グリッドにおけるセキュリティの概要と動向

産業技術総合研究所　グリッド研究センター

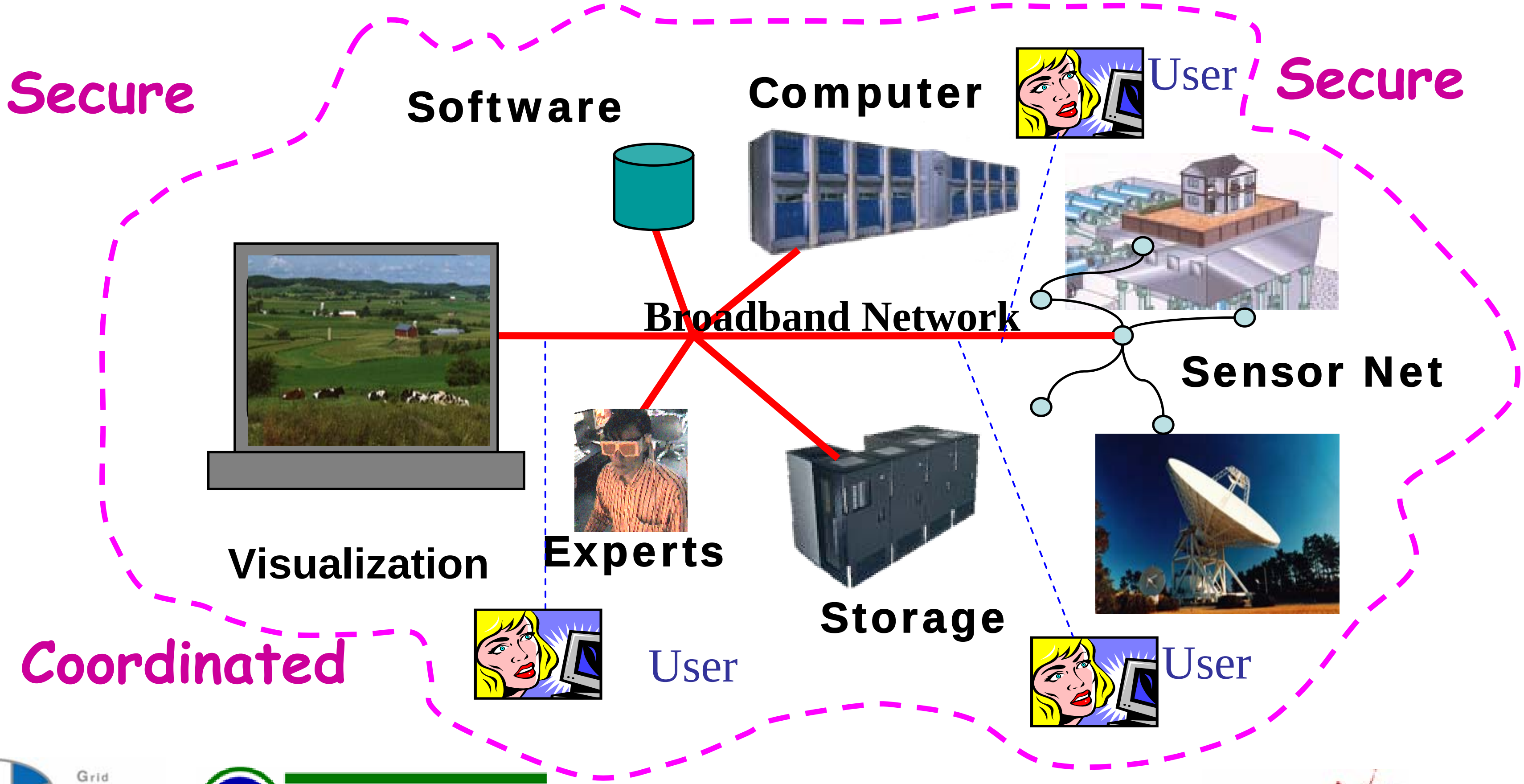
田中　良夫

話の内容

- **グリッドの紹介**
- **グリッドにおけるセキュリティの肝**
    - グリッド特有の要求事項
- **現状と動向**
    - 既存研究の成果
    - 現状および動向
- **全世界的な信頼関係の構築に向けて**
    - International Grid Trust Federationの紹介

グリッドとは？

- **Flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources**
  - resources include not only computers but various kinds of resources such as databases, networks, sensors, etc.

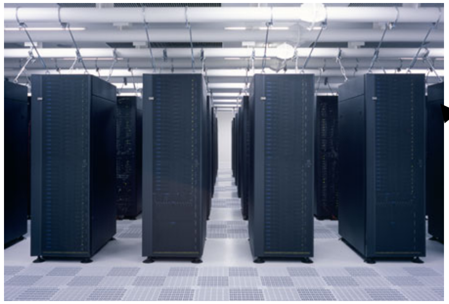

Secure
Software
Computer
User
Secure
Broadband Network
Sensor Net
Visualization
Experts
Storage
User
User
Coordinated

グリッドの歴史

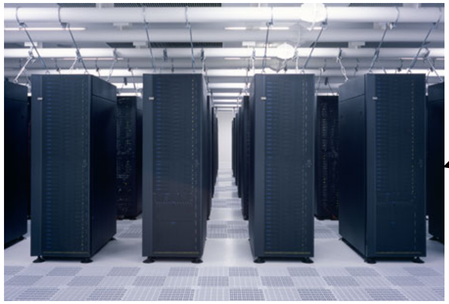
- **90年代はじめ**
  - 広域分散計算、グローバルコンピューティング、 メタコンピューティング
- **90年代中ごろ～終わり**
  - (アカデミック)ソフトウェアの開発、実証実験
  - “Grid”という用語が会議・論文等ではじめて使われたのは97年9月(たぶん)
- **現在**
  - 科学技術計算分野における多数のプロジェクト、コミュニティ
  - テストベッドの構築
    - NASA IPG, TeraGrid, UK-eScience, EUDG, EGEE, ApGrid, …
  - 大規模実証実験
  - 事実上の標準ソフトウェアの登場: Globus Toolkit™
  - 技術的にはかなりmatureになってきている。
  - 産業界からも注目
  - Global Grid Forum: ~1000 people, 30+ countries

Large-scale QM/MD simulation on AIST-TeraGrid @ SC2004

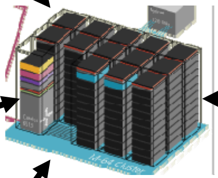
P32 (512 CPU)

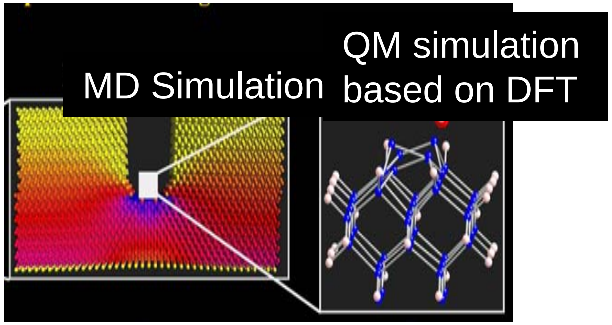


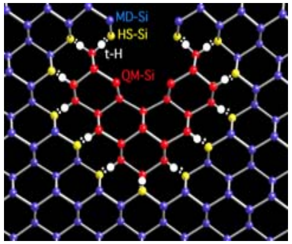
P32 (512 CPU)



