



IRAN-GRID Certification Authority

مرکز بین المللی تأیید هویت و صدور شناسنامه
دیجیتالی در ایران

Majid Arabgol
IRAN-GRID CA
Grid Computing Group
IPM

مجید عرب گل

آذر 1378

<http://cagrid.ipm.ac.ir>



- امنیت در **grid** و سطح دسترسی
- فناوری **PKI** – شناسنامه دیجیتالی
- ایجاد یک مرکز مورد اعتماد برای تأیید هویت (**CA**)
- **IGTF** مرکز بین المللی قانون گذار برای **CA** های معتبر
- **IRAN-GRID Certification Authority**
- خلاصه و جمع بندی



امنیت در grid و سطح دسترسی

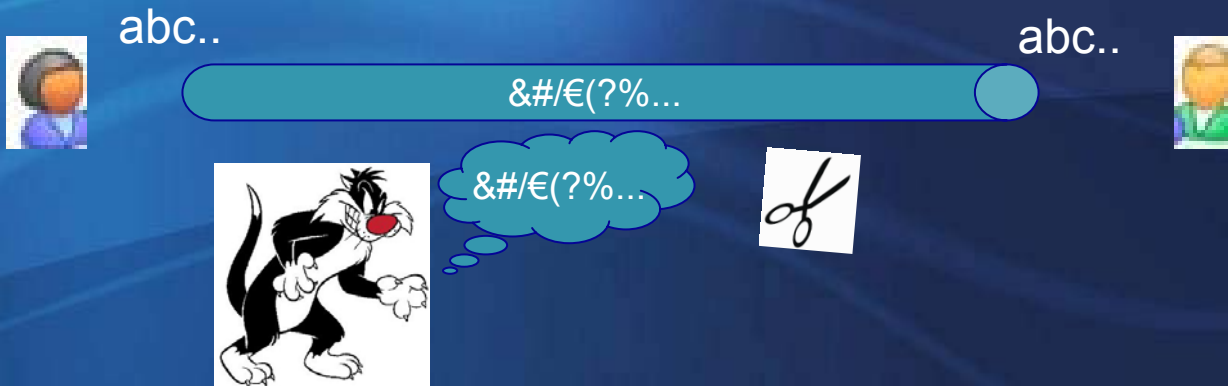
- grid یک سیستم توزیع شده (مدیریت مرکزی وجود ندارد)
- تبادل امن اطلاعات بین دو پایانه
- هویت کاربر Identification
- شناسایی کاربر Authentication
- شناسنامه دیجیتالی Digital Certificate
- مجوز استفاده از منابع Authorization
- یک بار ورود single sign on



تبادل امن اطلاعات بین دو پایانه

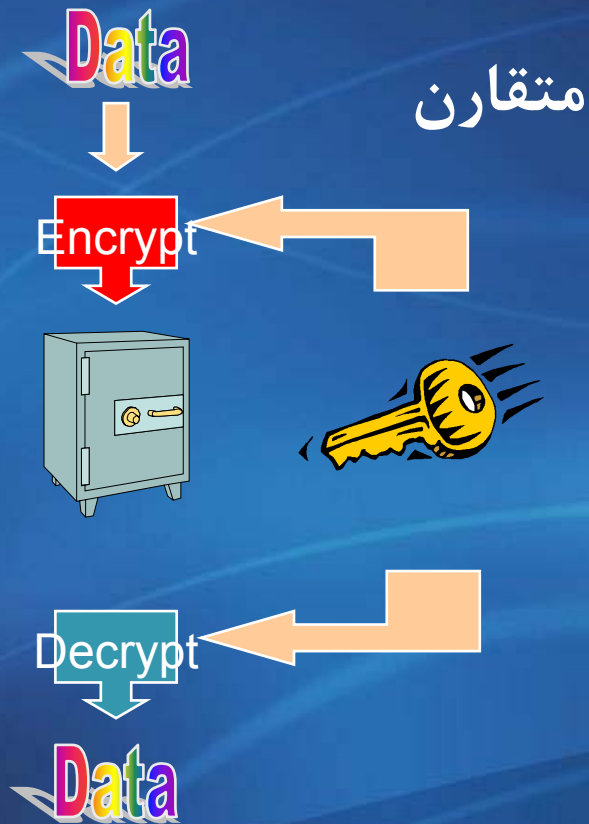


- محرمانه **privacy**
- تحریف پیام قابل تشخیص باشد **integrity**
- رمز کردن پیام با استفاده از کلید محرمانه **cryptography**





تبادل امن اطلاعات بين دوپايانه





فناوری Public Key Infrastructure(PKI)

• با رمز گذاری نا متقارن هر کسی می تواند دو عدد کلید داشته باشد.

