

グリッド協議会 第2回Grid Hotline
【技術動向】セキュリティに関する動向
Federated Identity Workshop, OGSA - Authz, OGSA - AuthN, ...

2007/03/23

日本電気株式会社
森 拓也

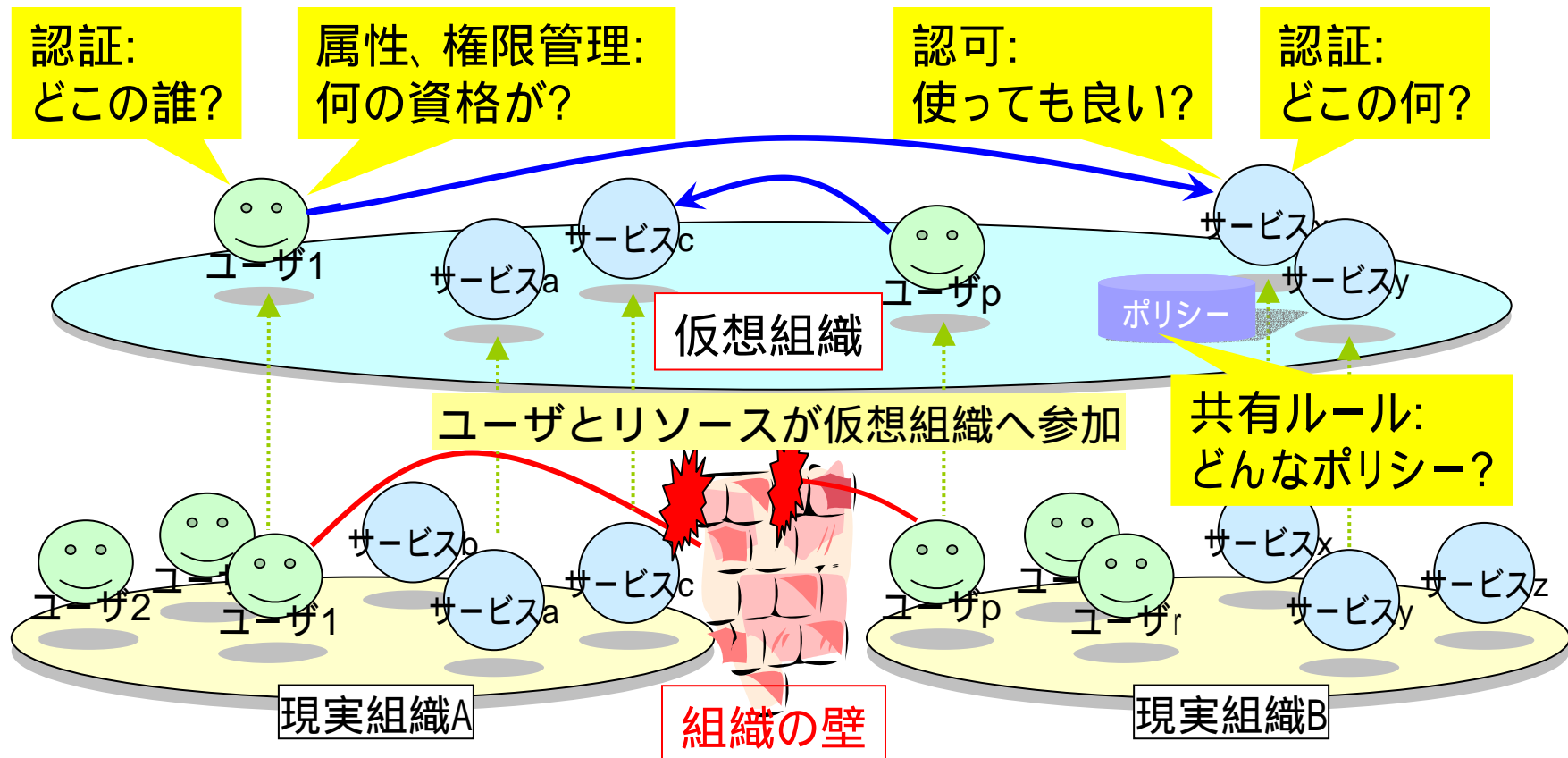
目次

- グリッドセキュリティ、おさらい
- OGF19でのセッションの様子
 - OGSA - AuthZ - WG
 - OGSA - AuthN - BoF
 - Security Area Meeting
- Federated Identity Workshop
 - ID連携、Shibbolethについて
 - グリッドでのShibbolethの利用
 - 権限管理、etc...
- まとめ

1. グリッドセキュリティ、おさらい

Grid 仮想組織...

- 簡単に言えば、組織の境界を越えたリソース利用に関する認証と認可の問題...
- だけど、簡単ではない...