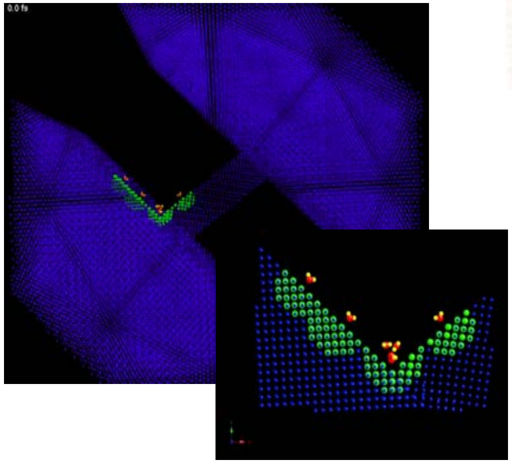
F32 (256 CPU)




MD Simulation
QM simulation based on DFT


MD-Si
HS-Si
t-H
QM-Si

TCS (512 CPU)
@ PSC



Run the simulation for more than 10 hours on 1793 cpus on AIST Super Cluster and TeraGrid

Grid World

グリッドの旬

Grid World 2006

IBM Grid and Grow Zone
Microsoft
Microsoft
Grid World 2006
Grid World 2006

3809 pre-registration

3163 show up

31 Exhibitors booth

グリッドにおけるセキュリティの肝

グリッド特有の要求事項

Three key functions in a Grid security model ※

- **Multiple security mechanisms**
  - VOに参加する各組織の（複数の）セキュリティ機構を利用
- **Dynamic creation of services**
  - 管理者の干渉なしに、ユーザが新しいサービスを動的に生成できる
- **Dynamic establishment of trust domains**
  - ユーザとリソースの間だけではなく、VOにおけるリソース間の信頼(trust domain)も確立する
  - それらのtrust domainは複数の組織にまたがり、動的に適応する

※ Von Welch, et.al., Security for Grid Services, HPDC-12, 2003

Security Challenges in a Grid Environment ※

- **The Integration Challenge**
  - 既存のセキュリティ技術を（相互）利用、統合
- **The Interoperability Challenge**
  - 複数のドメイン、Hosting Environment同士が協調するために、複数のレベルでのinteroperabilityが必要
    - Protocol level
      - メッセージ交換の機構が必要(SOAP/HTTPなど)
    - Policy level
      - 各サイト(party)が（相手方に望む）ポリシーを指定できる
      - 表現されたそれぞれのポリシーは互いに理解できる
    - Identity level
      - ドメインをまたいでのIdentityの確立
      - 物理的なIdentityの確立ではなく、（各ドメインにおける）IdentityとCredentialとのマッピング

※ Nataraj Nagaratnam, et.al., Security Architecture for Open Grid Services

Security Challenges in a Grid Environment ※ （続き）

- **The Trust Relationship Challenge**
  - 動的かつユーザによって制御（生成、管理）されるグリッドサービスにおける問題（挑戦）
    - Identity and authorization
      - サービスを実行する際のidentity, privilegeを制御する
    - Policy enforcement
      - サービスに対するポリシーの制定、制御
    - Assurance level discovery
      - セキュリティのレベルを知りたい
      - Privacy, virus protection, firewall usage, VPN, etc.
    - Policy composition
      - ポリシは（1つのリソースオーナではなく）複数のソースにより生成
    - Delegation

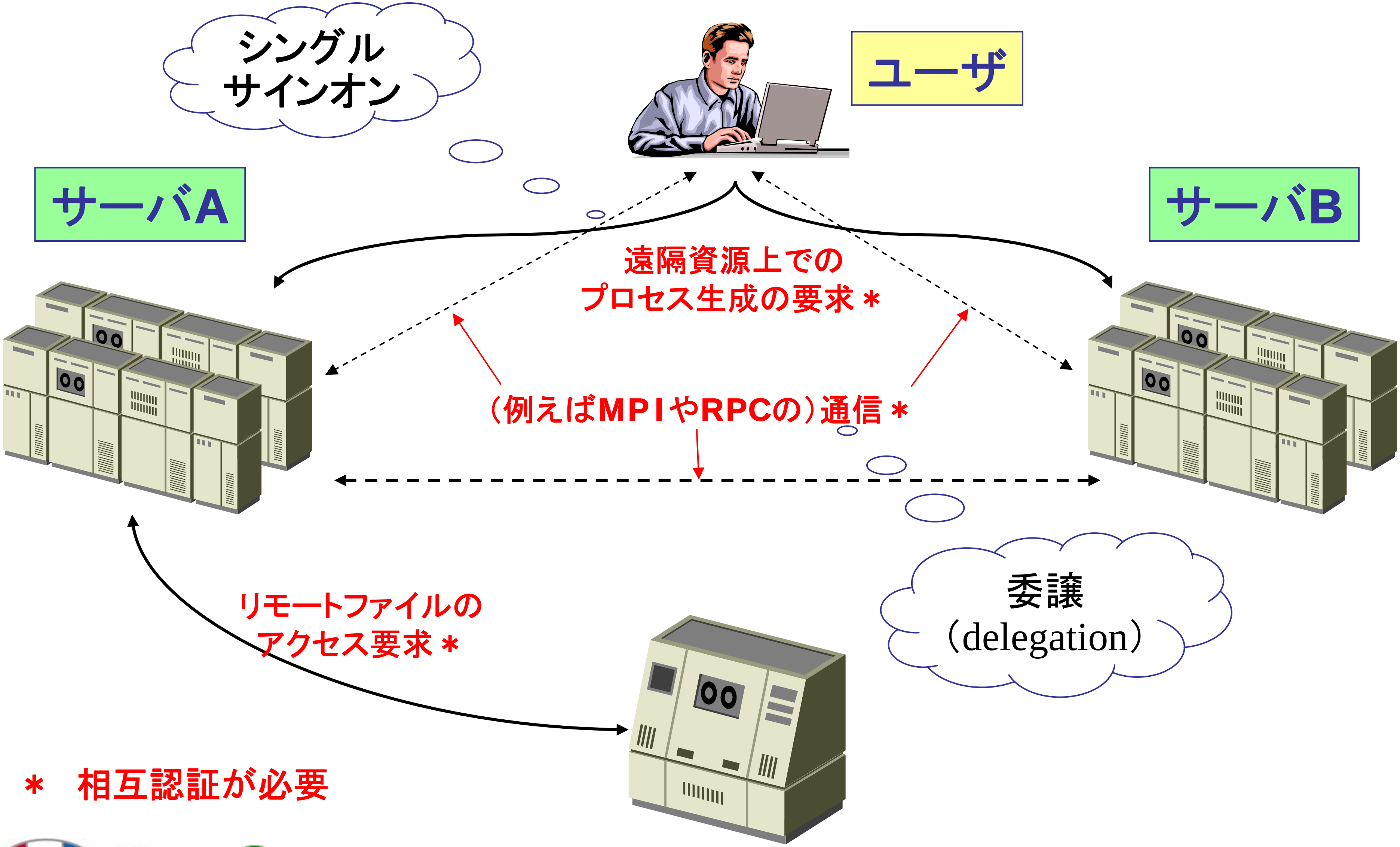
※ Nataraj Nagaratnam, et.al., Security Architecture for Open Grid Service

