IRAN-GRID Certification Authority

مرکز بین المللی تائید هویت وصدور شناسنامه دیجیتالی در ایران

Majid Arabgol

IRAN-GRID CA

Grid Computing Group

IPM

http://cagrid.ipm.ac.ir

مجید عرب گل

آذر 1378

IRAN-GRID Certification Authority

GRID COMPUTING GROUP

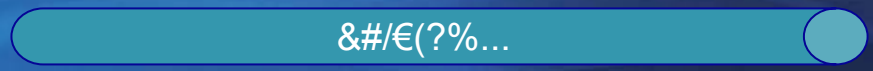
- امنیت در grid و سطح دسترسی
- فناوری PKI – شناسنامه دیجیتالی
- ایجاد یک مرکز مورد اعتماد برای تائید هویت (CA)
- IGTF مرکز بین المللی قانون گذار برای CA های معتبر
- IRAN-GRID Certification Authority
- خلاصه و جمع بندی

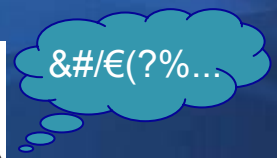
امنیت در grid و سطح دسترسی

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

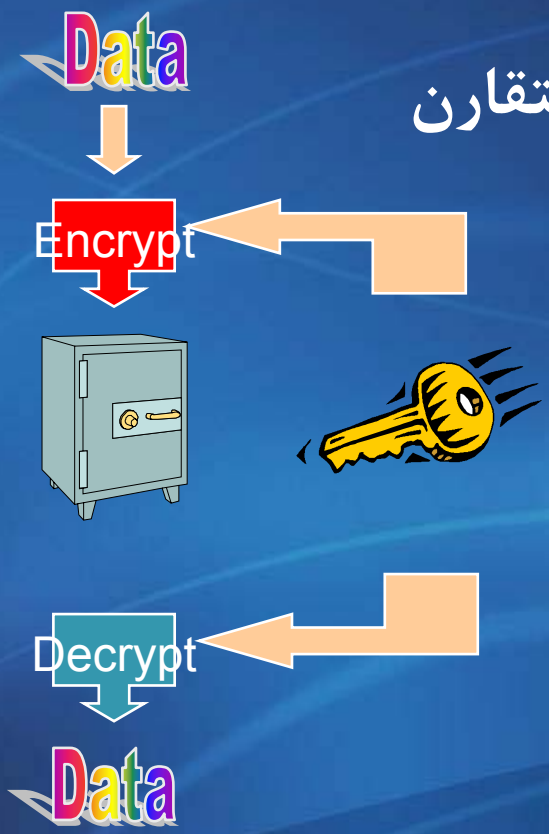
تبادل امن اطلاعات بین دوپایانه

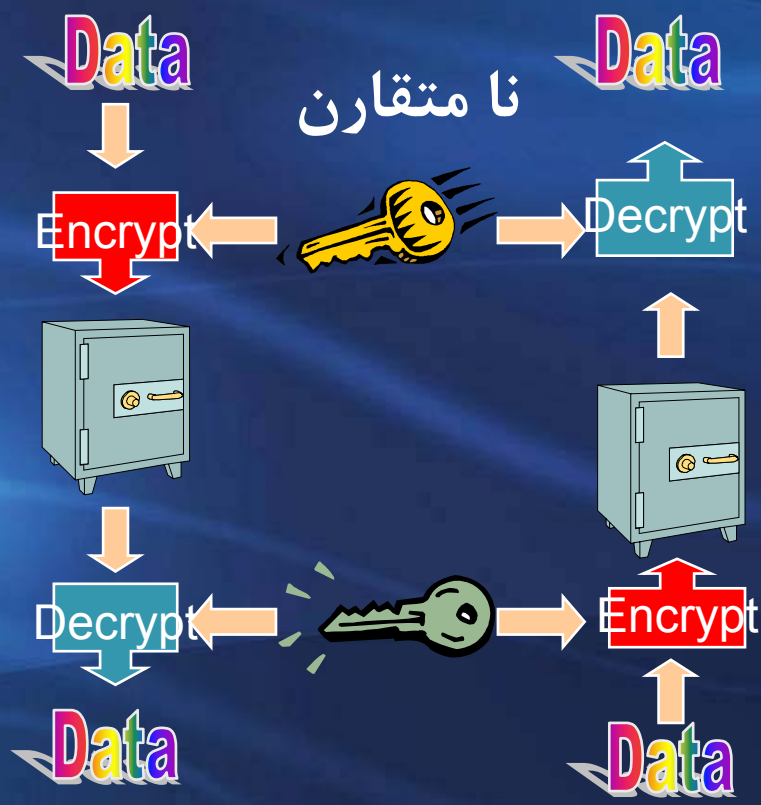
- محرمانه privacy
- تحریف پیام قابل تشخیص باشد integrity
- رمز کردن پیام با استفاده از کلید محرمانه cryptography