• کلید عمومی – قابل کپی برداری برای همه

• کلید خصوصی – فقط نزد صاحب آن باید باشد

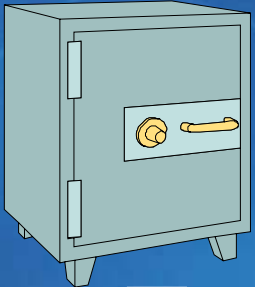




فناوری Public Key Infrastructure(PKI)

Data

Encrypt



Decrypt

Data



- هر پیامی که با کلید عمومی رمز شود توسط کلید خصوصی رمز گشائی می شود و بر عکس
- کلید خصوصی فقط نزد صاحب آن است و تنها صاحب آن می تواند رمز گشائی کند (محرمانه)



فناوری Public Key Infrastructure(PKI)

message



Secure Hash



Encrypt



Signature



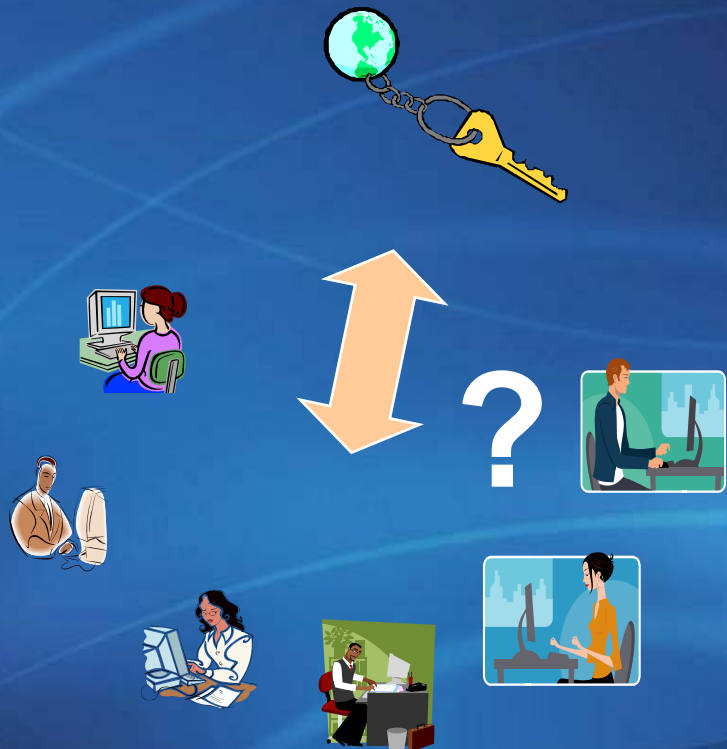
امضای دیجیتالی digital signature

در صورت تحریف پیام قابل تشخیص

فرستنده یا امضا کننده قابل تشخیص است - فقط با کلید عمومی فرستنده قابل فهم است



شناسنامه دیجیتالی Digital Certificate



سوال اساسی : از کجا می توان
مطمئن شده کلید عمومی یک کاربر
مشخص حقیقتا متعلق به همان
شخص است ؟

