
グリッドにおけるセキュリティの動向

～ 認証から認可、ID連携へ～

産業技術総合研究所 グリッド研究センター
田中 良夫



OGFにおけるセキュリティ関連の活動

eScience Function

▶ Grid Operations

@ Certificate Authorities Operations WG (caops-wg)

Standards Function

▶ Security

@ Firewall Issues RG (fi-rg)

@ OGSA Authorization WG (ogsa-authz-wg)

@ Trusted Computing RG (tc-rg)

Others

▶ Shibboleth-Grid BOF

▶ OGSA Authentication WG (planned)

話の内容

- Gridセキュリティの現状と動向(概要)
- CAOPs WG、 PMA と IGTF
- Shibboleth + Grid AA
- OGSA AuthN WG (new)

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

グリッドセキュリティの肝

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

解決すべき課題

🌐 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

解決すべき課題 (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)

④ Identity and authorization

- ✦ サービスを実行する際のidentity, privilegeを制御する

④ Policy enforcement

- ✦ サービスに対するポリシーの制定、制御

④ 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.

④ Policy composition

- ✦ ポリシは (1つのリソースオーナーではなく) 複数のソースにより生成

④ Delegation

グリッドセキュリティの現状と動向(まとめ)

● 認証

- ▶ GSI (X.509証明書 + PKI)によるシングルサインオンと権限委譲

● 認可 & VO管理

- ▶ grid-mapfile を用いて UNIX アカウントに帰結
- ▶ VOMS (Virtual Organization Membership Service)
- ▶ PERMIS (PrivilEge and Role Management Infrastructure Standards Validation)

● 標準化

- ▶ IGTF (International Grid Trust Federation)
 - ◎ 認証局の承認(お墨付きをあたえる)
 - ◎ 認証プロファイルの策定
- ▶ GIN (Grid Interoperation Now) におけるVOMSを用いた相互接続実験

● 動向

- ▶ 技術開発としては、認証から認可へ
- ▶ Shibbolethを中心とするID管理システムの利用
- ▶ ポータル?