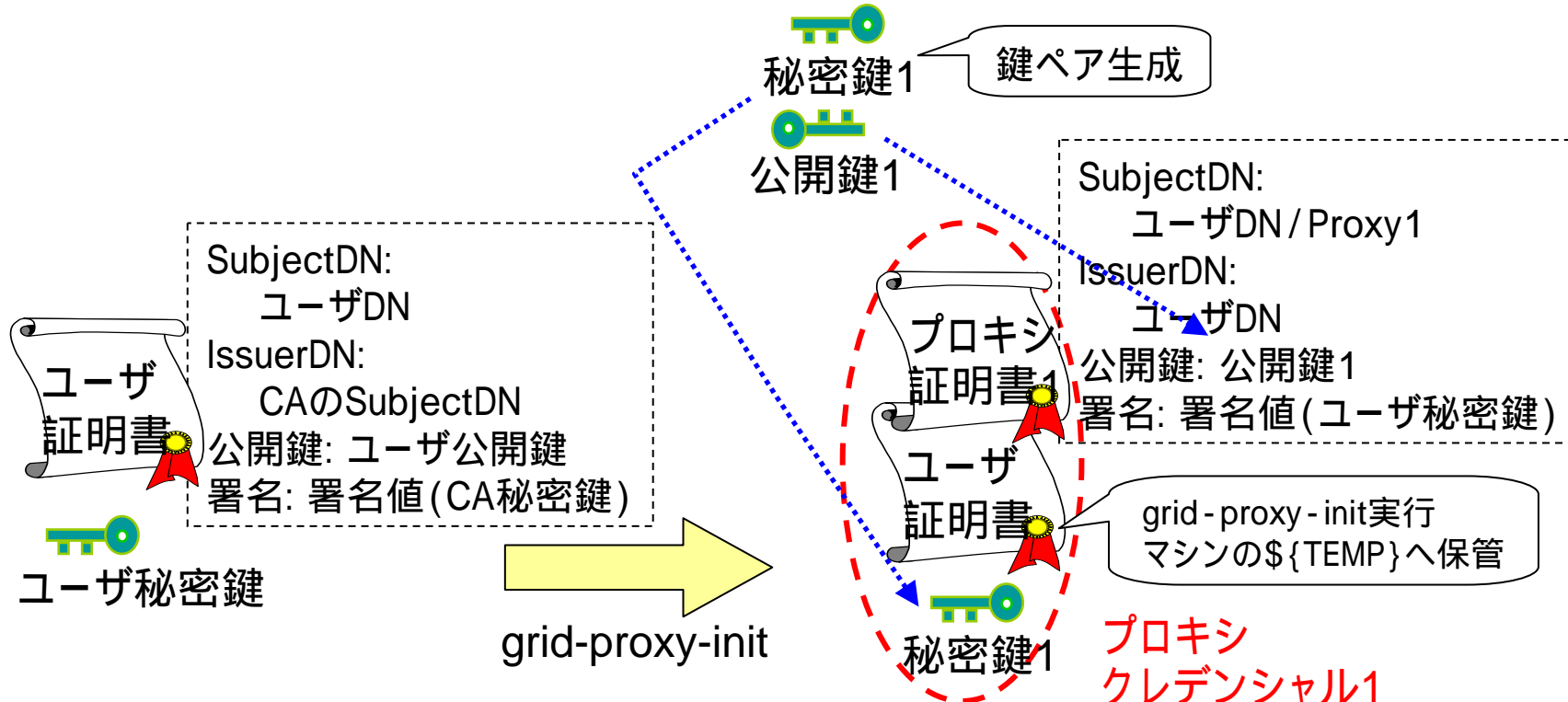


グリッド特有の要求

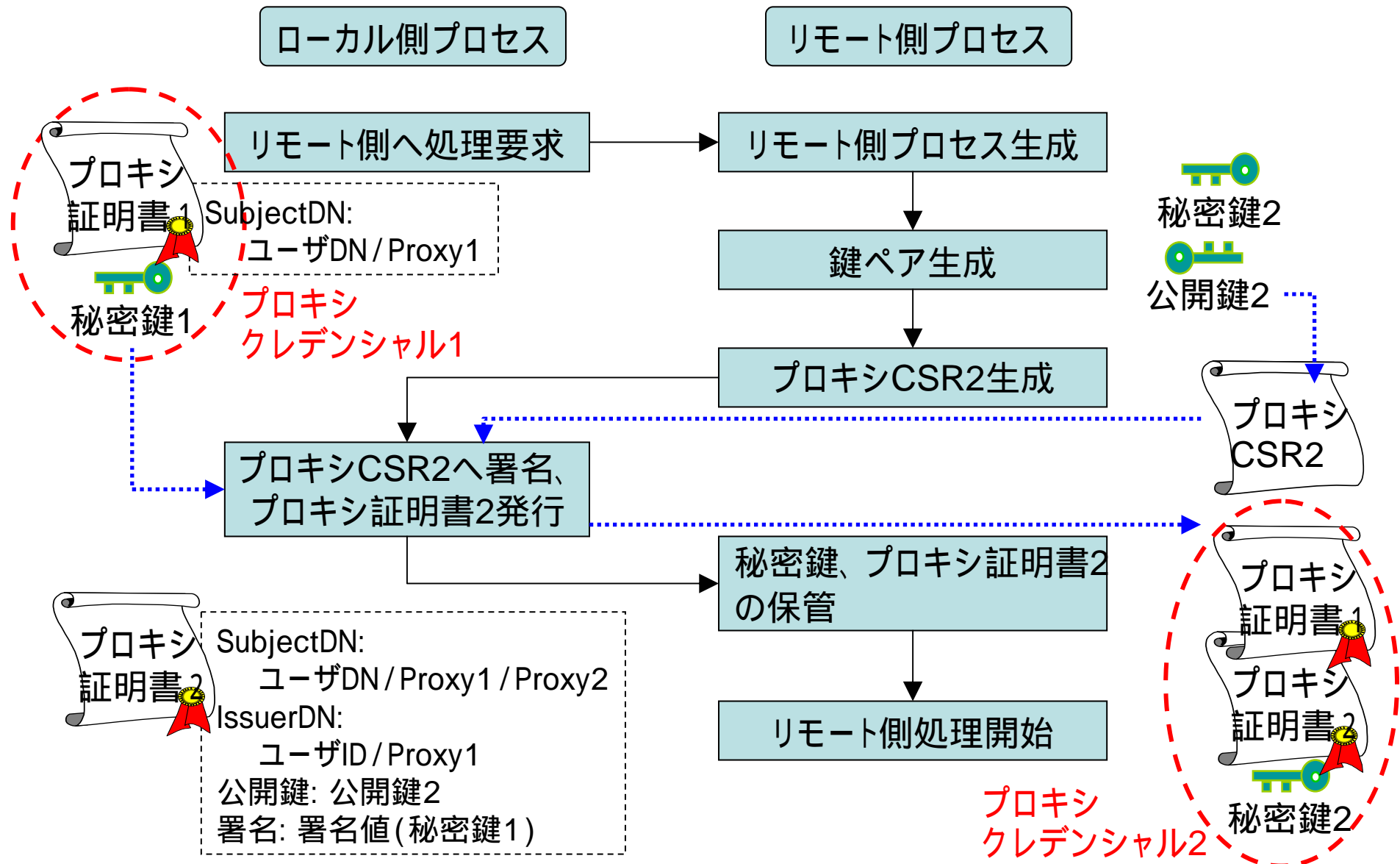
- サイトをまたがる認証と認可の実現
 - ユーザがサイトをまたがりサービスを生成
 - ユーザがサイトをまたがりサービスをアクセス
- シングルサインオンの実現
 - ユーザが複数のサービスを別々の場所に生成
 - ユーザが生成したサービスがさらに別のサービスを生成
 - ユーザが生成したサービスが別のサービスをアクセス
- 権限委譲 (デレゲーション)
 - サービスはユーザに成り代わって動作
 - ユーザが生成したサービスがさらに別のサービスを生成
 - サービスにユーザの権限を委譲することが必要

