در راستای اعتبارسنجی محتوای متن و حفاظت از اطلاعات در مقابل تغییر و دستکاری آنها انجام نمی‌دهند.

یک شکل خاص از رمزنگاری که به عنوان رمزنگاری کلید عمومی<sup>۹</sup> شناخته شده است، نیازمندی‌های اینترنت را تکمیل می‌کند امضای دیجیتال روش دیگری است که از رمزنگاری بهره می‌گیرد. در مکانیزم امضای دیجیتال مبتنی بر کلید عمومی افراد از طریق کلید عمومی خود شناسایی می‌شوند. در نتیجه باید ارتباط قابل اطمینانی بین صاحب کلید و کلید وجود

---

<sup>1</sup> Open Design

<sup>2</sup> Privacy/Confidentiality

<sup>3</sup> Authentication

<sup>4</sup> Cryptography

<sup>5</sup> Digital Signature

<sup>6</sup> Digital Certificate

<sup>7</sup> Data Integrity

<sup>8</sup> Non-Repudiation

<sup>9</sup> Public Key Cryptography

داشته باشد. برای این منظور از گواهی الکترونیکی استفاده می‌شود که می‌تواند هویت یک شخص

را به کلید عمومی آن مرتبط سازد. این کار زیر نظر مرکز صدور گواهی دیجیتال<sup>1</sup> (CA) انجام خواهد شد. در حقیقت، گواهی دیجیتال یک بسته اطلاعاتی به فرمت مشخص (که حاوی اطلاعاتی شامل مشخصات صاحب گواهی، تاریخ صدور، تاریخ اعتبار، مشخصات صادر کننده گواهی، کلید عمومی، کاربرد گواهی و...) است که توسط یک مرکز و یا به عبارتی به وسیله یک کلید خصوصی امضا شده است.

هر مرکز صدور گواهی دیجیتال، دارای یک کلید عمومی<sup>2</sup> و یک کلید خصوصی<sup>3</sup> است که توسط کلید خصوصی گواهی کاربران را امضا و آن‌ها را منتشر می‌نماید. اعتبار این مراکز به صورت مستقیم یا غیر مستقیم، سلسله مراتبی یا درهم از طرف دولت‌ها تامین می‌شود. این مراکز می‌توانند به صورت متمرکز یا توزیع شده باشند. بدلیل گستردگی روزافزون تعاملات دیجیتالی و تامین امنیت آنها، نیاز به مراکز مختلف صدور گواهی دیجیتال شدیداً احساس می‌شود. گسترش این مراکز باید به صورتی باشد که هم اعتبار آنها کاهش پیدا نکرده و زیر سوال نرود و هم یکپارچگی آنها حفظ شود.

بهترین رویکرد برای صدور گواهینامه‌های دیجیتالی روشی است که به زیرساخت کلید عمومی<sup>4</sup> (PKI) شهرت یافته است و همچنین موضوع اصلی این پایان‌نامه می‌باشد. زیرساخت زیرساخت کلید عمومی یک سیستم کاربردی و قابل اعتماد برای انتشار کلیدهای عمومی ارائه می‌کند و همچنین اتصال مابین یک کلید عمومی منتشر شده و هویت نگهدارنده کلید را تضمین میکند. در این روش اتصال مابین یک کلید عمومی و نگهدارنده آن با امضای دیجیتالی یک موجودیت ثالث قابل اعتماد<sup>5</sup> تضمین می‌شود. یک موجودیت ثالث قابل اعتماد در یک زیرساخت کلید عمومی شبیه به دفاتر اسناد رسمی در جهان واقعی است. از این رو همه

---

<sup>1</sup> Certificate Authority (CA)

<sup>2</sup> Public Key

<sup>3</sup> Private Key

<sup>4</sup> Public Key Infrastructure (PKI)

<sup>5</sup> Trusted third party (TTP)



زیرساخت اصلی سیستم‌های کلید عمومی وابسته به یک یا چند نقطه اعتماد<sup>۱</sup> است، طراحی و چیدمان این نقاط اعتماد واقعاً یک چالش بوده و موضوع اصلی بحث ماست. طراحی و آرایش یک زیرساخت کلید عمومی زمانی که یک زیرساخت برای استفاده دولت مدل سازی می‌شود، بسیار مشکل است. ارتباطات مابین دولت در مقایسه با یک سازمان تجاری بسیار پیچیده است. هر سازمان دولتی باید برای انجام وظایفش با شهروندان، سازمانهای کسب و کار عمرانی و سازمان‌های دولتی در ارتباط باشد. زمانی که این ارتباطات در محیط الکترونیکی محقق می‌شود دولت باید بنا به طبیعت حساس وظایف خود، بسیار محتاط باشد.