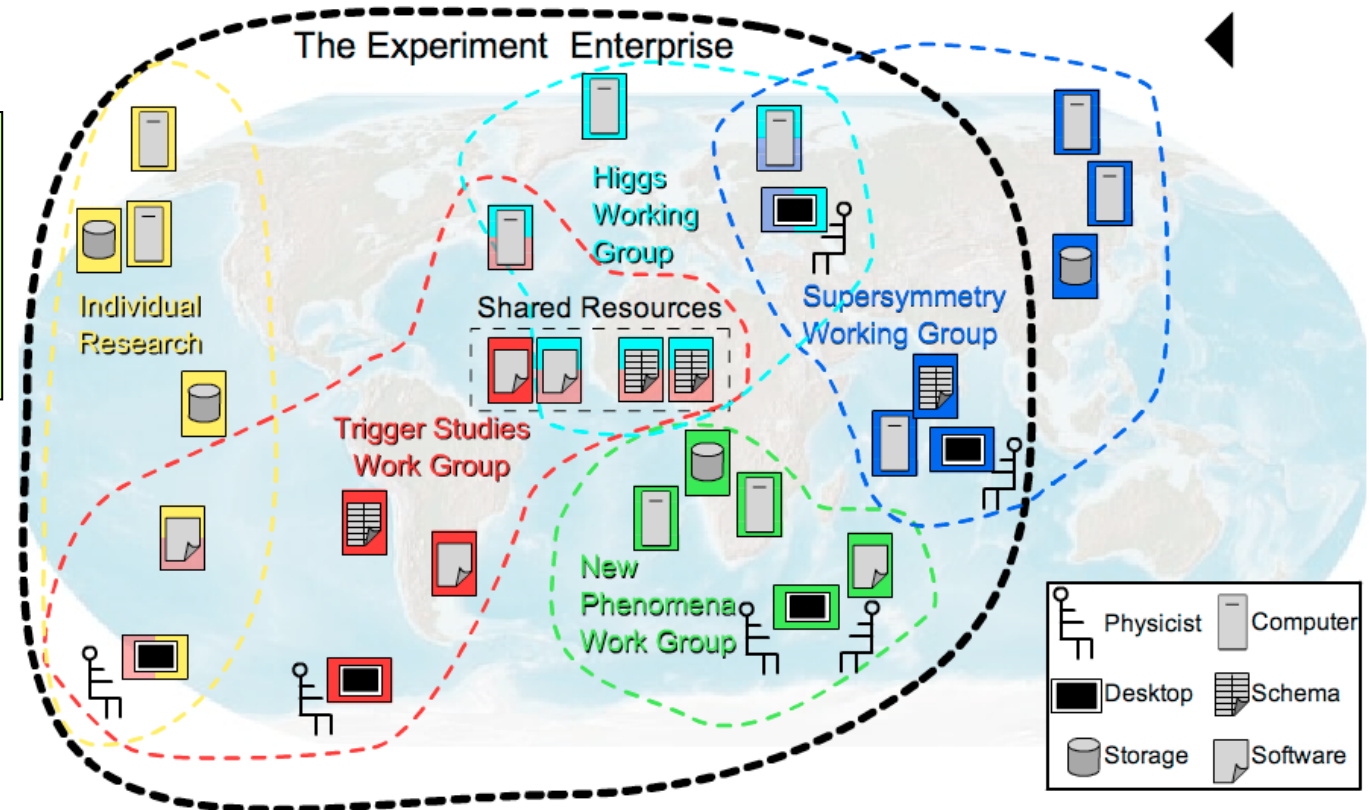
全世界的な信頼関係の構築に向けて

International Grid Trust Federationの紹介

グリッドにおけるセキュリティ基盤の構築

- 現状はX.509証明書とPKI (公開鍵暗号)を用いた認証が一般的
 - ▶ 各組織は認証局を運用し、ユーザや計算サーバ等に証明書を発行
 - ▶ 各組織は互いの認証局を信頼しあうことにより、他組織のユーザ・計算サーバ等を認証

実質的には「認証局を信頼しあう組織」が仮想的な組織を構成する



● 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

March 2003: The Tokyo Accord

- ... meet at GGF conferences. ...
- ... work on ... Grid Policy Management Authority:
GRI DPMA.org
- develop Minimum requirements – based on EDG work
- develop a Grid Policy Management Authority Charter
- [with] representatives from major Grid PMAs:
 - ▶ European Data Grid and Cross Grid PMA:
16 countries, 19 organizations
 - ▶ NCSA Alliance
 - ▶ Grid Canada
 - ▶ DOEGrids PMA
 - ▶ NASA Information Power Grid
 - ▶ TERENA
 - ▶ Asian Pacific PMA:
AI ST, Japan; ASCC, Taiwan

現在3つのPMAが存在する

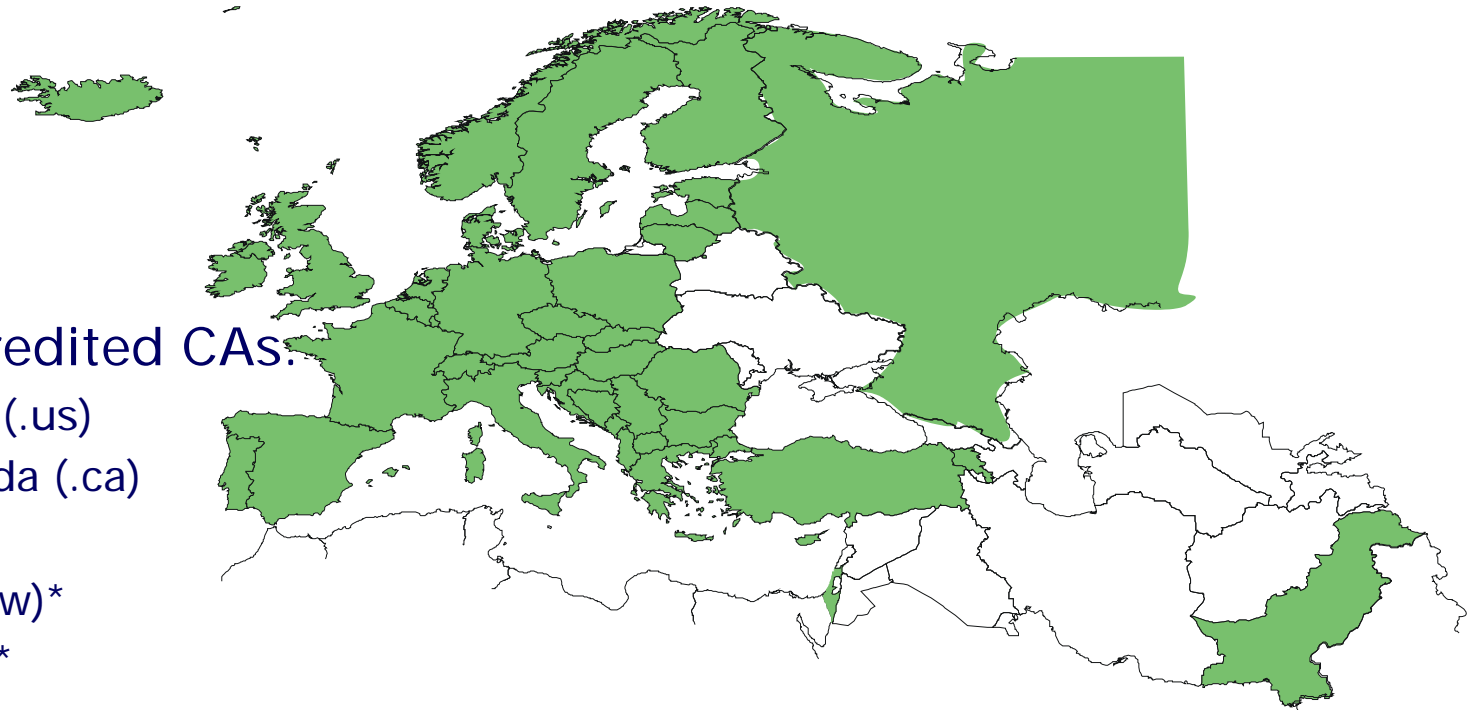
- ▶ EUGrid PMA (established May 2004)
 - @ Former: EUDG WP6 CA Coordination Group (started in 2002)
- ▶ TAG PMA (going to be established)
 - @ Former: DOEGrid PMA (started in 2002)
- ▶ APGrid PMA (established June 2004)
 - @ Unofficially started in 2003