グリッドの現状 GSI

- GSI(Grid Security Infrastructure)
 - PKI、X.509証明書ベースの認証方式
 - プロキシ証明書(IETF RFC 3820)を用いてサブジェクトを認証
 - 認証・認可が必要なリソースの利用時にプロキシ証明書を生成 (grid-proxy-initコマンドを実行)
 - サブジェクトのIDはエンド・エンティティの公開鍵証明書のサブジェクト名から取得

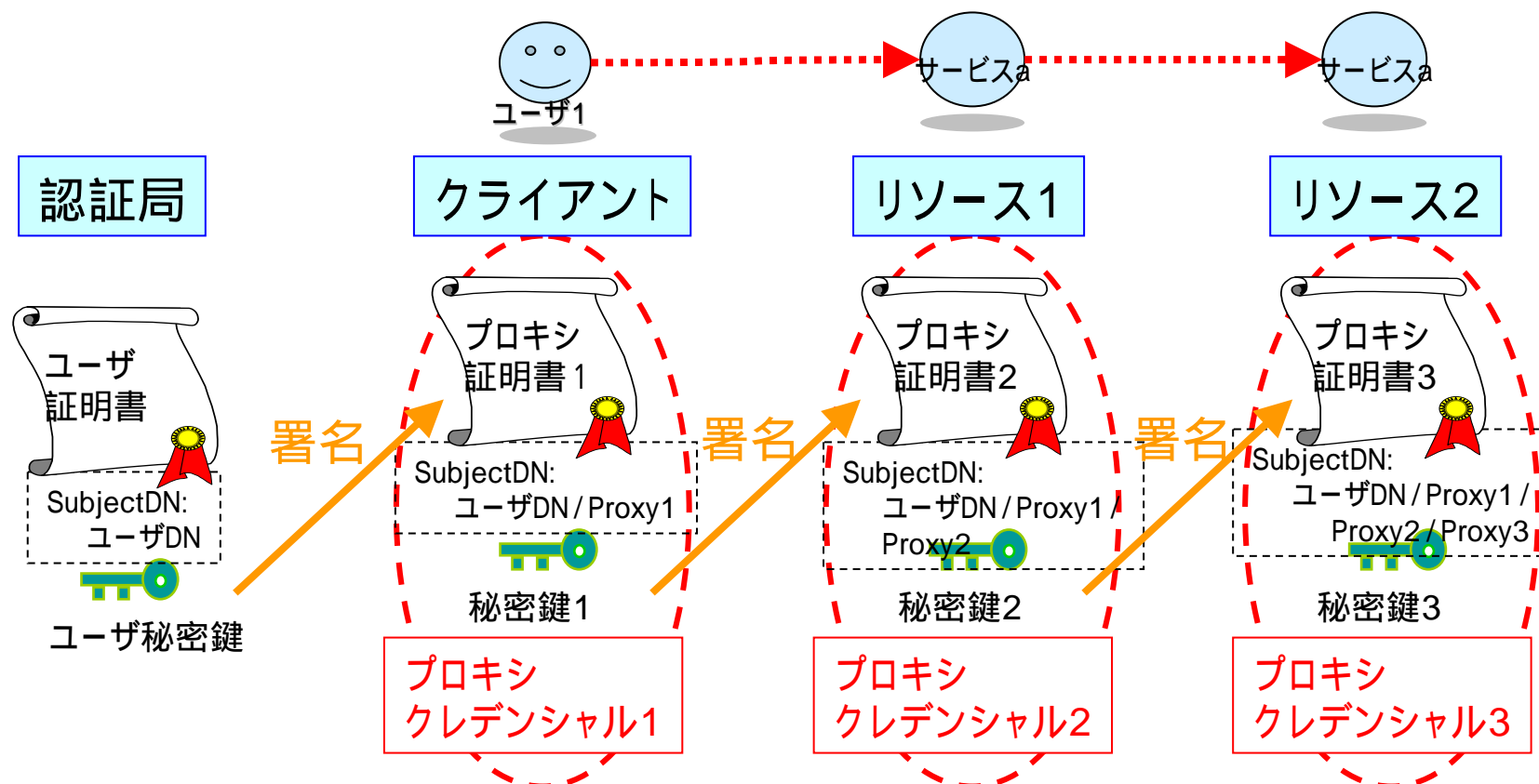


GSI - デレゲーションの流れ



プロキシ証明書チェーン

- プロキシクレデンシャルは各サーバのファイルシステム上へ保存
- リソース管理者はユーザのプロキシクレデンシャルを触らないという程度の信頼関係を仮定
- でも、ユーザDNはずっと先のリソースまで伝わる