تبادل امن اطلاعات بین دوپایانه

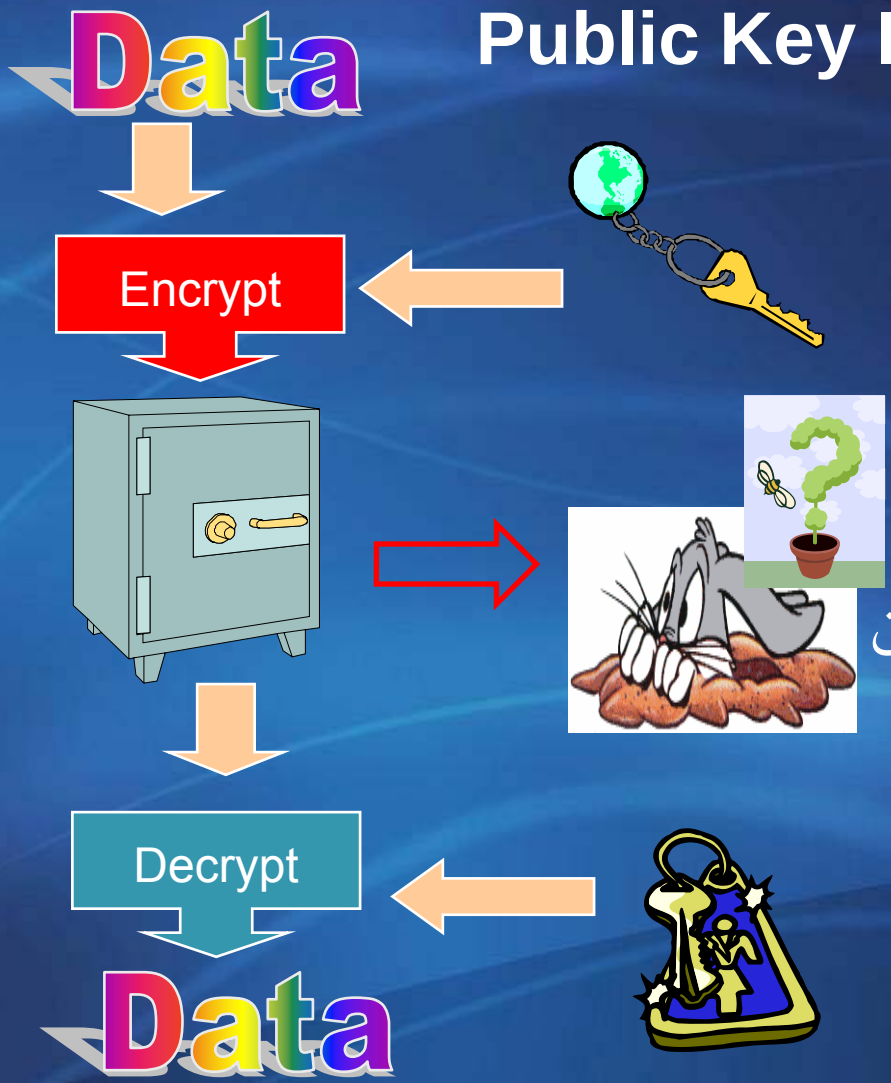




فناوری Public Key Infrastructure(PKI)