شناسنامه دیجیتالی



شناسنامه دیجیتالی Digital Certificate

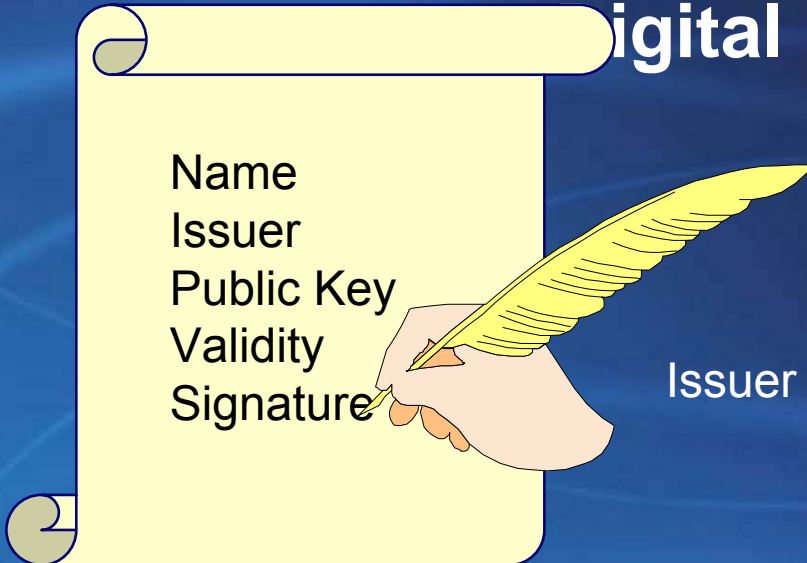
Name= Majid Arabgol
Issuer= IRAN-GRID
Public Key =10100011
Validity =10 December 09
Signature = signed by IRAN-GRID

- شناسنامه دیجیتالی مشابه گذرنامه یا گواهینامه
- استاندارد شناسنامه دیجیتالی به فرمت X.509 است (RFC3280)



شناسنامه دیجیتالی Digital Certificate

Name
Issuer
Public Key
Validity
Signature



Issuer

شناسنامه ها توسط یک مرجعی
به نام **certification Authority**
امضا می شوند

اعتبار یک شناسنامه با کلید
عمومی CA قابل شناسائی است
تحریف در شناسنامه امکان پذیر
نیست





مرجع تائید هویت و صدور شناسنامه دیجیتالی

Certification Authority

مولفه های اصلی یک CA

• متقاضی Subscriber

• مرجع تائید هویت (RA) Registration Authority

• مرجع امضا و صدور شناسنامه (CA) Certification Authority

• مخزن اطلاعات on line Repository

• استفاده کنندگان (کاربران) شناسنامه های دیجیتالی Relying

Party

• آئین نامه و نحوه صدور شناسنامه Certificate Policy and

Certificate Practice Statement (CP/CPS)



مرجع تأیید هویت و صدور شناسنامه دیجیتالی Certification Authority وظایف Certification Authority(CA)

- امضا و صدور شناسنامه دیجیتالی
- ارسال شناسنامه به متقاضی
- ابطال شناسنامه در صدور لزوم و مطابق آئین نامه
- صدور لیست شناسنامه های باطل شده
- ایجاد یک website برای نگهداری شناسنامه ها معتبر و باطل شده



مرجع تائید هویت و صدور شناسنامه دیجیتالی Certification Authority وظایف Registration Authority (RA)

- تائید هویت متقاضی محلی Authentication
- تشخیص صلاحیت متقاضی برای شناسنامه دیجیتالی
- ارسال کلید عمومی متقاضی تائید شده به CA برای امضا