これまでのGGF、OGFでのグリッドセキュリティの動向

- OGSA - WG: 2つのセキュリティ・プロファイルが公開された
 - OGSA Basic Security Profile 1.0 – Core
 - OGSA Security Profile 1.0 – Secure Channel
- OGSA - AuthZ - WG: OGSAでの認可サービスのプロトコルと標準属性フォーマットを規定
 - OGSi (Open Grid Service Interface)、SAML 1.1がベース
 - OGSA WSRF Basic Profileや、SAML 2.0、XACML 2.0などの最新の標準化動向へのキャッチアップが必要
- OGSAにおける認証に関する標準仕様の必要性が高まる
- ShibbolethによるID連携の応用が特にホット
- IGTF (International Grid Trust Federation):
 - 世界規模でのグリッド用のCA局の認証の枠組み
 - 各地域PMA (Policy Management Authority)での連携が軌道に乗っている

2. OGF19でのセッションの様子

OGSA - AuthZ - WG

- 議長: David Chadwick (英、ケント大学)
- 主な議題:
 - 今後のスケジュール: 電話会議日程 (2/13, 3/7, 4/3, 4/23)
 - 文書進捗:
 - グリッド・サービス・プロバイダのための認可サービスミドルウェアの機能要素 (認可アーキテクチャ)
 - 課題1件のみ。解決したいWGのファイナル・コールへ
 - プロトコル文書 (認可アーキテクチャで3つのプロトコルが規定)
 - 2つへ集約の方向 (WS-Trustプロファイル、XACML request/responseプロファイル)
 - Nate Klingenstein氏よりOASISではXACML request/responseプロトコルを破棄して新プロトコルを検討していると指摘
 - XACML request/responseプロトコルに関しては継続調査へ
 - VOMS属性プロファイル
 - MLで議論中
 - 属性取得プロトコル
 - Tom Scavo氏が執筆者となる予定
 - その他
 - Von Welch氏が共同議長を退任する予定 (後任を募集)

OGSA - AuthZの認可アーキテクチャ

- Functional Components of Grid Service Provider Authorisation Service Middleware
 - OGSAの認可に必要な機能を規定
 - それらの機能の4通りのインタラクションのパターンを規定

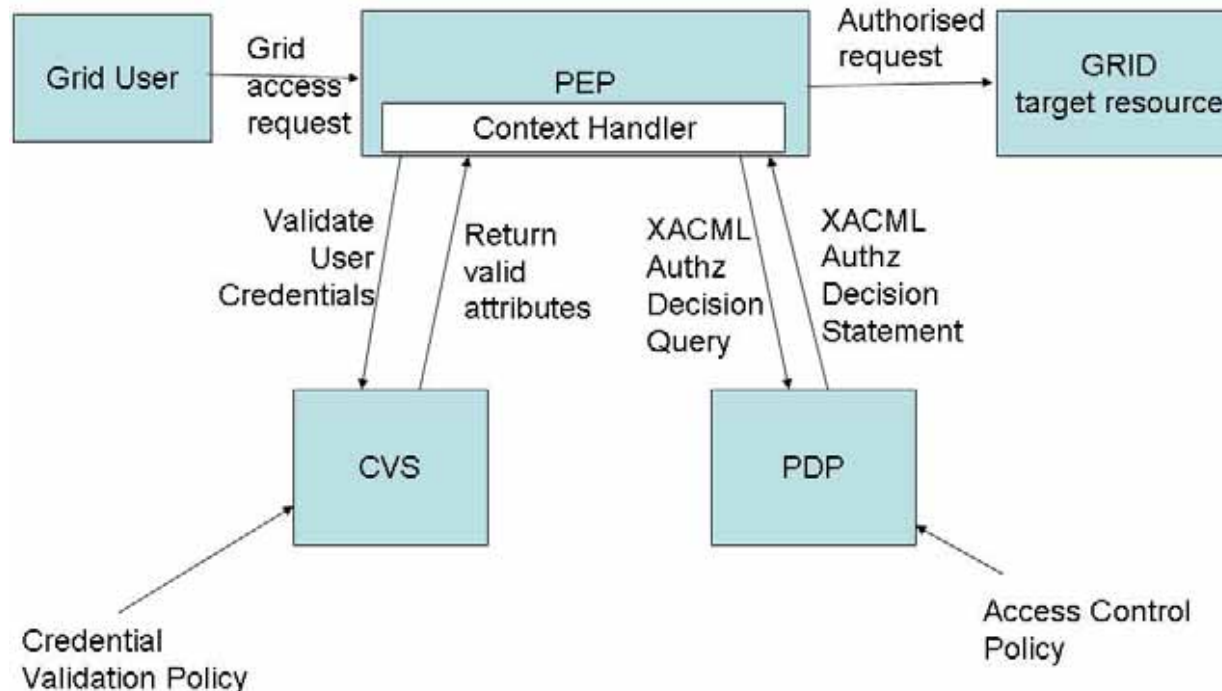


Fig 1 PEP Context Handler – Push Credential

XACML Context Profile

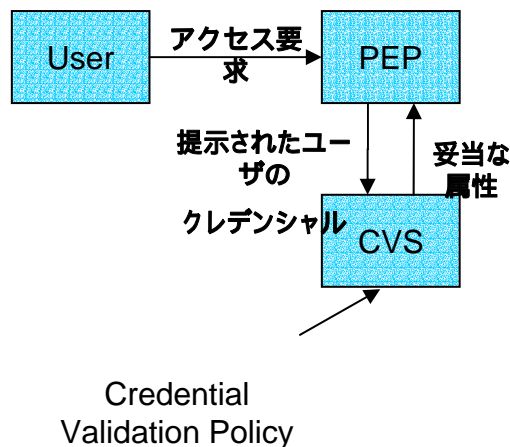
- Use of XACML Request Context to access a PDP
 - “SAML 2.0 profile of XACMLv2.0 (*)”のプロファイルを定める
- PDPへの認可問い合わせと応答の Protokol
 - SAML Request と Response Protokolを利用 (XACML Authz Decision Query と XACML Authz Decision Responseを定める)
 - 認可問い合わせにおいてXACML Request Contextを利用
 - 認可応答においてXACML Response Contextを利用
 - XACML Request Context中に埋め込む属性の形式を規定
 - 例)
ResourceAttributeには属性
”urn:oasis:names:tc:xacml:1.0:resource:resource - id”
の値として要求メッセージの<wsa:To>要素の内容を用いること など