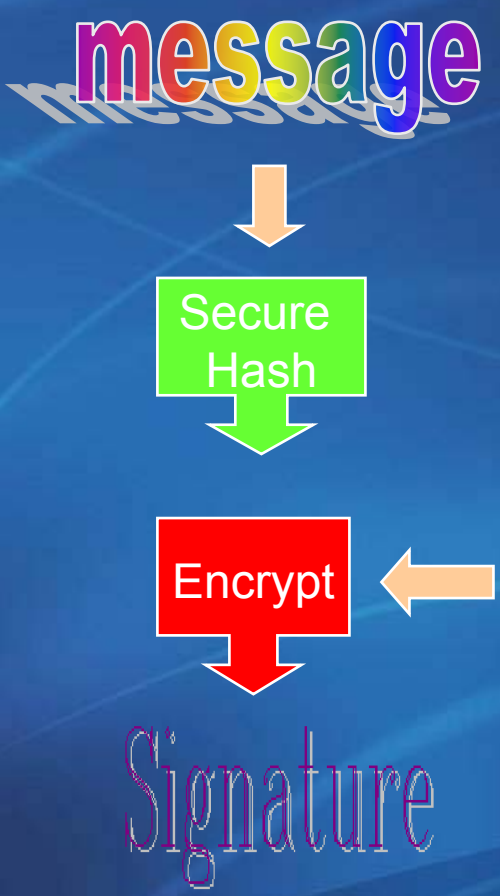
- با رمز گذاری نا متقارن هر کسی می تواند دو عدد کلید داشته باشد.
  - کلید عمومی – قابل کپی برداری برای همه
  - کلید خصوصی- فقط نزد صاحب آن باید باشد

Public Key Infrastructure(PKI) فناوری



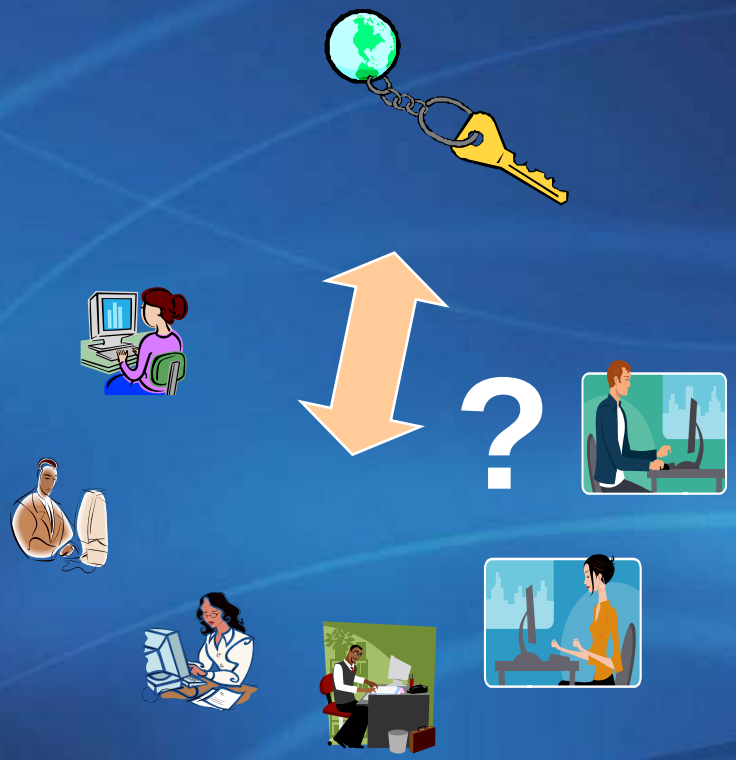
- هر پیامی که با کلیدعمومی رمز شود توسط کلید خصوصی رمز گشائی می شود و بر عکس
- کلید خصوصی فقط نزد صاحب آن است و تنها صاحب آن می تواند رمز گشائی کند(محرمانه)

Public Key Infrastructure(PKI) فناوری



- امضای دیجیتالی digital signature
- در صورت تحریف پیام قابل تشخیص
- فرستنده یا امضا کنند قابل تشخیص است - فقط با کلید عمومی فرستنده قابل فهم است