技術の紹介

Grid Security Infrastructure (GSI)
現状と動向

Grid Technology Research Center AIST

Single Sign On と delegation

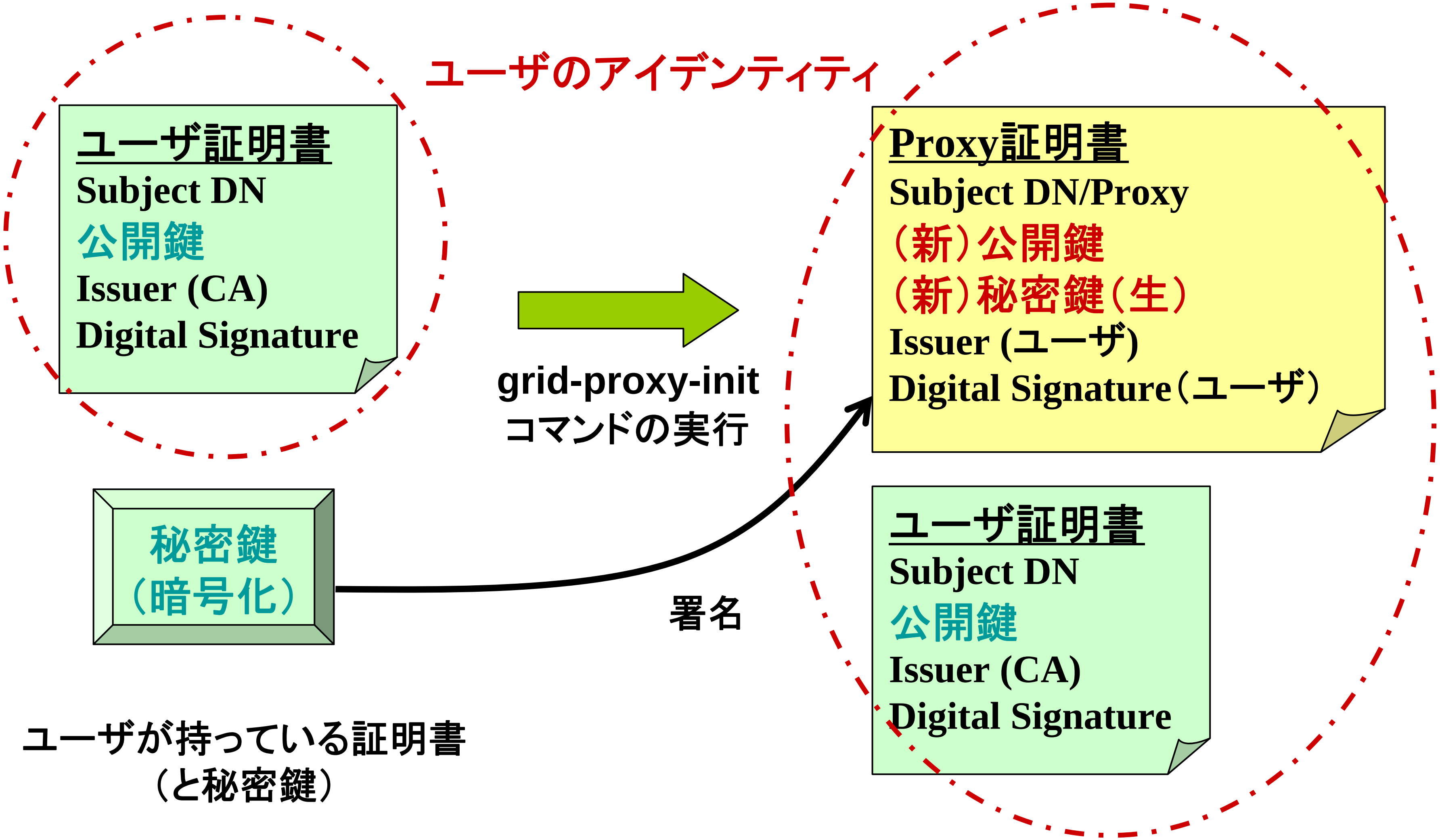

シングル
サインオン
ユーザ
サーバA
サーバB
遠隔資源上での
プロセス生成の要求＊
（例えばMPIやRPCの）通信＊
リモートファイルの
アクセス要求＊
委譲
（delegation）

＊　相互認証が必要

GSI: Grid Security Infrastructure

- **「グリッド」の名がつく技術の中で、もっとも偉大な成果(私見)**
- **PKIとX.509証明書を用いた認証および認可**
  - SSL protocol や WS-Security を利用
  - ユーザ、サービス、ホストはX.509証明書を保持する必要がある
- **Proxy証明書**
  - X.509証明書の拡張(RFC3820)
  - シングルサインオンと委譲を実現