各PMAの主たる役割

- ▶ 各地域内の認証局ポリシーの調整
- ▶ 他のPMAとの認証局ポリシーの調整

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)

14 CAs, 7 Relying Parties

CA

- Argentina UNLP
- Brazilian Grid CA
- CANARIE
- DOEGrids
- EELA LA Catch all
- ESnet/DOE Office Science
- FNAL
- Mexico UNAM
- NCSA
 - ▶ Classic
 - ▶ SLCS

CA

- Purdue Univ. TeraGrid
- REUNA Chilearn CA
- TACC
 - ▶ Root
 - ▶ Classic
 - ▶ SLCS
- Venezuela
- Univ. of Virginia USHER

RP

- Dartmouth HEBCA
- EELA
- OSG
- SDSC
- SLCS
- TeraGrid
- THEGrid

- 2004年6月1日に設立
- Minimum CA requirements を定義
- APGrid PMA は2つのレベルの認証局を認可
 - ▶ Experimental-level CA
 - ⊗ テストに利用
 - ▶ Production-level CA
 - ⊗ 欧米のコミュニティにも信頼される
- Two memberships
 - ▶ 13 Ex officio membership
 - ▶ 4 General membership
- Meetings
 - ▶ 月例ビデコン
 - ▶ 年1回のF2F会議

10 Accredited CAs

▶ In operation

- Ⓜ AI ST (Japan)
- Ⓜ APAC (Australia)
- Ⓜ ASGCC (Taiwan)
- Ⓜ CNI C (China)
- Ⓜ I HEP (China)
- Ⓜ KEK (Japan)
- Ⓜ NAREGI (Japan)

▶ Will be in operation

- Ⓜ NCHC (Taiwan)
- Ⓜ NECTEC (Thailand)

2 CA under review

- ▶ NGO (Singapore)

1 CA will be ready for review soon

- ▶ PRAGMA (USA)

Planning

- ▶ ThaiGrid (Thailand)
- ▶ KI STI (Korea)

General membership

- ▶ Osaka U. (Japan)
- ▶ U. Hong Kong (China)
- ▶ U. Hyderabad (India)
- ▶ USM (Malaysia)

- 参加メンバーの管理
- チャーターの策定、管理
- 認証プロファイルに基づいたminimum CA requirementsの策定、管理
 - ▶ 現状はClassic PKI Profileのみ
- Minimum CA requirementsに基づいた認証局の承認
- 認証局の監査
- メンバ認証局の名前空間の管理
- メンバ認証局のルート証明書配布
- 認証プロファイルの策定、提案

- **GGF CAOPs WGで始まった活動**
 - ▶ (文字通り)グリッドにおける信頼の連合(の構築)
- **GGF7@Tokyo, March 2003**
 - ▶ First meeting with EU, DOE, and AP members
 - ▶ Agreed with working on forming the Grid PMA.
 - ⊗ develop minimum requirements
 - ⊗ develop GridPMA charter
- **世界的な枠組みの構築に向けて議論を開始**
 - ▶ 2004年9月のブリュッセル会合
 - ⊗ DOEGrid PMA, EUGrid PMA, APGrid PMAが議論を開始
 - ⊗ 各PMAが地域を代表して世界的な枠組みを構築していくことで同意
 - ⊗ 互いの認証局運用要件を査読する事からはじめることで同意
 - ▶ 2005年3月のソウル会合
 - ⊗ PMA間で互いが認めた認証局同士を実験的に信頼しあうことに同意
 - ⊗ International Grid Trust Federationについて文書化を開始
 - ⊗ 監査方法についてAPGrid PMAが提案
 - ▶ 2005年5月のタリン会合
 - ⊗ 具体的な信頼の手順
 - ⊗ 認証局運用要件および監査手順の標準化など