## 1-1 مفاهیم اولیه زیر ساخت کلید عمومی

هدف از این فصل معرفی مفاهیم اولیه این پروژه است به نحوی که درک بیان مسئله آسان شود. این فصل به دو بخش تقسیم می‌شود. بخش اول با مروری کلی بر رمزنگاری و انواع آن، امضای دیجیتال و توابع درهم‌ساز<sup>۲</sup> آغاز می‌شود، سپس مفاهیم کلی و جزئیات فنی زیرساخت کلید عمومی اعم از اجزا و عملکردهای اصلی زیرساخت کلید عمومی، گواهی دیجیتال، خط-مشی‌ها و سیاست‌های گواهی‌نامه<sup>۳</sup> و توزیع و انتشار اخبار و اطاعیه‌های ابطال گواهی‌نامه ارائه شده و در بخش دوم مفهوم اعتماد<sup>۴</sup> برای زیرساخت کلید عمومی معرفی می‌شود و انواع مدل-های اعتماد<sup>۵</sup> زیرساخت کلید عمومی برای معماری‌های مختلف زیرساخت کلید عمومی تعریف می‌شود. ارائه این مطالب به جهت آشنایی با عملکردها و مدل‌های زیرساخت کلید عمومی و پایه‌ای برای ارائه مدل زیرساخت کلید عمومی دولتی است

### 1-1-1 امضای دیجیتال

مفهوم امضا در محیط‌های دیجیتالی با مفهوم امضا در محیط‌های سنتی تفاوت اصولی دارد و امضا در محیط‌های دیجیتالی باید بسته به محتوای داده مورد امضا برای هر نامه متفاوت

---

<sup>1</sup> Trust Anchor

<sup>2</sup> Hash Functions

<sup>3</sup> Certification Policy

<sup>4</sup> Trust

<sup>5</sup> Trust Models

باشد. روش‌های تولید و اعتبارسنجی امضاهای دیجیتال از طریق علم رمزنگاری امکان‌پذیر است. برای این منظور، از الگوریتم‌های نامتقارن و همچنین توابع درهم‌ساز استفاده می‌شود.

در دنیای مجازی امروز هر مکانیزمی که بتواند سه نیاز زیر را در خصوص اسناد و مدارک دیجیتال برآورده کند، «امضای دیجیتالی» نامیده می‌شود:

ا. دریافت‌کننده سند یا پیام الکترونیکی بتواند هویت صاحب سند را به درستی تشخیص دهد و از جعلی نبودن آن اطمینان حاصل کند.

ب. صاحب و امضاکننده سند بعداً نتواند محتوای سند یا پیام ارسالی خود را به هیچ طریقی انکار کند.

ج. یک متقلب شخص ثالث نتواند پیام‌ها یا اسناد جعلی تولید و آن‌ها را به دیگران منتصب کند.

نیازهای فوق در سیستم‌های اقتصادی و مرتبط با گردش پول و اعتبار حیاتی است و برای جلوگیری از هرگونه جعل و کلاهبرداری و حفظ منافع طرفین یک پیش‌نیاز به شمار می‌آید.

روش‌های متعددی برای پیاده‌سازی امضای دیجیتالی معرفی شده است که عبارتند از :

- امضاهای دیجیتالی مبتنی بر چکیده پیام؛ در این نوع مکانیزم بدون آن‌که محتوای سند رمزنگاری شود یا محرمانه ماندن آن مد نظر باشد یک امضای کوچک چند بایتی برای آن تولید می‌گردد.

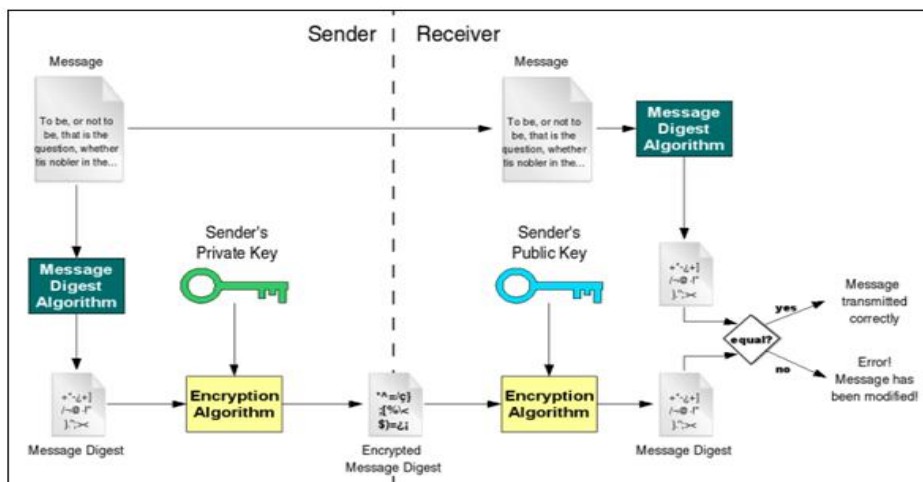
- امضاهای دیجیتالی کلید متقارن مبتنی بر یک مرکز مورد اعتماد برای گواهی امضاء.