شناسنامه دیجیتالی Digital Certificate



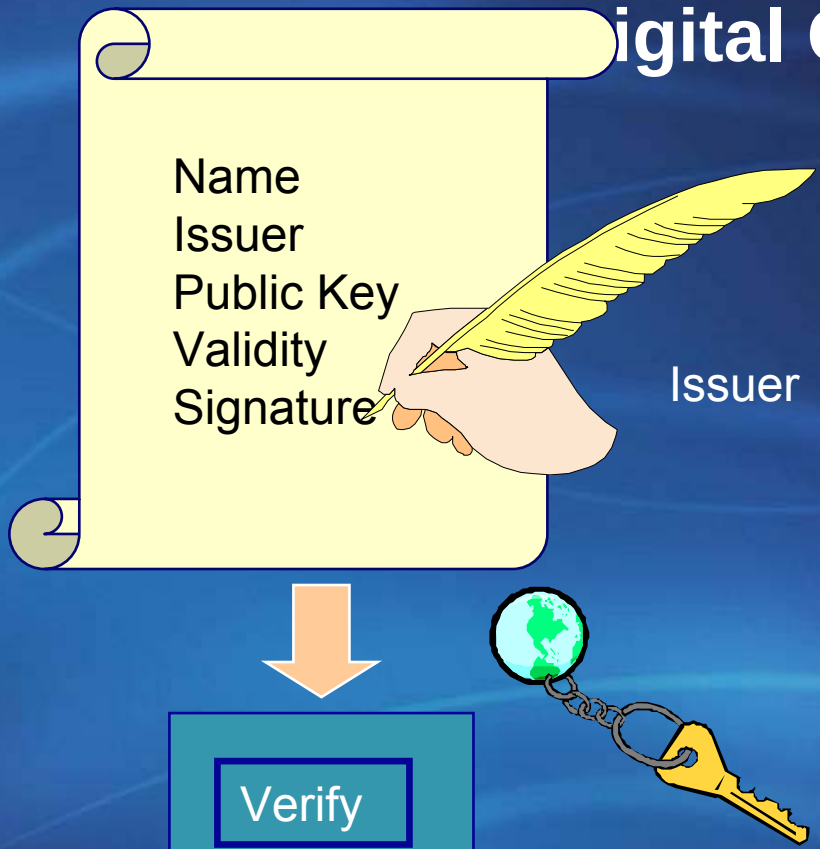
- سوال اساسی : از کجا می توان مطمئن شده کلید عمومی یک کاربر مشخص حقیقتا متعلق به همان شخص است ؟
- شناسنامه دیجیتالی

شناسنامه دیجیتالی Digital Certificate

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

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

شناسنامه دیجیتالی igital Certificate



- 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 Certification Authority(CA)
- مخزن اطلاعات on line Repository
- استفاده کنندگان (کاربران) شناسنامه های دیجتالی Relying Party
- آئین نامه و نحوه صدور شناسنامه Certificate Policy and Certificate Practice Statement (CP/CPS)

GRID COMPUTING GROUP

مرجع تائید 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 دیجتالی
- ارسال کلید عمومی متقاضی تائید شده به CA برای امضا