Proxy証明書



ユーザのアイデンティティ

ユーザ証明書
Subject DN
公開鍵
Issuer (CA)
Digital Signature

grid-proxy-init
コマンドの実行

秘密鍵
（暗号化）

署名

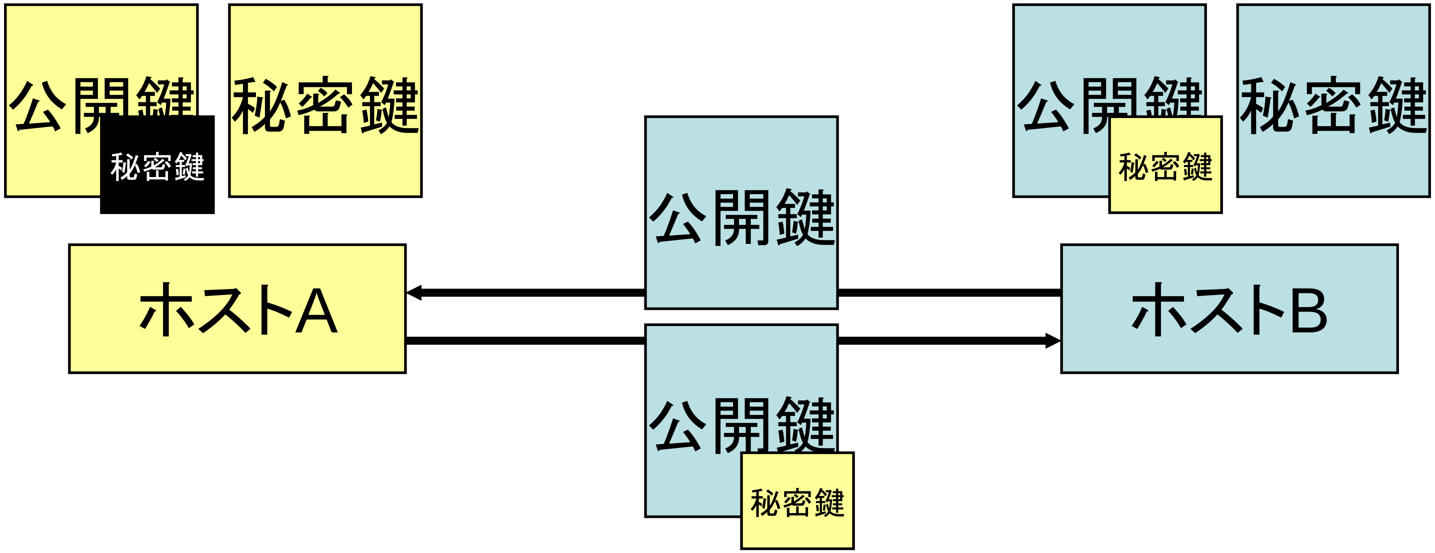
Proxy証明書
Subject DN/Proxy
（新）公開鍵
（新）秘密鍵（生）
Issuer (ユーザ)
Digital Signature（ユーザ）

ユーザ証明書
Subject DN
公開鍵
Issuer (CA)
Digital Signature

ユーザが持っている証明書
（と秘密鍵）

委譲の実装

- **プロキシ証明書の遠隔生成**
  - 証明書は、秘密鍵とサインされた公開鍵のペア


公開鍵
秘密鍵
秘密鍵
公開鍵
秘密鍵
秘密鍵
公開鍵
ホストA
ホストB
公開鍵
秘密鍵

技術のまとめ

- **Proxy証明書を使ったSingle Sign On + Delegationはグリッドの普及に大きく貢献した**
  - 既存技術プラスアルファ
  - Globus Toolkitによる参照実装とその普及
  - 実際、とても便利
- **関連技術の開発**
  - My Proxy
  - Grid Portal
- **今後もProxy証明書を使ったAuthentication & delegationが基本 (by Globus Alliance)**

技術的動向

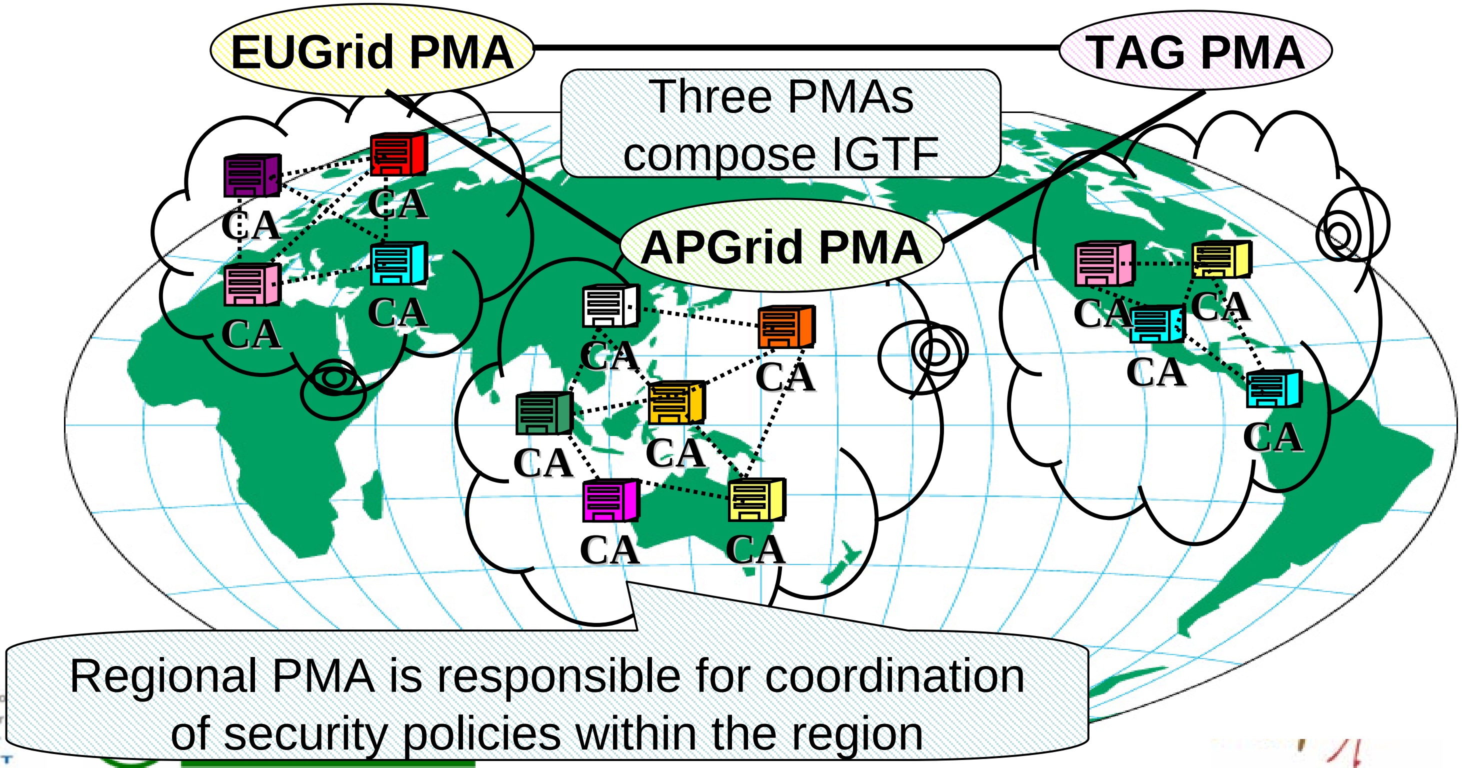
- **SAML, XACMLなどなどWebサービスの技術がどんどん取り入れられるようになってきている。**
- **Proxy証明書を使わないSingle Sign On, Delegationが実装されるだろう。**
- **Authorizationについてはまだまだ発展途上**
  - VOMS, CAS
- **ID managementを含めて今ホット**
  - GridShib, etc.
- **ポータルの標準的お作法が確立してきたようだ**
  - Long Lived証明書はユーザに管理させない・持たせず、データセンターで管理
  - 一極集中型の弱点は認識している。でもユーザに任せるよりは良いという判断
  - そうすると、いわゆるパスワード認証にもなるので、OTPの利用が進んでいる
- **VMも流行ってくると思う。**

全世界的な信頼関係の構築に向けて

APGrid PMA and
International Grid Trust Federation

Status and challenges

- **Need AuthN and AuthZ federation**
  - within a VO, and between VOs
- **AuthN federation**
  - foundation for building/experimenting with Grids
  - need to coordinate security (CA) policies
- **AuthZ federation**
  - still a grand challenge