- امضاهای مبتنی بر روش‌های رمزنگاری کلید عمومی.

- امضاهای مبتنی بر تبدیل‌های مستقل از سیستم‌های رمزنگاری.

امروزه در بسیاری از کشورها قوانین قضایی مستحکمی در ایجاد در ایجاد پشتوانه حقوقی برای امضاهای دیجیتالی وضع شده‌اند و دادگاه‌ها قادرند مناقشات حقوقی در این زمینه را بر اساس قوانین موجود حل و فصل کنند.

برای ایجاد امضای دیجیتال به ازای هر سند پس از مشخص کردن قالب استاندارد و دقیق برای اسناد، چکیده درهم‌فشرده شده آن را استخراج و پس از رمزنگاری با کلید خصوصی صاحب سند، به انتهای آن ضمیمه و ارسال شود. در این روش هیچ اخلاص‌گری قادر نیست در میانه راه در محتوای سند تغییری ایجاد کند. چرا که با تغییر در هر نقطه از پیام یا افزایش یا کاهش طول آن، چکیده آن تغییر خواهد کرد و گیرنده پس از محاسبه چکیده پیام و مقایسه آن با حاصل رمزگشایی شده امضاء، براحتی هرگونه هرگونه تغییرات احتمالی در پیام را تشخیص خواهد داد. شکل 1-1 نشان دهنده الگوی مفهومی امضای دیجیتالی است.



شکل 1-1 الگوی مفهومی امضای دیجیتالی مبتنی بر چکیده پیام

در امضای دیجیتالی مبتنی بر چکیده پیام برای رمزنگاری کلید عمومی از الگوریتم RSA استفاده می‌شود و برای تولید چکیده پیام الگوریتم SHA-1 بکار برده می‌شود. اگرچه این الگو برای امضای دیجیتال بسیار رایج است ولی روش‌های پیچیده‌تری هم در این زمینه وجود دارد.

«استاندارد امضای دیجیتالی (DSS)»<sup>1</sup> یکی از این روش‌هاست که توسط اداره استاندارد دولت فدرال آمریکا به ثبت رسیده است.<sup>2</sup> در این روش نیز از تابع درهم سازی SHA-1 برای محاسبه چکیده پیام استفاده شده ولی به جای رمزنگاری چکیده به روش RSA، از روش پیچیده‌تر «طاهرالجمال» استفاده شده است.

همانطور که میدانید، در یک سیستم رمزنگاری کلید عمومی کلیدهای خصوصی توسط صاحبان آن‌ها محرمانه نگه داشته می‌شوند، در حالی که کلیدهای عمومی متناظر با آن‌ها در یک انبار عمومی به نام صاحبانشان ذخیره می‌شوند. برای یک چنین سیستمی سؤالات احتمالی که باید پاسخ داده شود عبارتند از:

- چه کسی جفت کلید عمومی و خصوصی را تولید خواهد کرد؟
- قالب داده (کلید عمومی، هویت صاحب کلید عمومی و دیگر اطلاعات مربوطه) ذخیره شده در انبار (مخزن داده) چیست؟
- آیا مکانیزمی برای نگه داشتن این اطلاعات بدون تغییر در انبار وجود دارد؟
- چگونه می‌توان اتصال مابین کلید عمومی و هویت مدعی داشتن کلید عمومی را تضمین کرد؟
- چگونه کاربران به این انبارها دسترسی خواهند داشت؟
- چگونه کاربر از هر تغییر مخرب در داده‌های ذخیره شده در مخزن آگاه خواهند شد؟
- چه اتفاقی برای کلید عمومی که کلید خصوصی مرتبط با آن به خطر افتاده است (کشف رمز شده است) می‌افتد؟
- آیا سیاست‌هایی برای تمام مسائل فوق وجود خواهد داشت؟

<sup>1</sup> Digital Signature Standard

<sup>2</sup> در سند FIPS-180 و US Patent 5231668 در ژولای 1991