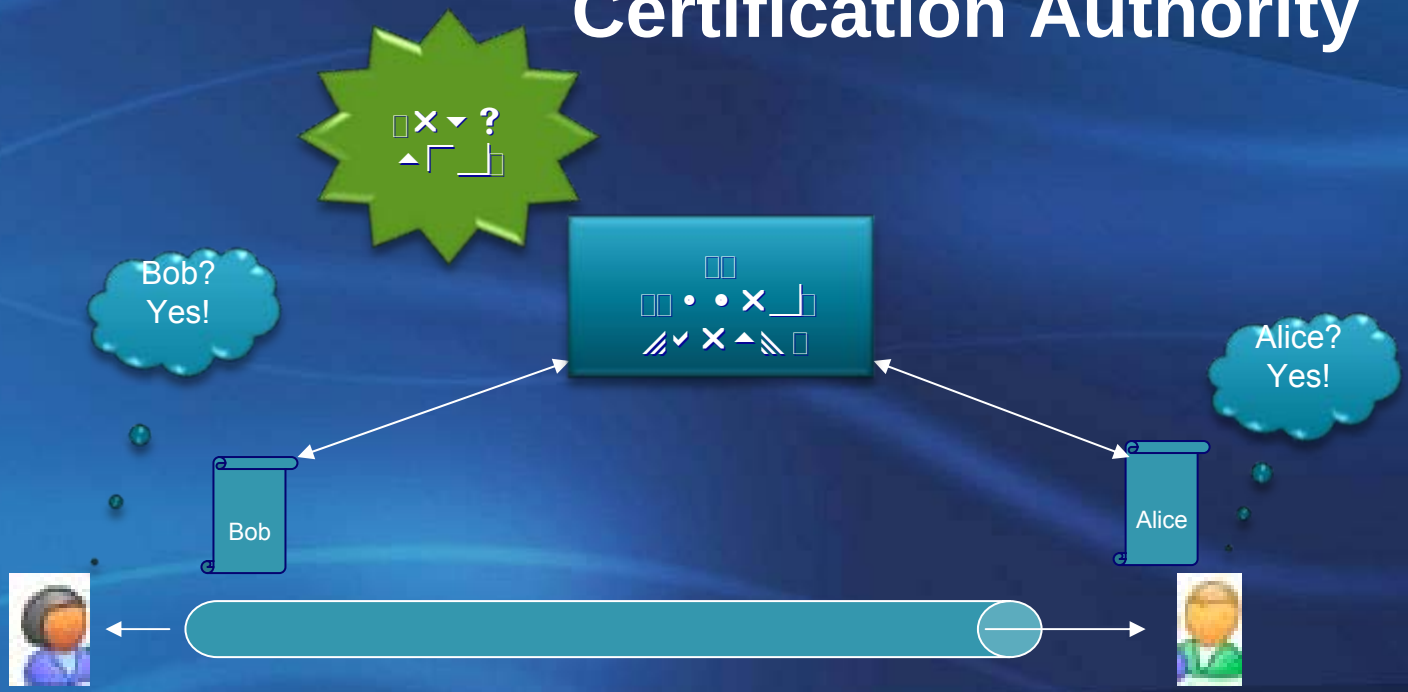
IRAN-GRID Certification Authority

GRID COMPUTING GROUP

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

مرجع تائید 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 صادرنمی 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)

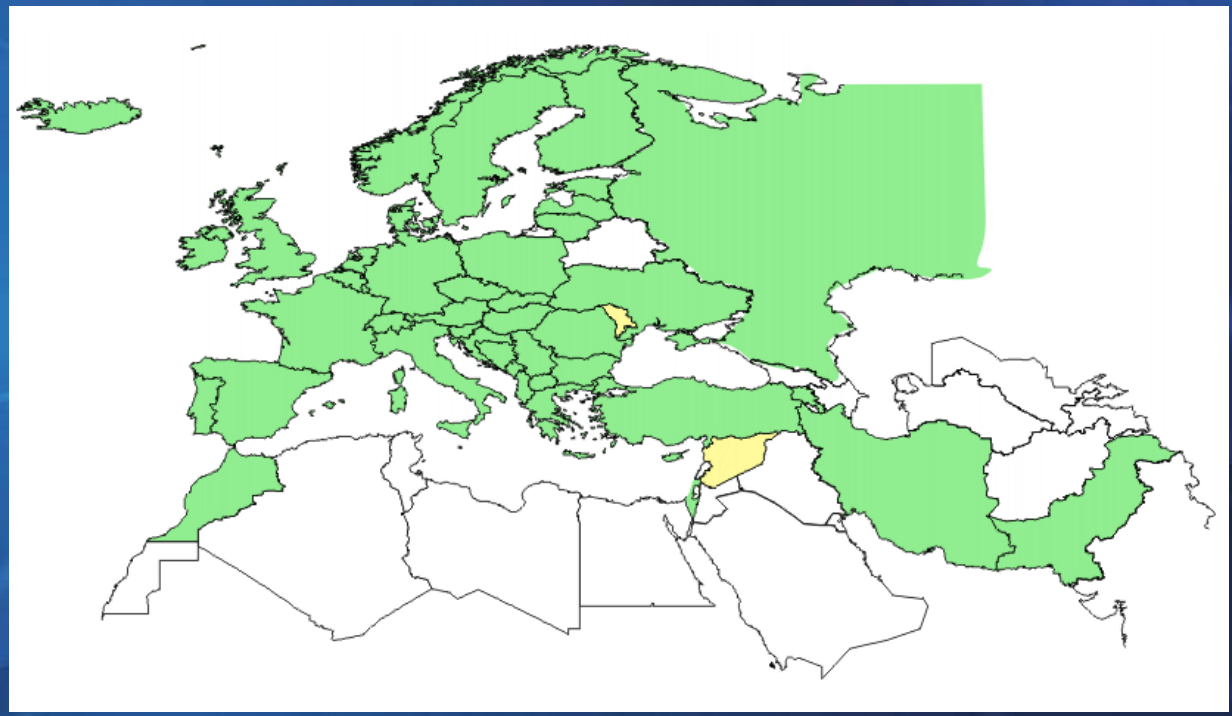
- اعضای هر منطقه جغرافیائی هر ۴ ماه یک نشست دارند و هر نشست اساسنامه خود را با توجه به آخرین تغیرات فناوری grid در جهان به روز می کنند.
- در این نشست ها تقاضای اعضای جدید بررسی می شود و بر اساس رای دیگر اعضا عضو جدید پذیرفته می شود.
- معمولا از هر کشور یک CA به عنوان نماینده در IGTF پذیرفته می شود.