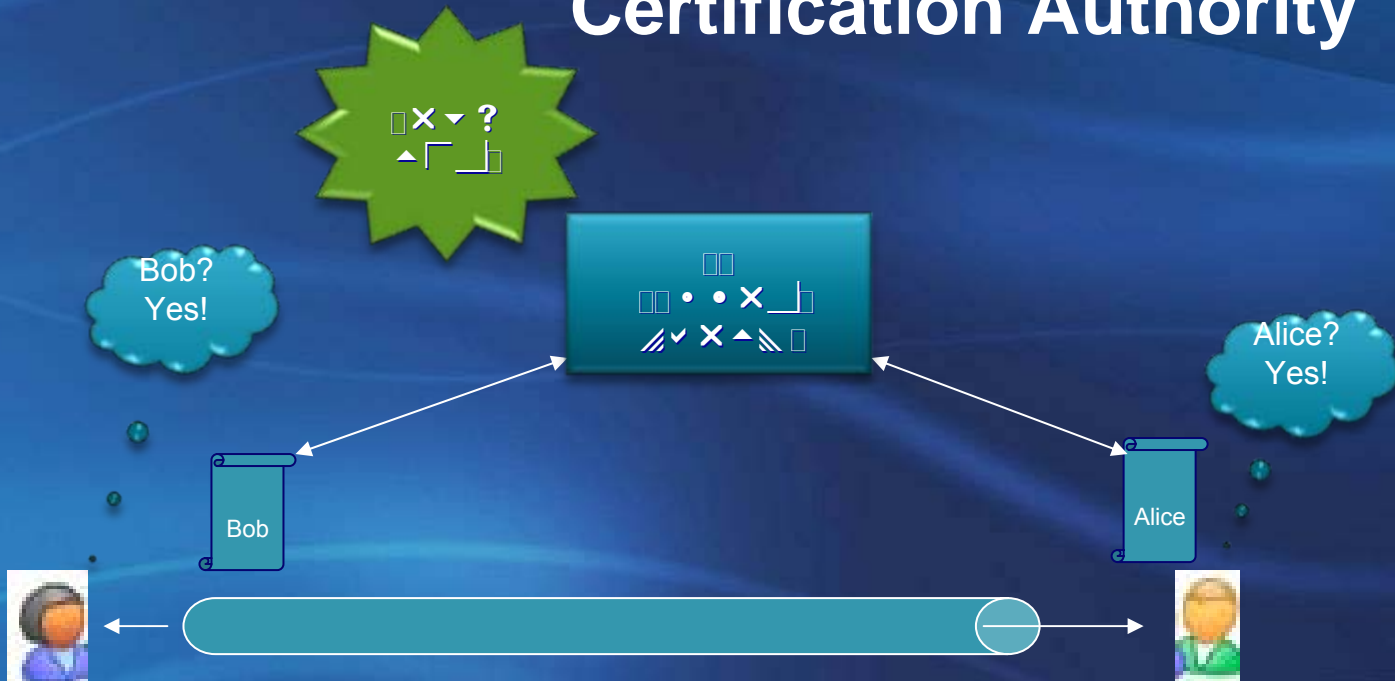


مرجع تأیید هویت و صدور شناسنامه دیجیتالی Certification Authority چرخه صدور شناسنامه دیجیتالی در یک CA





مرجع تأیید هویت و صدور شناسنامه دیجیتالی Certification Authority





International Grid Trust Federation (IGTF)

● مرجع قانون گذار برای CA های که شناسنامه دیجیتالی صادر می کنند

● این شناسنامه ها برای استفاده از grid به وسعت جهانی معتبر خواهند بود

● IGTF به هیچ وجه شناسنامه صادر نمی کند ولی تضمین می کند اعضای آن و شناسنامه های که توسط اعضا آن صادر می شود قابل اعتماد هستند

● <http://www.igtf.net>



International Grid Trust Federation (IGTF)



IGTF به منطقه سه جغرافیای تقسیم شده:

آسیا و اقیانوسیه APgridPMA
<http://www.apgridpma.org/>

اروپا EUgridPMA
<http://www.eugridpma.org>

امریکا TAGPMA (کانادا - آمریکای شمالی - مرکزی و جنوبی)
<http://www.tagpma.org/>



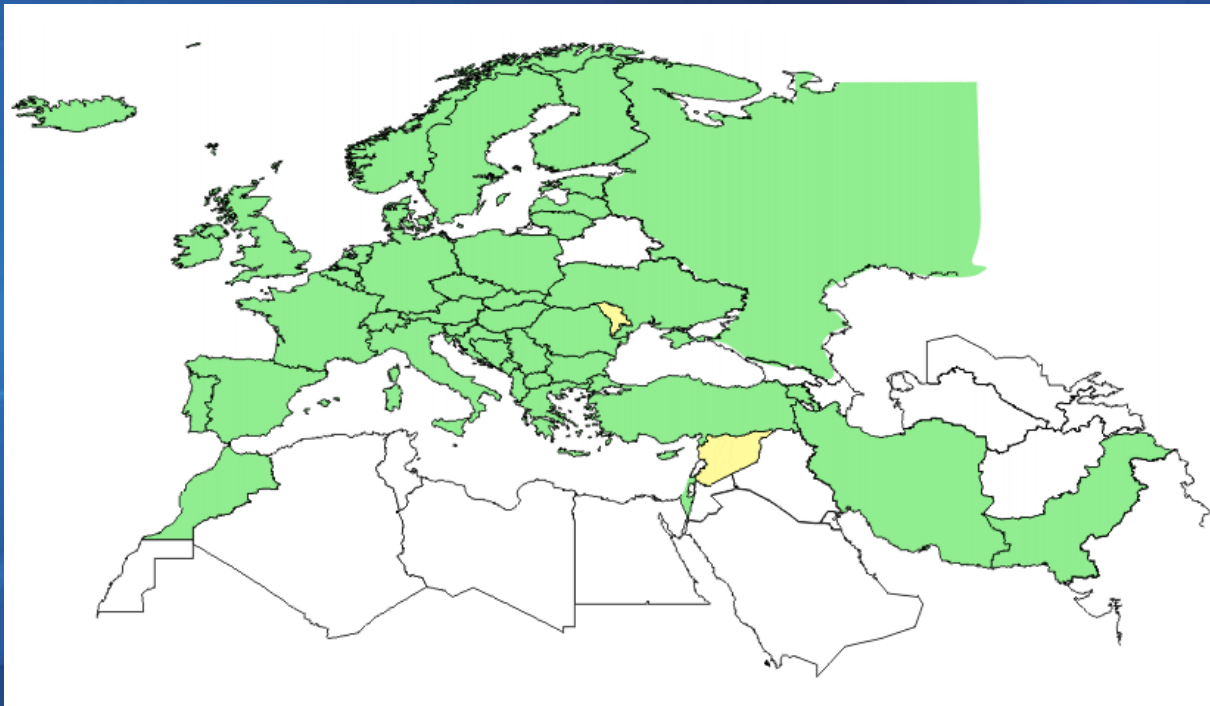
International Grid Trust Federation (IGTF)

- اعضای هر منطقه جغرافیائی هر ۴ ماه یک نشست دارند و هر نشست اساسنامه خود را با توجه به آخرین تغییرات فناوری **grid** در جهان به روز می کنند.
- در این نشست ها تقاضای اعضای جدید بررسی می شود و بر اساس رای دیگر اعضا عضو جدید پذیرفته می شود.
- معمولا از هر کشور یک **CA** به عنوان نماینده در **IGTF** پذیرفته می شود.



International Grid Trust Federation (IGTF)

<http://www.eugridpma.org/members/worldmap/> 





IRAN-GRID Certification Authority <http://cagrid.ipm.ac.ir>

- IRAN-GRID CA عضو از بخش اروپایی EUgridPMA
- IPM در خرداد ۱۳۷۷ تقاضای خود را برای عضویت فرستاد
- در اسفند ۱۳۷۷ در نشست دوازدهم IPM دلایل خود برای عضویت ارائه کرد.
- در خرداد ۱۳۷۸ در نشست سیزدهم IPM با ارائه آخرین دفاعیه خود ، به عنوان نماینده رسمی ایران در EUgridPMA پذیرفته شد.



IRAN-GRID Certification Authority

<http://cagrid.ipm.ac.ir>

- صدور شناسنامه دیجیتالی برای افراد حقیقی ، کامپیوتر و سرویس
- متقاضیان شناسنامه دیجیتالی باید عضو یک موسسه تأیید شده در ایران باشند.
- بر اساس آئین نامه جاری IRAN-GRID ، موسسات علمی ایران که زیر نظر وزارت علوم ، تحقیقات فناوری و وزارت بهداشت و علوم پزشکی می توانند عضو شوند
- IRAN-GRID CA به هیچ وجه برای پروژه های غیر علمی شناسنامه صادر نمی کند
- IRAN-GRID CA ۵ سال اعتبار دارد



IRAN-GRID Certification Authority

<http://cagrid.ipm.ac.ir>

IRAN GRID CA

Applying for certificate | CA certificate | Issued certificates | CRLs

» HOME

SEARCH IR GRID CA

- Policy Document (CP/CPS)
- CA Root Certificate
- Certificate Request
- Revoke Certificates
- Certificate Revocation Lists (CRLs)
- Authenticated Organizations
- Registration Authorities
- Contact us
- Links

IRAN-GRID Certificate Authority

IRAN-GRID Certification Authority is formed to provide X.509 certificates for identification and authentication purposes related to iranian grid activities in e-science.