* OASIS “SAML 2.0 profile of XACMLv2.0”. OASIS standard. 1 February 2005

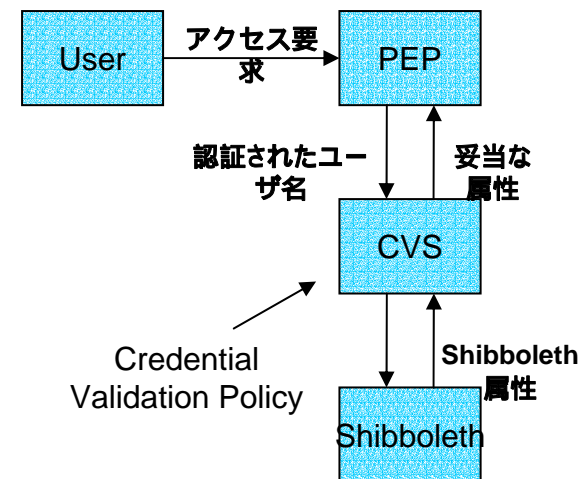
WS-Trust and SAML Profile

- Use of WS-TRUST and SAML to access a CVS
 - WS-TrustとProfiles for SAMLをベースにしたPEP、CVS間プロトコル
 - 提示されたユーザクレデンシャル(Push Mode)、あるいは、認証されたユーザ名(Pull Mode)を元に、CVSにより検証された当該ユーザの属性を要求するプロトコル
 - 応答メッセージにはXACML Request Contextへの変換を考慮した urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML 形式のSAML属性アサーションが返却される

Credential Push Mode



Credential Pull Mode



* Anthony Nadalin (Editor) "Web Services Trust Language (WS-Trust)",
Feb 2005 available from <ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf>

** OASIS. "Profiles for the OASIS Security Assertion Markup Language (SAML) V 2.0", OASIS Standard, 15 March 2005

OGSA - AuthN - BoFセッション

- 議長: Alan Sill (テキサス工科大学)
- 議題:
 - WG設立後の想定されるスコープについて議論が行われた
 - 認証とID引継ぎがスコープに入り、権限委譲はスコープ外、etc...
 - 作業項目に関する議論
 - 認証ユースケースとプロフィール [短期間で実現可能な物]
 - Username / Passwordなどによる認証に関する要件の検討
 - SAMLとグリッドの連携
 - より高機能な認証ユースケースの検討
 - 保証レベル(LoA)について
 - グリッドでの認証と認可にLoAが大きく関わる
 - LoA-RGによるアウトプット待ち
 - ロードマップ、マイルストーンについてはMLで継続検討
 - 現在の議論は主に、ShibbolethのNameIdentifierとX509証明書の属性のマッピングなどSAMLとGSIの連携に関することが中心

Security Area Meeting

- 議長: David Groep氏
- 議題:
 - Security Area Director交代の報告
 - David Groep氏 (UK e - Science Project)、Blair Dillaway氏 (Microsoft) が就任したことが報告された
 - Security Areaの動向報告
 - OGSA - AuthZ - WG
 - OGSA - AuthZ - WGのセッションの報告と共同議長募集の報告
 - FI - RG
 - 要求ドキュメントの完了と今後の活動方針について報告された
 - LoA - BoF
 - CAの保証レベル (Level of Assurance: LoA) に基づくきめ細かい認可の必要性について言及し、LoAに関するBoF提案の紹介とセッションへの参加呼びかけ
 - TC - RG
 - Trusted Computing - RGの活動が低調であることを理由に閉鎖されたことを報告
 - OGF内の関連活動について報告
 - CAOPs - WGとIGTF、OGSA - WG (Security Session)、HPC - Profile - WG、SAGA Security APIsに関して、セキュリティ関連動向について報告
 - Security Areaに属さないIWGなどでのセキュリティに対する関心の高まりについて言及
 - 特に認証への要求など

3. Federated Identity Workshop

Federated Identity Workshop

- 1/30(火) 9:00 ~ 17:30 (1.5h x 4 Sessions)
- 議長: Ken Klingenstein氏 (Internet2)
- Agenda:
 - Session 1: 全体的な概要
 - The Basics of Federated Identity: Ken Klingenstein@Internet2
 - Identity Federation: Some Challenges and Thoughts: Von Welch@NCSA
 - Session 2: 開発者よりの話
 - Rule-based data management: Reagan Moore@SDSC
 - Adapting to Federated Identity – SHEBANGS - : Mike Jones@Univ.of Manchester
 - Interoperability Shibboleth – gLite: Christoph Witzig@SWITCH
 - Federated Identity for Grid Architects: Tom Scavo@NCSA
 - Session 3: 運用者よりの話
 - All About Attributes (in federated identity): Nate Klingenstein@internet2
 - The Art of Federations: Ken Klingenstein@Internet2
 - The Role of the IGTF: Yoshio Tanaka@AIST
 - SuraGrid: Mary Fran Yafchak
 - TeraGrid: Von Welch@NCSA
 - Level of Assurance: Ning Zhang (UK e-Science)
 - Session 4: VO関連
 - Privilege Management: Ken and Nate Klingenstein@Internet2
 - caBig project: Grid Grouper:
 - Multiple source of Authorities
 - RP decision which SoA to rely on

Federated Identityとは?