EUGrid PMA
TAG PMA
APGrid PMA
CA
CA
CA
CA
CA
CA
CA
CA
CA
CA
CA
CA
CA
CA

Three PMAs compose IGTF

Regional PMA is responsible for coordination of security policies within the region

multi PKI domain の構築における問題点

- **アーキテクチャ**
  - Cross Certification, Cross Recognition, Bridged CA など、いくつか提案されている。それぞれPros/Consがある。
- **本質的な問題は技術面ではなくポリシーのすり合わせ**
  - すべての認証局は同じレベルで運営されるべき
    - 如何に認証局が安全に運営されているか？
      - HSMによる鍵管理、CAマシンの管理など
    - …
  - すべての認証局はポリシーの整合性を確保すべき
    - 如何に認証局はユーザを識別するか？
      - 面接？電話？….
    - …
- **Policy Management Authority (PMA) は認証局のポリシーおよび運用に関する整合性を取る調整機関**

APGrid PMA: Asia Pacific Grid PMA

- **アジア太平洋地域におけるPMA**
- **2004年6月1日設立**
- **議長は産総研田中**
- **Minimum CA requirementsを定義**
- **APGrid PMA は2つのレベルを規定**
  - Experimental-level CA
    - テスト用認証局であり、ルーズな運用が認められる
    - 地域内のみでのみ信頼可能
  - Production-level CA
    - 厳密な運用が求められる
    - 欧米のコミュニティにも信頼されるレベル

APGridPMA: Members

Affiliation	Name	Production CA	Experimental CA
AIST / Japan	Yoshio Tanaka	in operation	in operation (limited use)
ASCC / Taiwan	Eric Yen	in operation	none
KISTI / Korea	Sangwan Kim	in operation	in operation
CNIC/SDG / China	Kai Nan	accredited	in operation
IHEP / China	Gonxing Sun	in operation	none
APAC/Australia	David Bannon	in operation	will close
NAREGI/Japan	Shinji Shimojo	in operation	closed
NCHC / Taiwan	Tsung-Ying Wu	accredited	in operation (limited use)
SDSC(PRAGMA) / USA	Mason Katz	planning	planning
NECTEC / Thailand	Sornthep Vannarat	Planning	In operation
NGO / Singapore	Jon Lau	under review	none
KEK / Japan	Takashi Sasaki	in operation	will close
HKU / HongKong	Chen Lin, Elaine	no plan	in operation
U of Hyd / India	Arun Agarwal	no plan	in operation
USM / Malaysia	Boon Yaik	no plan	in operation
Osaka U / Japan	Susumu Date	no plan	in operation

APGridPMAの活動

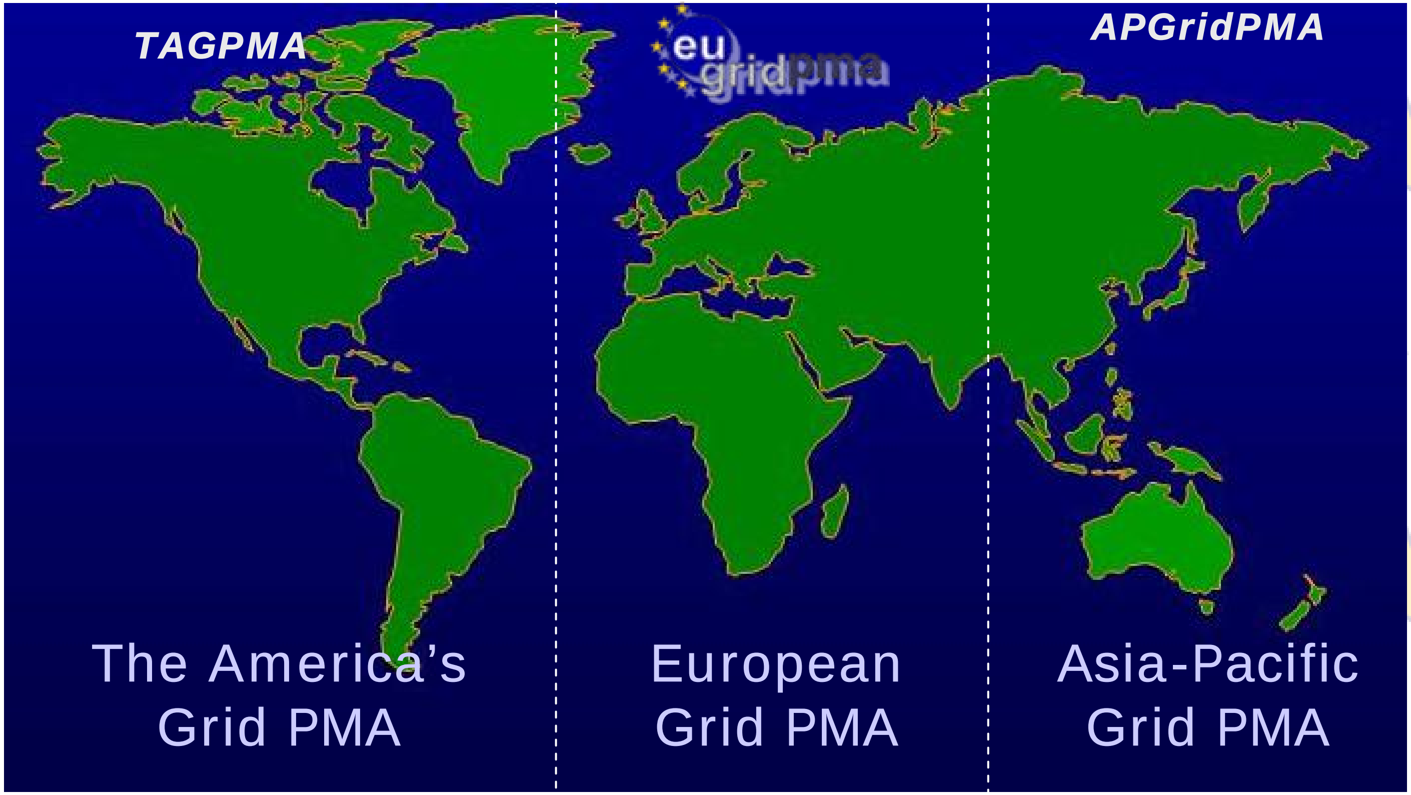
- **チャーター、minimum CA requirementsなどのドキュメントの作成、承認等**
- **認証局の承認**
  - 9つの認証局が「production CA」として承認されている
    - AIST, APAC, ASGCC, CNIC, IHEP, KEK, KISTI, NAREGI, NCHC
  - 7つの認証局が運用中
- **相互監査**
  - 監査のためのチェックリストがWebTrust™ と minimum CA requirementsをベースに作成
  - GGFにおいて "Guidelines for auditing Grid CAs"をInformational Documentとして作成中
  - AIST, ASGCC, IHEP, CNIC, APACが外部監査済み。