The IRAN-GRID CA is established via **CMS experiment** collaboration. IRAN-GRID CA at beginning will issue certificates for person and host of any organization who has collaboration with LHC experiments, but later will cover other organization (see **authenticated organizations**) in other branch of sciences which deal with international grid collaboration.

IRAN-GRID CA, is hosted and managed by IPM Grid Computing Group (GCG). Users can request personal and host/service certificates via the web interface provided. Also



IRAN-GRID Certification Authority



Index of /distribution/igt/1.25/accredited/RPMS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://dist.eugridpma.info/distribution/igt/1.25/accredited/RPMS/

Most Visited Getting Started Latest Headlines

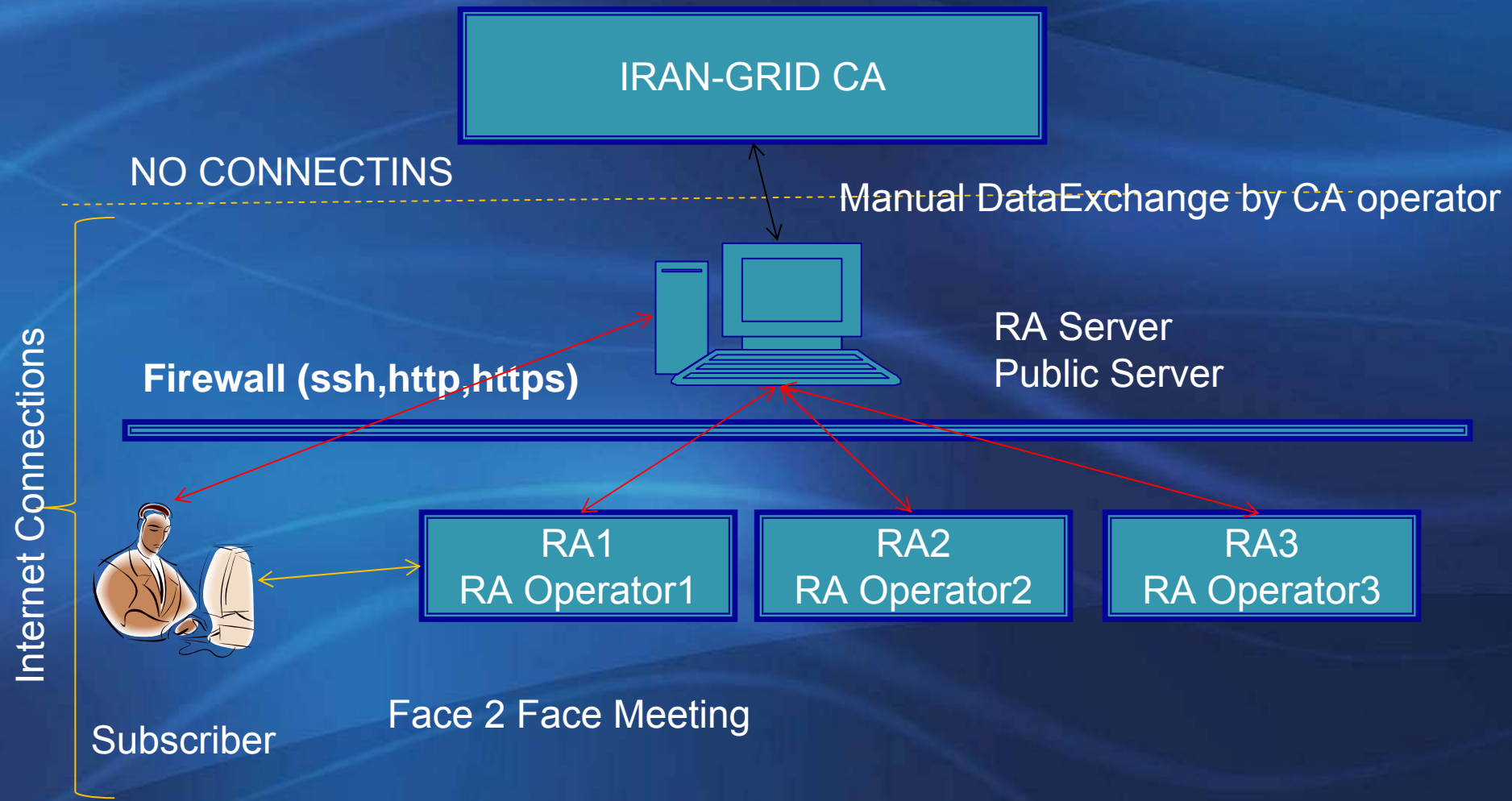
Google Search