IRAN-GRID Certification Authority

GRID COMPUTING GROUP

International Grid Trust Federation (IGTF)

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



IRAN-GRID Certification Authority

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

- IRAN-GRID CA عضوی 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 سینزدهم IPM با ارائه آخرین دفاعیه خود ، به عنوان نماینده رسمی ایران در EUgridPMA پذیرفته شد.

GRID COMPUTING GROUP

IRAN-GRID Certification Authority

http://cagrid.ipm.ac.ir

- صدور شناسنامه دیجیتالی برای افراد حقیقی ، کامپیوتر و سرویس
- متقاضایان شناسنامه دیجتالی باید عضو یک موسسه تائید 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

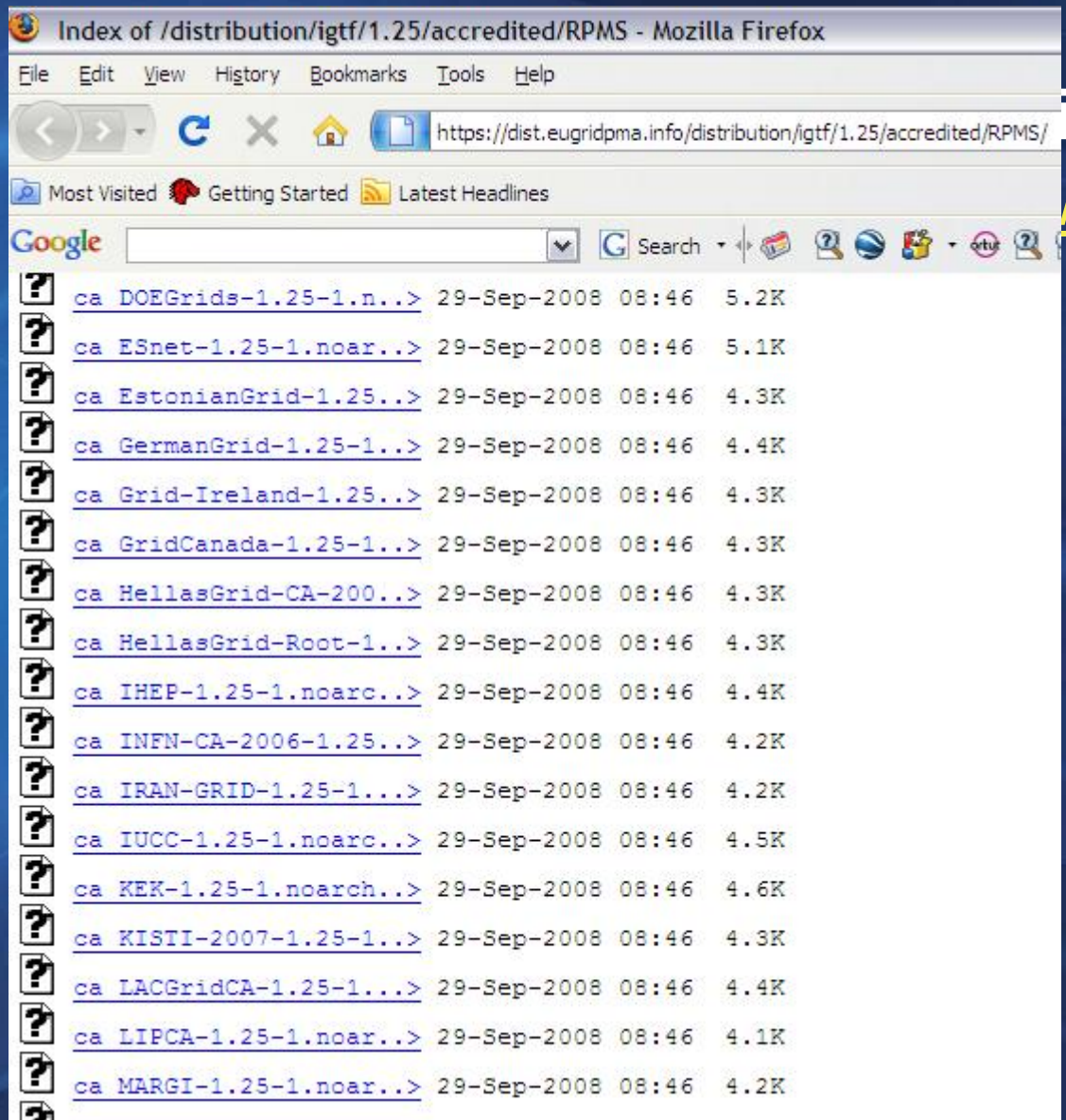
GRID COMPUTING GROUP

IRAN-GRID Certification Authority

http://cagrid.ipm.ac.ir

IRAN-GRID Certification Authority

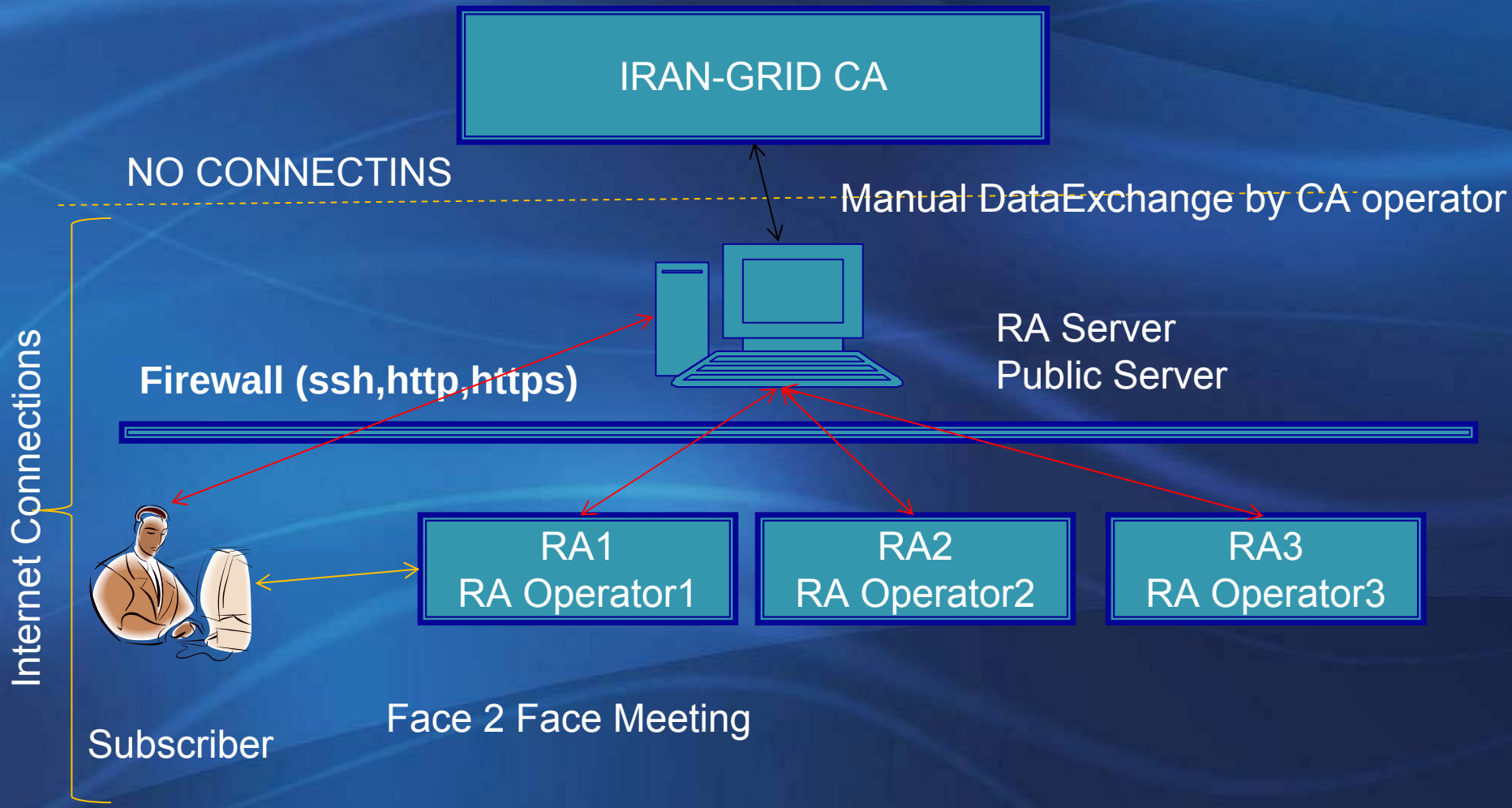
GRID COMPUTING GROUP



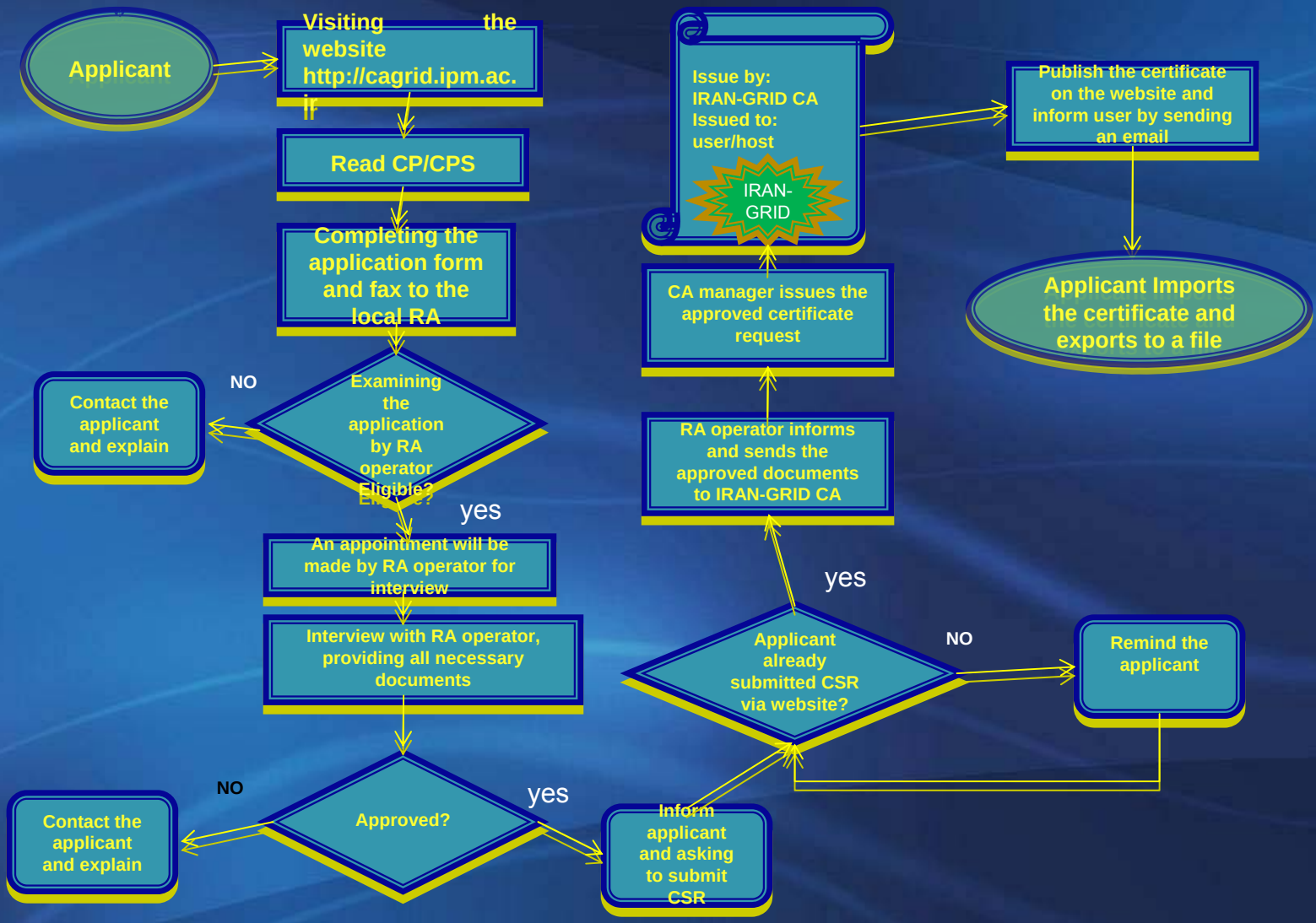
ication Authority

/cagrid.ipm.ac.ir

IRAN-GRID Certification Authority



IRAN-GRID Certification Authority



GRID COMPUTING GROUP

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,O=IRAN-GRID,O=IPM,C=IR
Valid…
…GMT
…MT
Subje… …O=IRAN-GRID,C=IR
Subj…
P… …
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:ec:07:5d:97:38:dc:e9:dd:0b:af:00:68:73:1a:

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

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 هرکشور 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؟