- 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 foundation of the IGTF



Slide by courtesy of David Groep (EUGrid PMA chair)

- **メンバPMAは認証局の審査、承認を行う**
- **IGTFは認証プロフィール(Authentication Profile)を管理する。**
 - ▶ 証明書の用途、保証レベル、認証局の運用要件に応じた認証プロフィールを規定
- **現在の認証プロフィール**
 - ▶ Classic AP (EUGrid PMA)
 - ▶ Short Lived Credential Services (SLCS) AP (TAGPMA)
 - ▶ Member Integrated Credential Services (MICS) AP (TAGPMA)

- APへの変更が提案されると、すべてのPMAに議長を通して変更が伝えられる。
- 変更はすべてのPMAで承認される必要がある。
 - ▶ クレームがついた場合の手順など、まだ確立していない部分もある。
- 例
 - ▶ EUGrid PMAは10月初旬のF2F会議においてClassic APへの変更を承認した。
 - ▶ APGrid PMAは10月15日のF2F会議において、いくつか修正を要求することを決定し、PMA議長に通達。
 - ▶ EUGrid PMAで再度議論し、変更を受諾することが決まった。
 - ▶ 変更案は11月下旬のTAGPMA F2F会議で議論され、承認されれば変更案がIGTFの新しいプロファイルとして有効なものとなる。

- **各PMAはすべての認証局の情報を管理する**
 - ▶ Root certificate
 - ▶ CRL Distribution Point
 - ▶ Point of contact
 - ▶ Signing policy file
 - ▶ Point to the CP/CPS
- **すべてのPMAのすべての認証局の情報は1つのファイルに固められ、IGTF CA Distributionとして配布される。基本的に1ヶ月に1度程度の頻度。**
 - ▶ No hierarchies. All accredited CAs are included in a flat structure
 - ▶ Once you will be accredited by the APGrid PMA, you will be an IGTF-accredited CA
- **認証局の情報はEUGrid PMAが管理するCVSサーバに置かれている。**
 - ▶ APGridPMA, TAGPMAの議長はアカウントを持ち、適宜コミット。
- **IGTF CA Distribution は EUGrid PMAおよびAPGrid PMAのウェブサイトからダウンロード可能**

● IGTF、PMAの活動とCAOPs WGは密接に連携している。

▶ CAOPsでは

- ◎ PMAのモデル、チャーターテンプレートを策定
- ◎ CP/CPSのテンプレートを策定
- ◎ 証明書のプロファイルを策定

▶ IGTFでは認証プロファイルを策定

● PMAの会議

- ▶ EUGrid PMA: 年3回のF2F
- ▶ TAGPMA: 年3回のF2F
- ▶ APGrid PMA: 年1回のF2F+毎月のVTC

● EUGrid PMAとTAGPMAのF2Fでは、CAOPsセッションを設けている

● OGFにおいてはCAOPs WGは通常2セッション行い、そのうち1セッションはIGTFセッション

- IGTF Logo and style
 - Tony Genovese, LBNL/ESnet
- Updates from regional PMAs (5")
 - APGrid PMA (Yoshio)
 - EUGrid PMA (David)
 - TAGPMA (Darcy)
- Authentication Profiles
 - Member Integrated Credential Services AP (Tony) (10")
 - Classic AP Updates (David) (10")
 - Root Certificate AP (Yoshio) (5")
- Profile change process (Yoshio) (5")
- Business issues (Yoshio) (5")
 - Review of the mailing list
 - Distribution frequency
- AOB

- IGTFの活動により、認証局のレベルが客観的に判断できるようになった。
- Grid Interoperation Nowなどでも、「IGTF accredited CAでやりましょう」という感じで簡単に話がまとまる。
- まだ細かなところを詰めていかないといけない。
- 商用認証局の利用にいくつか問題が出ている。
 - ▶ CRLの有効期間、発行頻度
 - ▶ 監査、承認、情報開示
 - ▶ プロファイルが要件を満たさない