ca DOEGrids-1.25-1.n...>	29-Sep-2008 08:46	5.2K
ca ESnet-1.25-1.noar...>	29-Sep-2008 08:46	5.1K
ca EstonianGrid-1.25...>	29-Sep-2008 08:46	4.3K
ca GermanGrid-1.25-1...>	29-Sep-2008 08:46	4.4K
ca Grid-Ireland-1.25...>	29-Sep-2008 08:46	4.3K
ca GridCanada-1.25-1...>	29-Sep-2008 08:46	4.3K
ca HellasGrid-CA-200...>	29-Sep-2008 08:46	4.3K
ca HellasGrid-Root-1...>	29-Sep-2008 08:46	4.3K
ca IHEP-1.25-1.noarc...>	29-Sep-2008 08:46	4.4K
ca INFN-CA-2006-1.25...>	29-Sep-2008 08:46	4.2K
ca IRAN-GRID-1.25-1...>	29-Sep-2008 08:46	4.2K
ca IUCC-1.25-1.noarc...>	29-Sep-2008 08:46	4.5K
ca KEK-1.25-1.noarch...>	29-Sep-2008 08:46	4.6K
ca KISTI-2007-1.25-1...>	29-Sep-2008 08:46	4.3K
ca LACGridCA-1.25-1...>	29-Sep-2008 08:46	4.4K
ca LIPCA-1.25-1.noar...>	29-Sep-2008 08:46	4.1K
ca MARGI-1.25-1.noar...>	29-Sep-2008 08:46	4.2K

ation Authority
[/cagrid.ipm.ac.ir](https://cagrid.ipm.ac.ir)