APGridPMAの活動（続き）

- **Regular (monthly) VTC.**
  - 各認証局の状況の簡単な報告
  - 特定の認証局に関する詳細な報告
  - 決定事項
    - 認証局の審査
    - ドキュメントの承認
  - 議論
- **（最低）年1度のF2F会議**
  - 第1回：2005年12月＠北京
  - 第2回：2006年10月＠大阪
- **電子メールを介した議論**
  - PMA内、PMA間

Solution to Extending Trust: IGTF – the International Grid Trust Federation

- common, global best practices for trust establishment
- better manageability and coordination of the PMAs


TAGPMA
eu gridpma
APGridPMA
The America's Grid PMA
European Grid PMA
Asia-Pacific Grid PMA

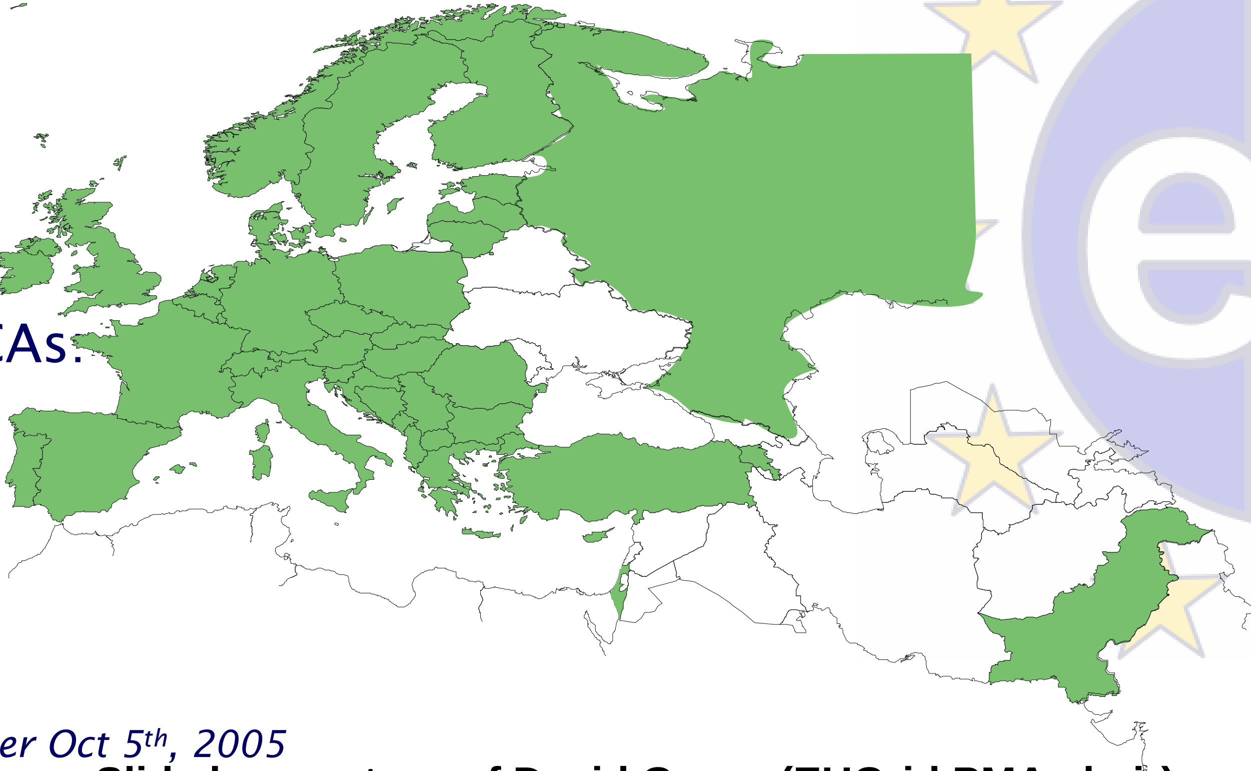
2005年9月 2004年5月 2004年6月

Slide by courtesy of David Groep (EUGrid PMA chair)

Coverage of the EUGridPMA

Green: Countries with an accredited CA

- 23 of 25 EU member states (all except LU, MT)
- + AM, CH, IL, IS, NO, PK, RU, TR, “SEE-catch-all”



Other Accredited CAs:

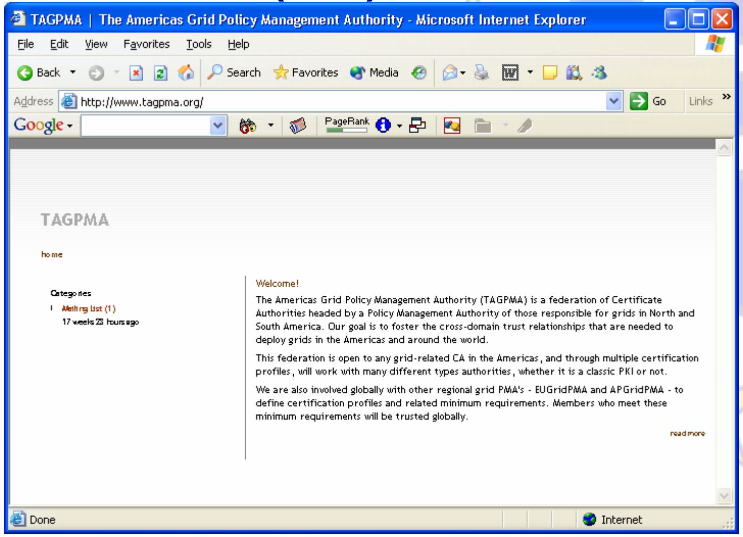
- DoEGrids (.us)
- GridCanada (.ca)
- CERN
- ASGCC (.tw)*
- IHEP (.cn)*

** Migrated to APGridPMA per Oct 5th, 2005*

Slide by courtesy of David Groep (EUGrid PMA chair)

TAGPMA

- 10 members to date,
  chaired by Darcy Quesnel (Canarie)
  - Canarie (.ca)
  - OSG (.us)
  - TERAGRID (.us)
  - Texas H.E. Grid (.us)
  - DOEGrids (.us)
  - SDSC (.us)
  - FNAL (.us)
  - Dartmouth (.us)
  - Umich (.us)
  - Brazil (.br)
- Launched June 28th, 2005
- Pioneered new “SLCGS” (Kerberos CA & al.)


TAGPMA | The Americas Grid Policy Management Authority - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.tagpma.org/
Go Links
Google
PageRank
Done
Internet

TAGPMA

home

Categories

- Mailing List (1)
  17 weeks 23 hours ago

Welcome!

The Americas Grid Policy Management Authority (TAGPMA) is a federation of Certificate Authorities headed by a Policy Management Authority of those responsible for grids in North and South America. Our goal is to foster the cross-domain trust relationships that are needed to deploy grids in the Americas and around the world.

This federation is open to any grid-related CA in the Americas, and through multiple certification profiles, will work with many different types authorities, whether it is a classic PKI or not.