Grid-Shibboleth Integration

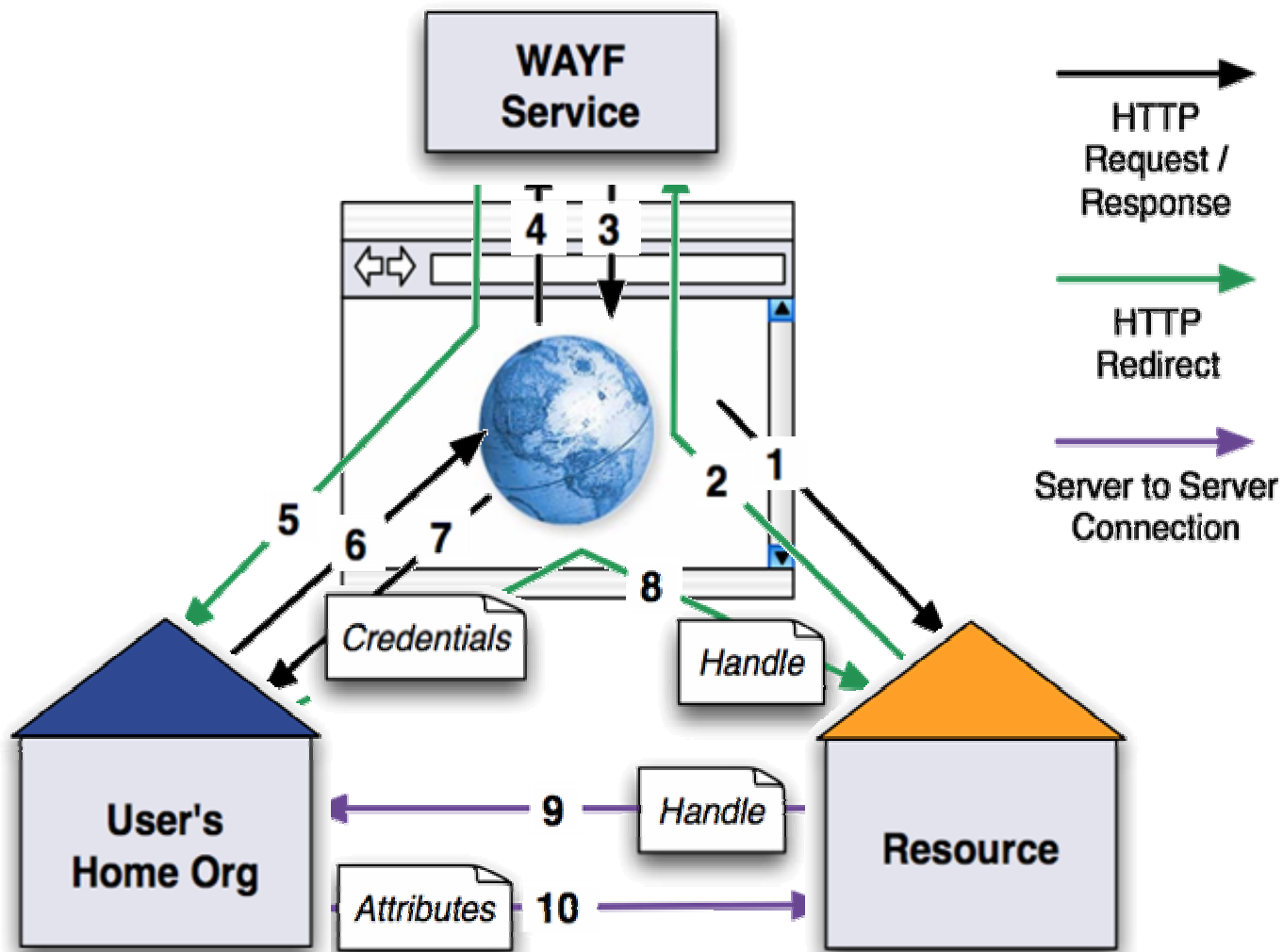


Shibbolethとは？



- Internet2のプロジェクト
- AAI = Authentication and Authorization Infrastructure
- Web-based single sign on (SSO)
 - ▶ ユーザがリソースにアクセスする際に
 - ◎ Identity Provide (IdP)によって認証が行われる。(リソースとは独立)
 - ◎ リソースはユーザの属性をIdPから受け取り、それに基づいてアクセス権限を決定する
- SAML: security assertion markup language を利用

動作の概要



Shibboleth-Grid integrationの動き

● GGF16にてBOFが開かれた(2セッション)