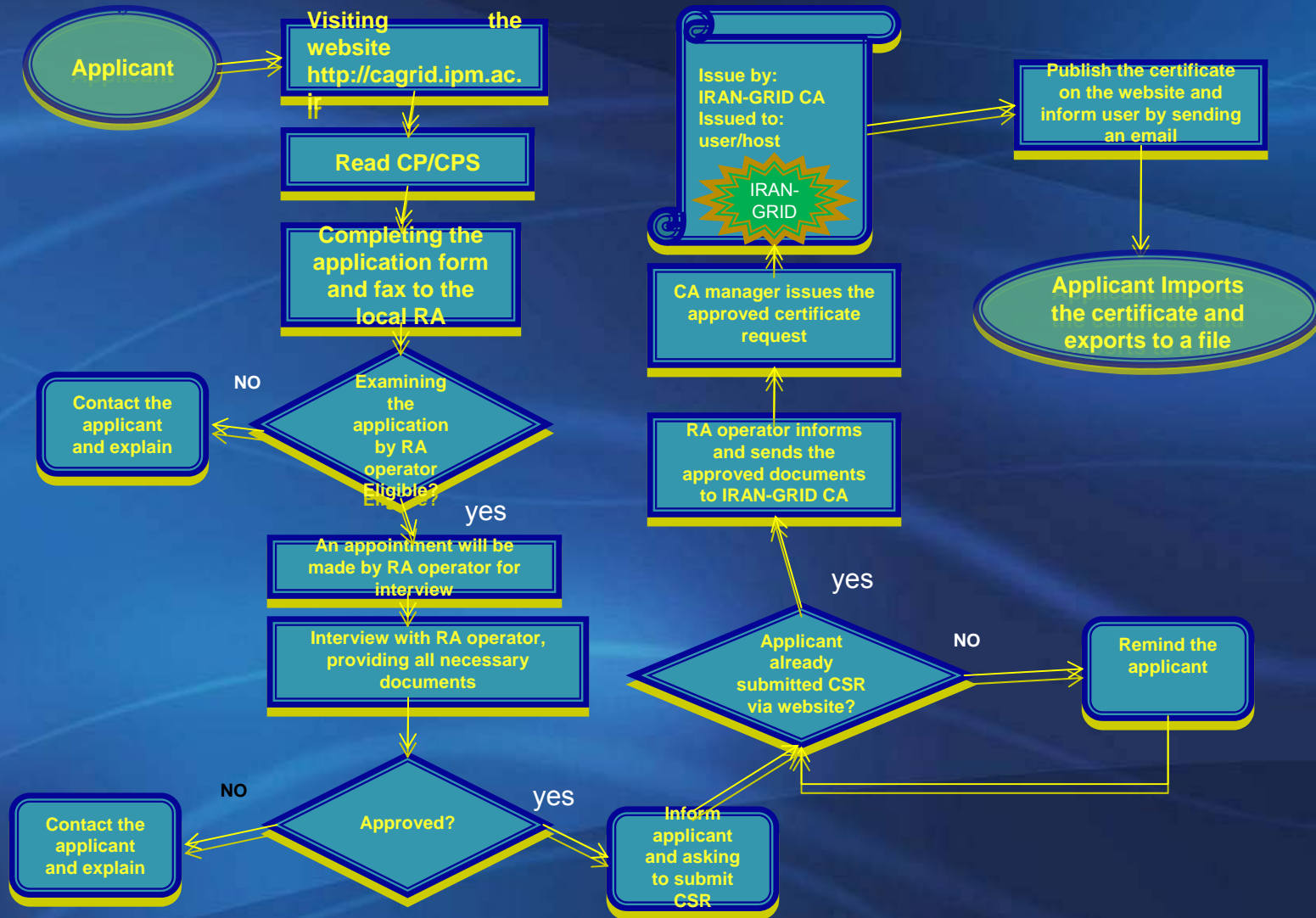


IRAN-GRID Certification Authority





IRAN-GRID Certification Authority





IRAN-GRID Certification Authority

<http://cagrid.ipm.ac.ir>

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x3)

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=IRAN-GRID, CA=IRAN-GRID, O=IPM, C=IR

Validity: Name= Majid Arabgol
Issuer= IRAN-GRID

Subject: Public Key = 1010001!
Validity = 10 December 09

Signature = signed by IRAN-GRID

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ec:07:5d:97:38:dc:e9:dd:0b:af:00:68:73:1a:



خلاصه و جمع بندی(1)

- در فناوری **grid** امنیت فرد، پروژه، داده، منابع یکی از مهمترین مسائل **grid** محسوب می شود
- تمامی اشیا در **grid** که از طریق **internet** تبادل اطلاعات می کنند توسط شناسنامه دیجیتالی شناخته می شوند
- شناسنامه های دیجیتالی باید توسط سازمان های معتبری بنام **Certification Authority** صادر شوند
- **CA** ها باید عضوی از **IGTF** باشند
- داشتن شناسنامه دیجیتالی به معنی دسترسی به منابع محاسباتی دنیا نیست!!



خلاصه و جمع بندی(2)

- IGTF سازمان بین المللی است که وظیفه آن تدوین قانون و نظارت بر CA های عضو خود را دارد
- IGTF به سه منطقه جغرافیائی آسیا، اروپا و آمریکا تقسیم می شود
- معمولا هر کشور یک نماینده می تواند در IGTF داشته باشد.
- هر کشوری که نیاز به فناوری grid در سطح برون مرزی دارد نیاز دارد نماینده ای در IGTF داشته باشد
- IRAN-GRID CA عضو اروپای IGTF است
- تلاش برای کسب اعتبار و پذیرفته شدن در IGTF (۳ سال)
- تاسیس IRAN-GRID CA صرفا برای نیاز آکادمیک ایران
- نگهداری و مسئولیت IRAN-GRID CA هزینه دارد



متشکرم

سوال؟