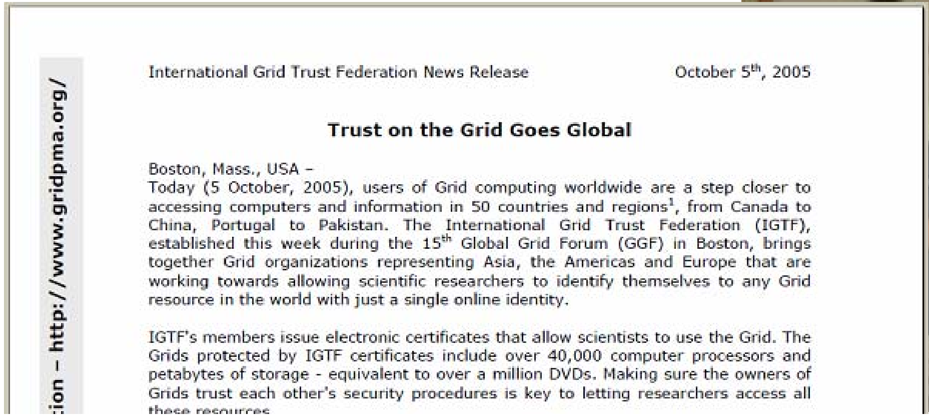
We are also involved globally with other regional grid PMA's - EUGridPMA and APGridPMA - to define certification profiles and related minimum requirements. Members who meet these minimum requirements will be trusted globally.

read more

Slide by courtesy of David Groep (EUGrid PMA chair)

Timeline

- March 2005: IGTF Draft Federation Document GGF13
- July 27th : APGridPMA approved version 0.7
- September 28th: EUGridPMA approval version 0.9
- October 5th: TAGPMA approved version 1.0
- October 5th: formal fou



ion – http://www.gridpma.org/

International Grid Trust Federation News Release October 5th, 2005

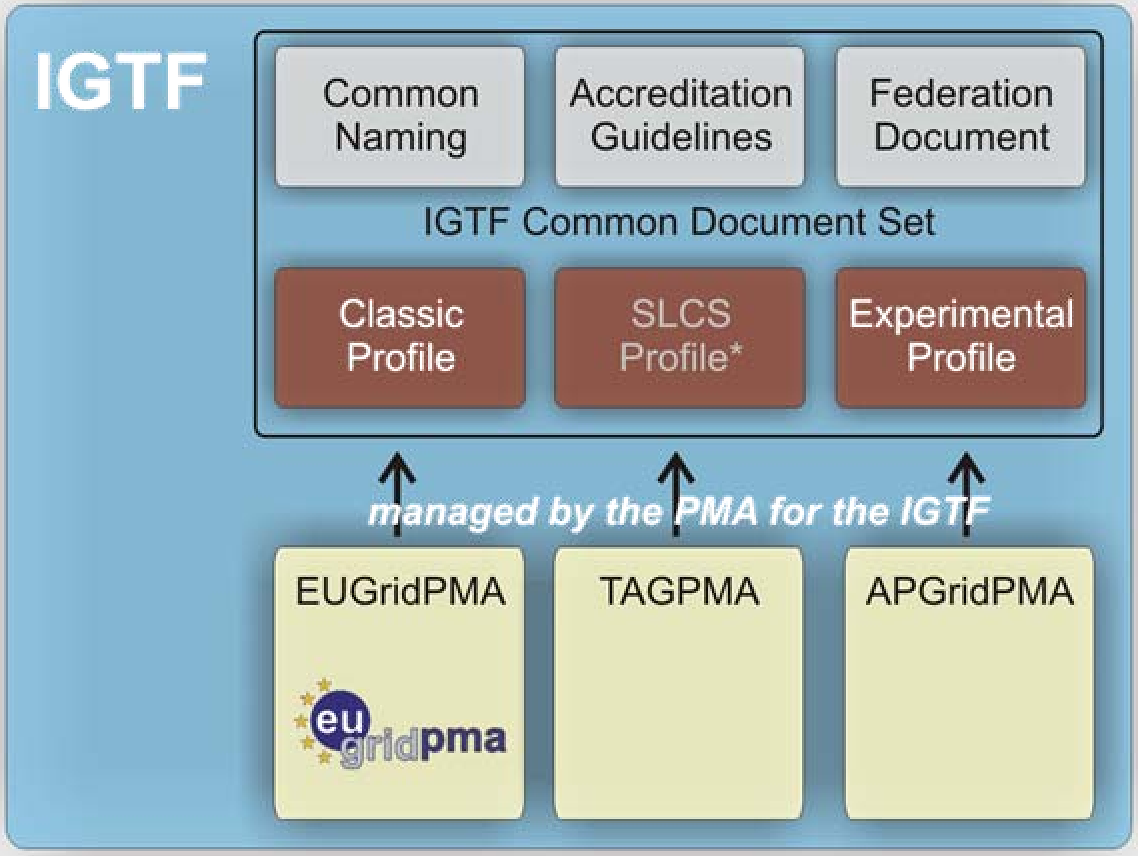
Trust on the Grid Goes Global

Boston, Mass., USA –
Today (5 October, 2005), users of Grid computing worldwide are a step closer to accessing computers and information in 50 countries and regions[1], from Canada to China, Portugal to Pakistan. The International Grid Trust Federation (IGTF), established this week during the 15th Global Grid Forum (GGF) in Boston, brings together Grid organizations representing Asia, the Americas and Europe that are working towards allowing scientific researchers to identify themselves to any Grid resource in the world with just a single online identity.

IGTF's members issue electronic certificates that allow scientists to use the Grid. The Grids protected by IGTF certificates include over 40,000 computer processors and petabytes of storage - equivalent to over a million DVDs. Making sure the owners of Grids trust each other's security procedures is key to letting researchers access all these resources

Slide by courtesy of David Groep (EUGrid PMA chair)

Common Guidelines across the IGTF



IGTF

Common Naming

Accreditation Guidelines

Federation Document

IGTF Common Document Set

Classic Profile

SLCS Profile*

Experimental Profile

managed by the PMA for the IGTF

EUGridPMA

TAGPMA

APGridPMA

Slide by courtesy of David Groep (EUGrid PMA chair)

Relying Party issues to be addressed

Characteristics Relying Party requests

1. standard accreditation profiles sufficient to assure approximate parity in CAs
2. monitor [] signing namespaces for name overlaps and issue unique names
3. a forum [to] participate and raise issues
4. [operation of] a secure collection point for information about CAs which you accredit
5. common practices where possible

(list courtesy of the Open Science Grid)

Slide by courtesy of David Groep (EUGrid PMA chair)

Guidelines: secured X.509 CAs

- Long-lived identity assertions
- Identity vetting procedures
  - Based on (national) photo ID's
  - Face-to-face verification of applicants via a network of Registration Authorities
  - Periodic renewal (once every year)
- Secure operation
  - off-line signing key or special (FIPS-140.3 or better) hardware
- Response to incidents
  - Timely revocation of compromised certificates