- ▶ 約50名の参加者
- ▶ 8つのプレゼンテーション
 - ◎ Oxford/CCLRC 'ShibGrid' project
 - ◎ Meta Access Management System (MAMS)
 - ◎ GridShib-Permis
 - ◎ SHEBANGS/Shib and GridSite
 - ◎ SWITCH
 - ◎ NeSC Glasgow activities
 - ◎ GridShib/MyProxy
 - ◎ Shibboleth 2.0 plans
- ▶ http://www.ggf.org/gf/event_schedule/index.php?id=213
http://www.ggf.org/gf/event_schedule/index.php?id=214

● GGF18にて2度目のBOF(4セッション！)

- ▶ 約50名の参加者
- ▶ BOF@GGF16のアップデート
- ▶ 今後の展開についての議論
- ▶ <http://grid.ncsa.uiuc.edu/events/ggf18-shib-bof/>

Common Areas

- **Short-lived X509 credentials from Shib authn**
 - ▶ ShibGrid, SWITCH, SHEBANGS, GridShib
- **Access to user DN via Shib AA**
 - ▶ ShibGrid, GridSite
 - ▶ GridShib has working on binder
- **Shibboleth authentication to MyProxy**
 - ▶ MAMS, SHEBANGS, GridShib
- **N-tier problem/ Shib-Portal-Grid**
 - ▶ MAMS
 - ▶ VOTES/GLASS, ShibGrid, MAMS, SHEBANGS
- **VO Services**
 - ▶ MAMS, SHEBANGS
- **VOMS Integration**
 - ▶ SHEBANGS, GridSite, SWITCH

Other activities

GridShibPermis

- ▶ PERMIS PDP for Shib, GridShib, Apache

Shib 2.0

- ▶ Authn request
- ▶ Single Logout
- ▶ Enhanced Client
- ▶ Improved Attribute Push

Shib 2.1

- ▶ Attribute Aggregation
- ▶ Account linking
- ▶ Delegated authentication
- ▶ Improved Targeted Id

Shib ??

- ▶ Passive authN

例: SWITCH SLCS

SLCS Profile

🌐 SLCS = short lived credential service

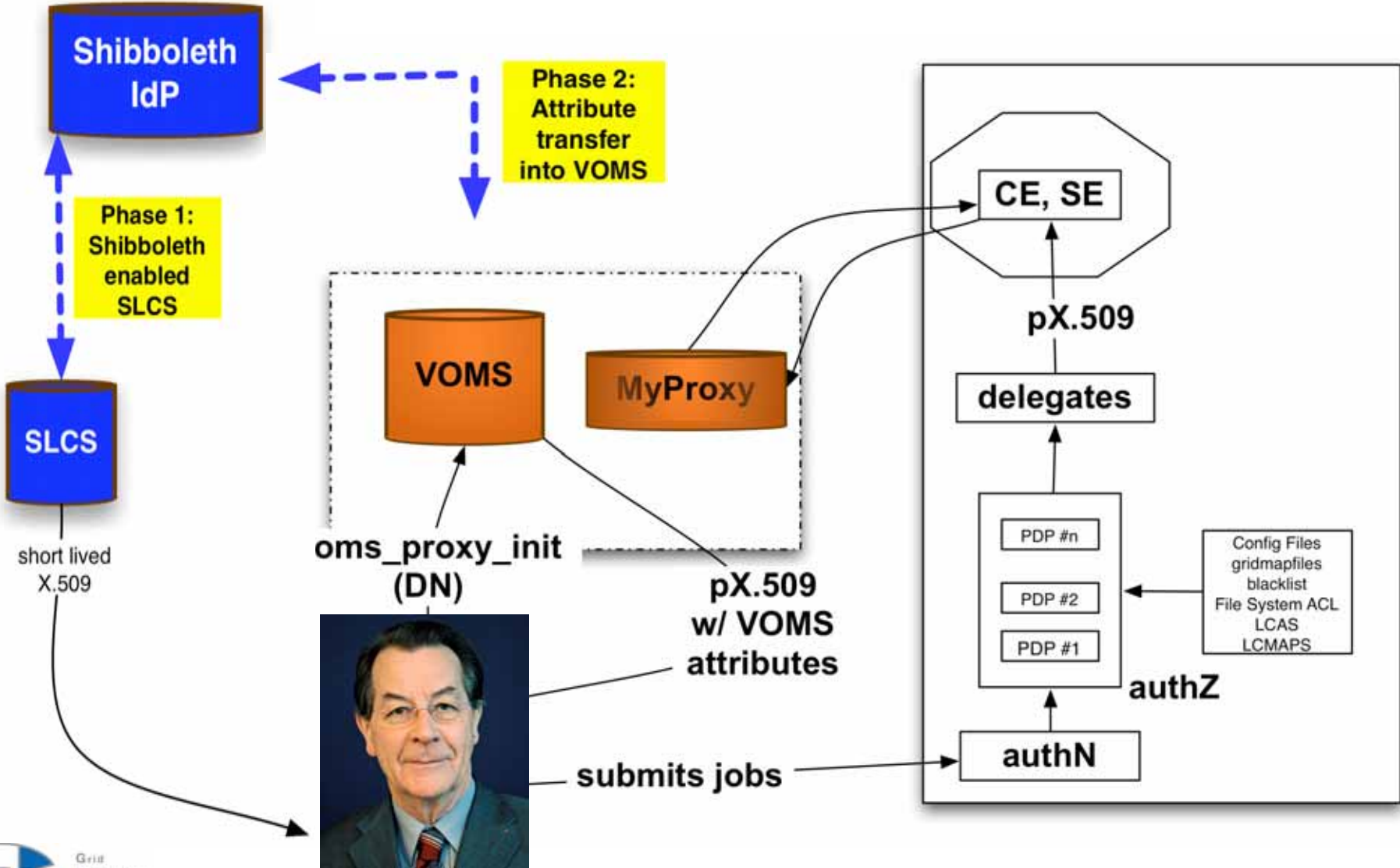
🌐 Minimum requirements:

SLCS	X.509 Certificate
Certificate is generated based on Identity Management system	“traditional” Registration Authority (e.g. passport)
Lifetime < 1mio sec	Lifetime < 1 year + 1 month
Revocation handling optional	Revocation handling

SWITCHaai

- スイスにはナショナルShibboleth-based AAIが構築されている。
- 2002年に開始し、今年の夏にプロダクションモードに入った。
- 現状
 - ▶ 約160'000 (75%) の高等教育機関がAAI-enabledアカウントを持っている。
 - ▶ 約10%が焼く100のリソースにアクセスするためにSWITCHaaiを日常的に利用している。

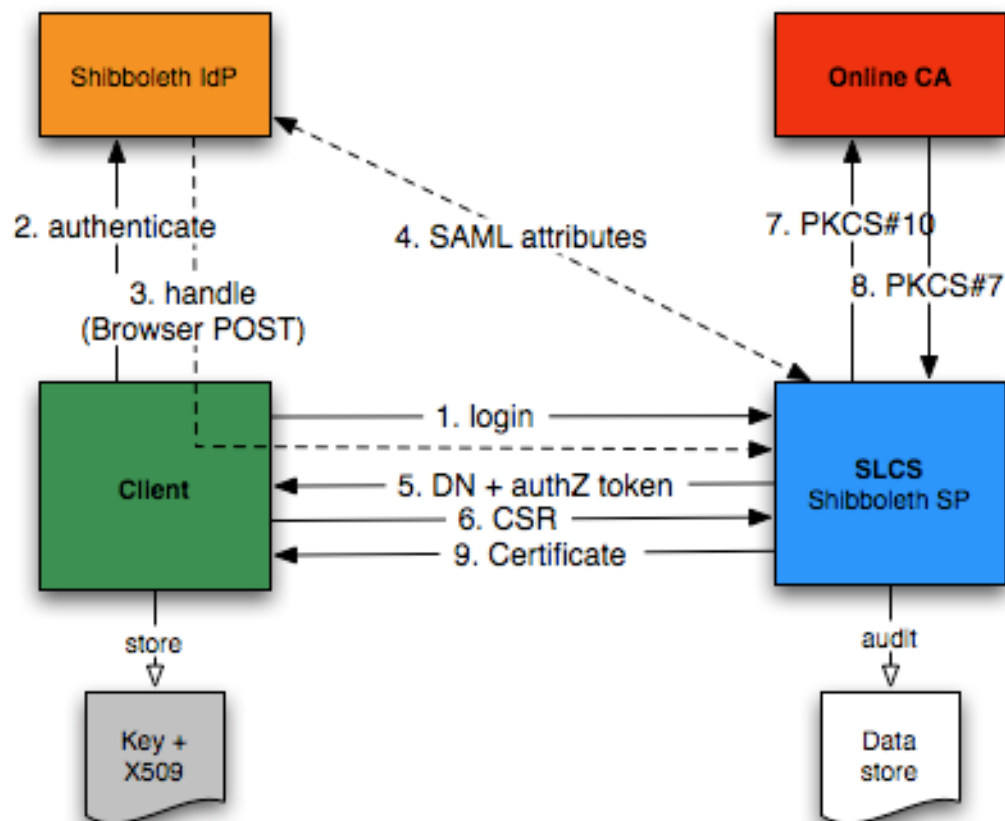
Overview Phase 1 and 2



SWITCHslcs

● デザインゴール

- ▶ 秘密鍵は送信しない
- ▶ 商用認証局の利用、標準プロトコルのみ利用
- ▶ モジュール化されたデザイン



例2: GridShib: Grid/Shibboleth Integration



Grid-Shibboleth Integration: A Policy Controlled Attribute Framework (Von Welch, Globus Alliance)