- Federated Identityとは
 - 連携しているIdentity(識別子)
 - IdPからSPへ渡される情報 (bi-lateral)
 - Federationは上記のbi-lateralな連携が組み合わさったもの
- Identityとは
 - 連携している組織で管理されている識別子
- 属性と資格の付与
 - プライバシー保護への第一歩
- 現状
 - 学術教育(R&E)分野では急速に普及、公的機関ではぼちぼち、企業セクタでもいくつか事例が...

Federated identity and federations

- Federated identity – passing of information from an identity provider (IdP) to a relying party or service provider (SP) for an access control decision
 - Bi-lateral, likely appended to an existing business relation
 - Usually uses SAML
- Federation – bi-lateral or compound passing of information from several IdP and others to a SP
 - Multi-institutional, broad communities with multiple IdP and SP
 - Needs metadata management, more sophisticated attributes (including scoped), multi-lateral trust management, agreements on standards, more sophisticated AAP and ARP mechanisms, etc.
 - Usually uses Shibboleth or a compatible



Three Types of Identity

- Global basic identity
 - Passport, driver's license, qualifying X.509 cert
- Federated enterprise
 - Enterprise provides identity management for its users
 - Enterprises federate to build inter-realm trust and identity; federations peer
- Peer to peer
 - Self asserted, individual to individual
 - Lots of approaches, many clever
- Hybrids and others

Slide courtesy of Ken Klingenstein @Internet2

INTERNET² Attributes

- Attributes have well-defined syntax and semantics across the relevant community
 - Typically have controlled vocabulary of possible values, though some values are open-ended in meaning.
 - May be personally identifiable or more general
- Exist in many forms, from storage (LDAP) to transport (SAML, attribute certificates) to metadata (OIDs, rfc's, etc.)
- Come from “sources of authority”
- Are often used to determine access
- In shifting the focus from identity to attributes lies the ability to preserve privacy

- A particular and common attribute, giving a person permissions to use certain resources
- Are often delegated, constrained, time-limited, etc.
- Can be managed, at enterprise and end-user levels, with a privilege manager (e.g. Signet)
- Controlled complexity
- Have much to offer VOs in moving from identity-based authorization to better models

- Almost all software built on OASIS SAML standard. Many vendors moving towards SAML 2.0
- Most R&E federations use Shibboleth 1.x or a compatible (e.g. properly configured Sun Identity Manager, A-Select, etc.)
 - SAML and Shib have been deeply joined from the beginning (c 2000). Shared design, OpenSAML a major part of Shib, Scott Cantor (OSU) lead Shib architect and SAML 2.0 editor...
 - SAML addresses more the bi-lateral use case; Shib the multi-lateral
 - Apache 2.0 type license open source
 - Shib 2.0 alpha due out in April
- WS-Fed, part of WS-*
 - Proprietary MS and IBM trust framework
 - Works well with ADFS and enterprise MS

Federated Applications

- Mostly access controls to content
- The first shibbed collaborative apps are appearing...
 - Several wikis
 - Digital repositories such as DSpace and Fedora
 - Learning Management Systems such as WebCT
 - IM, p2p fileshare (Lionshare), CVS
- Grid-Shib integration in several ways
- SIP based tools (videoconferencing, audioconferencing) within reach
- Bootstrapping from duct tape sometimes a problem

Current State – R&E

- R&E federations moving forward rapidly in many countries, including the US, UK, France, Germany, Sweden, Australia, Switzerland, Norway, Netherlands, Finland, Denmark, etc.
- State university systems federate – Texas, California, Maryland, Cal State, Ohio, etc.
- Use primarily is access to content and services, but eScience, collaborative apps and virtual organizations are on the map
- In the US, InCommon has approximately forty members.

Current State - Gov

- Several national governments are developing federations of agencies and offering services to external users
- Within the US, several national governments are developing federations 😊
 - GSA EAuthentication
 - NSF
 - NIH
- Close and strange working relationships with InCommon

米国: eAuthentication

The screenshot shows a Mozilla Firefox browser window displaying the E-Authentication Home page. The browser's address bar shows the URL <http://www.cio.gov/eAuthentication/>. The page features a large header with the E-Authentication logo and the tagline "SECURE GOVERNMENT ACCESS ONLINE". Below the header is a navigation menu with links for Home, Key Personnel, Library, Links, News, and Partners. The main content area is divided into several sections:

- E-Authentication Mission:** Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. E-Authentication makes that trust possible.
- E-Authentication is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used.** The initiative will focus on meeting the authentication business needs of the E-Gov initiatives, building the necessary infrastructure to support common, unified processes and systems for government-wide use. This will help build the trust that must be an inherent part of every online exchange between citizens and the Government.
- E-Authentication Federation Expands:** The *E-Authentication Federation* achieved significant growth last week with the addition of 15 new relying party systems. This expansion more than doubles the total of operational relying parties in the Federation, bringing that number to 31 systems. [Click here for more](#).
- E-Authentication Launches Federation:** The E-Authentication Initiative has successfully launched the E-Authentication Federation, a public-private partnership that will enable citizens, businesses and government employees to access online government services using log-in IDs issued by trusted third-parties, both within and outside the government. [Click here for more](#).
- E-Authentication Publishes Interface Specification 1.1**

On the right side of the page, there are several sections with links:

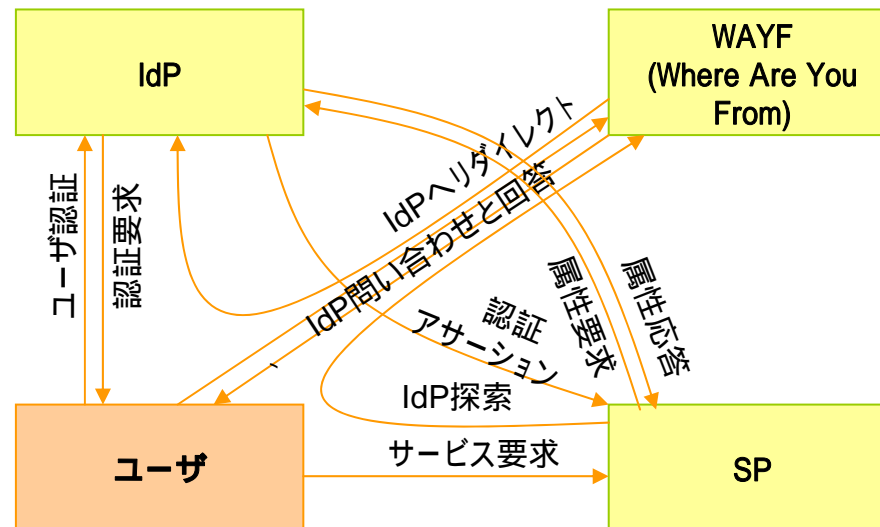
- Policy:** [Guidance for Federal Agencies](#), [NIST Special Publication 800-63](#), [X.509 CP for the E-Governance CA's](#)
- Getting Started:** [Legal Document Suite](#), [Technical Architecture](#), [Selecting an Approved Technology](#), [E-Authentication Federation Membership List](#), [Handbook for Federal Agencies](#), [Handbook for Credential Service Providers](#), [Cookbook](#)
- Assessment:** [E-RA](#), [Credential Assessment Suite](#), [Guide for Preparing a Credential Assessment](#)
- Testing:** [Lab Application](#), [Interoperability Lab Concept of Operations](#)
- Implementing E-Authentication:**

Shibbolethとは

- 米国Internet2 / MACE (Middleware Architecture Committee for Education) によるプロジェクト
- 大学・研究機関などの組織間でセキュアにリソース共有を実現するためのアーキテクチャと仕様、オープンソース実装を提供
 - 連携管理、属性ベース認可、プライバシー管理、標準仕様への準拠、複数のスケール可能な信頼とポリシーセットのフレームワーク、標準であるが拡張可能な属性の利用
 - Federationを実現できる

Shibboleth ブラウザ/アーティファクトプロファイル

- ~ 、WAYF(Where Are You From)を用いたIdP探索とリダイレクト
- 、 IdPによるユーザ認証
- IdPからSPへの認証アサーション送付
- 、 SPがIdPへ属性アサーション要求と応答
- IdPでユーザのログイン状況を把握することにより、2回目以降の認証要求に対してはSSOが可能
- SAML1.1 ブラウザ/アーティファクトプロファイルがベース



Federationの実例

Federation	国	概要	運営組織	参加組織数
InCommon	米国	商用レベルのFederation。ポリシーが厳密で、加入条件が厳しい。有料 URL: http://www.incommonfederation.org/	Internet2	約40
InQueue	米国	テスト目的Federation。世界各国から数多くの参加組織。現在は新規加入は停止し来年閉鎖予定 URL: http://inqueue.internet2.edu/	Internet2	約200
SWITCHaai	スイス	主にスイス国内の大学や研究機関がIdPとして参加。SPとしては欧州各国(ドイツ、オランダ、イタリア、ベルギー、フランス等)の組織が参加 URL: http://www.switch.ch/aai/	The Swiss Education & Research Network	約40
SDSS	英国	主にイギリス国内の大学や研究機関が参加。今後は、UK Access Management Federationに移行する予定。 URL: http://sdss.ac.uk/ URL: http://www.ukfederation.org.uk/	EDINA	約50
Haka	フィンランド	主にフィンランド国内の大学や研究機関が参加している。 URL: http://www.csc.fi/suomi/funet/middleware/english/	CSC (Finnish IT center for science)	約20

SHEBANGS

- SHEBANGS (Shibboleth Enabled Bridge to Access the National Grid Service)
- SHEBANGSは英国のNational Grid (NGS)での Federation適用の試み
- NGSへのログオンと利用はGSIクレデンシャルが必要
- Credential Translation Service (CTS)がShibboleth SPとしてIdPからユーザの属性を取得
- CTSがユーザの属性を元にGSIクレデンシャルを生成し、NGSのMyProxyへ格納 (On-line CAとして動作)
- ユーザはポータルを通じてNGSを利用 (上記でMyProxyに格納されたGSIクレデンシャルを利用する)

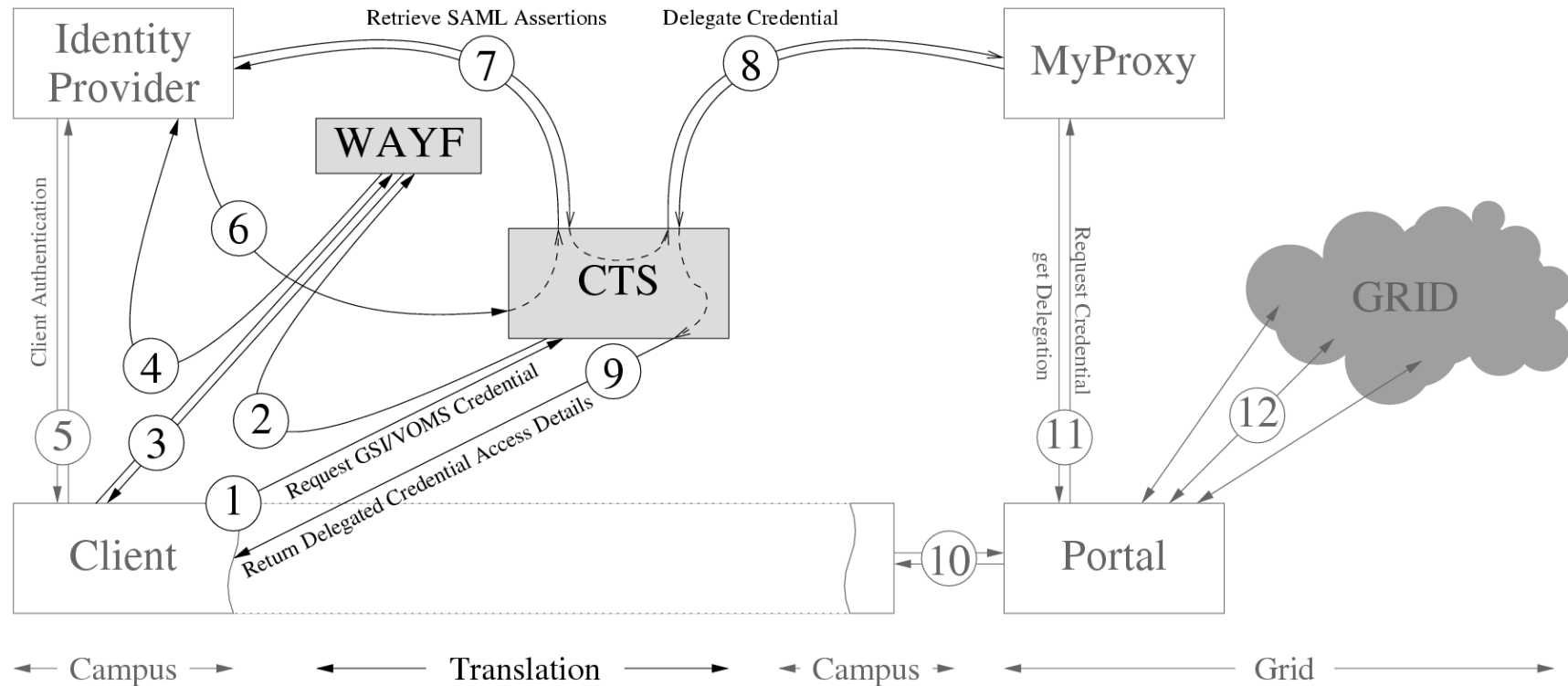
Portal Access to the National Grid Service Today