- Version 4.0 synchronised with Federation Document
- *The Annotated Minimum Requirements* on the Wiki

Slide by courtesy of David Groep (EUGrid PMA chair)

Guidelines: short-lived credential service

- Issue short-lived credentials (for grid: proxies) based on another site-local authentication system
  - e.g. Kerberos CA based on existing administration
- Same common guidelines apply
  - documented policies and processes
  - a reliable identity vetting mechanism
  - accreditation of the credential issuer with a PMA
- Same X.509 format, but no user-held secrets
- *New profile by TAGPMA in the Americas*

Slide by courtesy of David Groep (EUGrid PMA chair)

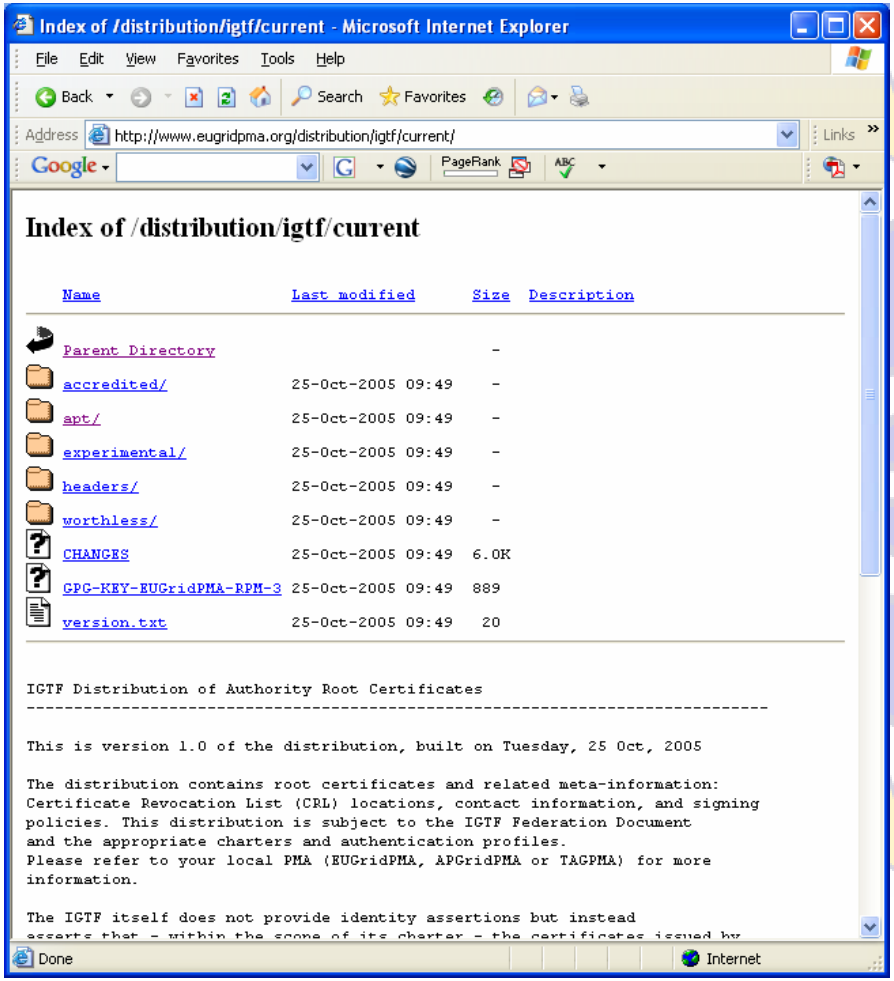
Common Naming: the Distribution

- Periodic, monthly, distribution of all trust anchors
  - Common for the entire IGTF
  - Includes all trust anchors for all profiles
    classic, SLCS, experimental*, …
  - Does not distinguished between accrediting PMAs
- Wide variety of formats
  - RedHat Package Management (RPM) system
    including a ‘meta’ package with dependencies per profile
  - ‘tar’ archives per CA, ordered per profile
  - Installation bundle suitable for ‘**`./configure && make install`**’
  - New formats (like JKS) on request
- Chairs can update the common back-end repository

Slide by courtesy of David Groep (EUGrid PMA chair)

Access to the Distribution Repository

- Web site
  http://www.eugridpma.org/distribution/igtf
- Should be mirrored by all PMAs
- Each PMA can/should sign the RPMs with their own PGP key
- Validation of content via TACAR (where possible)


Index of /distribution/igtf/current - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.eugridpma.org/distribution/igtf/current/
Links
Google
PageRank
Done
Internet

Index of /distribution/igtf/current

Name	Last modified	Size	Description
Parent Directory		-	
accredited/	25-Oct-2005 09:49	-	
apt/	25-Oct-2005 09:49	-	
experimental/	25-Oct-2005 09:49	-	
headers/	25-Oct-2005 09:49	-	
worthless/	25-Oct-2005 09:49	-	
CHANGES	25-Oct-2005 09:49	6.0K	
GPG-KEY-EUGridPMA-RPM-3	25-Oct-2005 09:49	889	
version.txt	25-Oct-2005 09:49	20	

```
IGTF Distribution of Authority Root Certificates
-------------------------------------------------------------------------------

This is version 1.0 of the distribution, built on Tuesday, 25 Oct, 2005

The distribution contains root certificates and related meta-information:
Certificate Revocation List (CRL) locations, contact information, and signing
policies. This distribution is subject to the IGTF Federation Document
and the appropriate charters and authentication profiles.
Please refer to your local PMA (EUGridPMA, APGridPMA or TAGPMA) for more
information.

The IGTF itself does not provide identity assertions but instead
asserts that - within the scope of its charter - the certificates issued by
```

Slide by courtesy of David Groep (EUGrid PMA chair)

IGTFの具体的成果と課題

- **成果**
  - 海外機関との共同プロジェクトにおいて、自前あるいは国内の認証局発行の証明書を利用できるようになった。
    - 高エネ研、東大 in LCG
    - 筑波大 in Lattice QC Grid
  - GGFにおけるGrid Interoperation Now (GIN)というプロジェクトにおいても、「認証局の相互信頼についてはIGTF-accredited CAでいきましょう…」というコンセンサスを簡単にとることができる。
  - （とりあえず）認証局の運用ポリシーのすり合わせについては、世界的な枠組みができあがった。
    - 参加するならこのポリシーに準拠すれば簡単
- **課題**
  - 商用認証局の利用
  - profile、minimum requirementsの精査
  - 相互監査
  - 規模拡大、コミュニティの運営
  - . . .

More Information

- **APGrid PMA**
  - http://www.apgridpma.org/
- **EUGrid PMA**
  - http://www.eugridpma.org/
- **TAGPMA**
  - http://www.tagpma.org/
- **GridPMA**
  - http://www.gridpma.org/
- **ApGrid**
  - http://www.apgrid.org/
- **PRAGMA**
  - http://www.pragma-grid.net/
- **GTRC/AIST**
  - http://www.gtrc.aist.go.jp