- NMIの2年プロジェクト(2004年12月に開始)
- Shibbolethが発行した属性証明をGrid(GT4)で利用
- Internet2のプロジェクトとして色々と標準技術を使っている
Shibbolethを認可に利用したい
- 技術的には
 - ▶ SAMLとX.509 Identity証明書の相補的な利用
 - ▶ SAMLとX.509属性証明書の相補的な利用
 - ▶ 属性管理を誰がどうやるか? などなど
- Pull Model
 - ▶ Globus ServicesがShibbolethに属性を取りに行く
 - ▶ GT4.xのWSおよびPre-WSコードに組みこまれる
 - ▶ クライアント側の修正は必要なし
- Push Model
 - ▶ ユーザがShibboleth属性を取得し、サービスに提示する。
 - ▶ VOMSやCASと同じ

目的

- ユーザがCamus ID Management システムを介してグリッドの認証を受ける。
 - ▶ Shibbolethが利用されていることを前提とする
- グリッドがCampusの属性を参照できるようにする。
- ユーザからX.509証明書の取り扱いをできるだけ見えなくする。

最近のR&D

- Shibboleth AAのGTへの組み込み
 - ▶ GTの認可においてユーザの属性をShib AAに問い合わせ、取得する。
 - ▶ GT 4.0 と Shibboleth 1.3 でテスト実装
- X.509 DN から Shibboleth の名前へのマッピングを行う。
- GridShib-CA
- ベータリリースが公開中
 - ▶ 正式版は GT 4.1/4.2

現状と今後

- 現在は単純な認可機構を実現
- サービスやコンテナを利用するための属性を取得
- 属性をGRAM経由のジョブ実行のためにローカルIDにマップする。
- 今後はPush Modelの実装
 - ▶ ポータルを介して認証を受ける
 - ◎ GridShib-CAが利用可能
 - ▶ ポータルはShibbolethを介して属性を集める
 - ▶ VOが発行する属性を相補的に利用
 - ▶ X.509証明書に属性を書き込む(push)
 - ◎ もともとのShibboleth Assertionもあわせて
 - ▶ AuthN Assertionもあわせて埋め込むことは可能

Shibboleth-Gridのまとめ

- **すでにいくつものプロジェクトが走っている**
 - ▶ **いくつかはプロダクション**
- **組み合わせには色々なアプローチがある。**
- **SLCS/MICS など、Shibbolethの扱いを念頭に置いたプロファイルもIGTFで承認・議論されている。**
- **Shibbolethがすでに利用されているのであればかなり魅力的。**
- **「これから導入」の場合、そのコストを考える必要はある。**
- **まだ色々と研究ネタ、開発が必要な項目はありそう。**

その他

OGSA AuthN WGの提案

- OGSA AuthN WGを立ち上げようという提案がなされた(議論中)。
 - ▶ OGSA AuthZ WGとの住み分けを明確に。歩調を合わせる。
 - ▶ IDを供給する側と連携する。
 - ▶ OGSAのroadmapとCAOPsの活動をうまくすりあわせる。
 - ▶ Bridge CAやShibboleth-Grid Integrationなどの新たな活動にきっかけを与える。
 - ▶ BOF or 1st WG @ GGF19

徒然なるままに

● ポータルにおけるセキュリティアーキテクチャ

- ▶ 秘密鍵の管理は誰がやる？
- ▶ 認証方式は？
- ▶ ポータル向けAPを提案予定

● PKI のフェデレーションはグリッドだけではない

- ▶ HEBCA (US, AP, etc)
- ▶ EDUROM

● 仮想マシン

- ▶ VM, VLAN, VPNでクリーンな環境を動的に構築
- ▶ グリッドセキュリティの出番は？

まとめ

- **認証はプロダクションに**
 - ▶ GSI が枯れてきた
 - ▶ I GTF の役割
- **認可 & Id 管理はホット**
 - ▶ VOMS, PERMIS による実証実験
 - ▶ Shibboleth
- **今後**
 - ▶ 引き続き認可 & Id 管理
 - ▶ ポータルセキュリティの確立
 - ▶ 仮想マシン
- **永遠の課題**
 - ▶ 利便性とセキュリティの確保