1-7 Client logs into CTS via Shibboleth Mechanisms

7.5 CTS creates an X509 Certificate based upon SAML Assertions

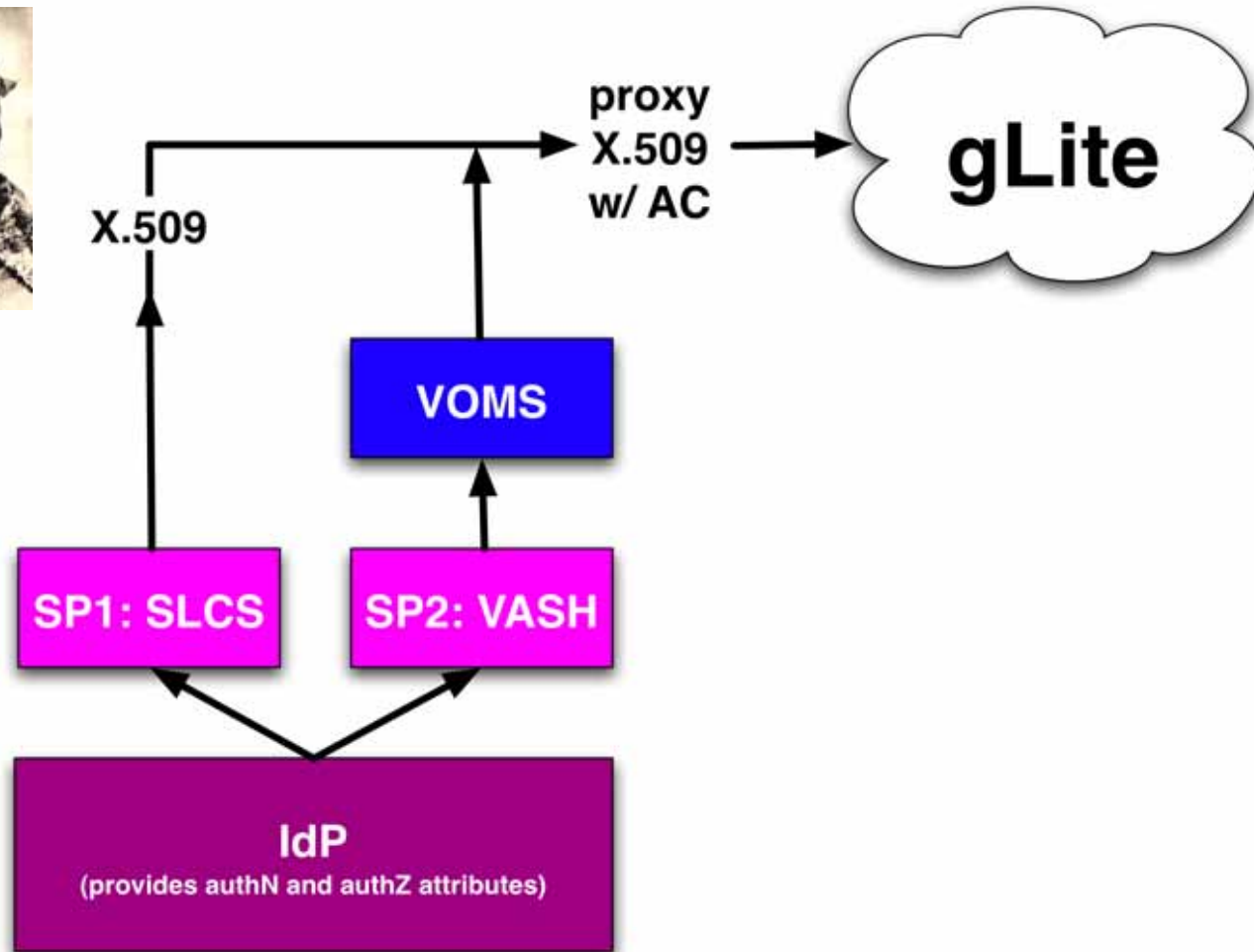
8 CTS delegates a GSI Proxy certificate to MyProxy

9-12 Client uses username/password/MyProxy triplet to access the Grid via the Portal



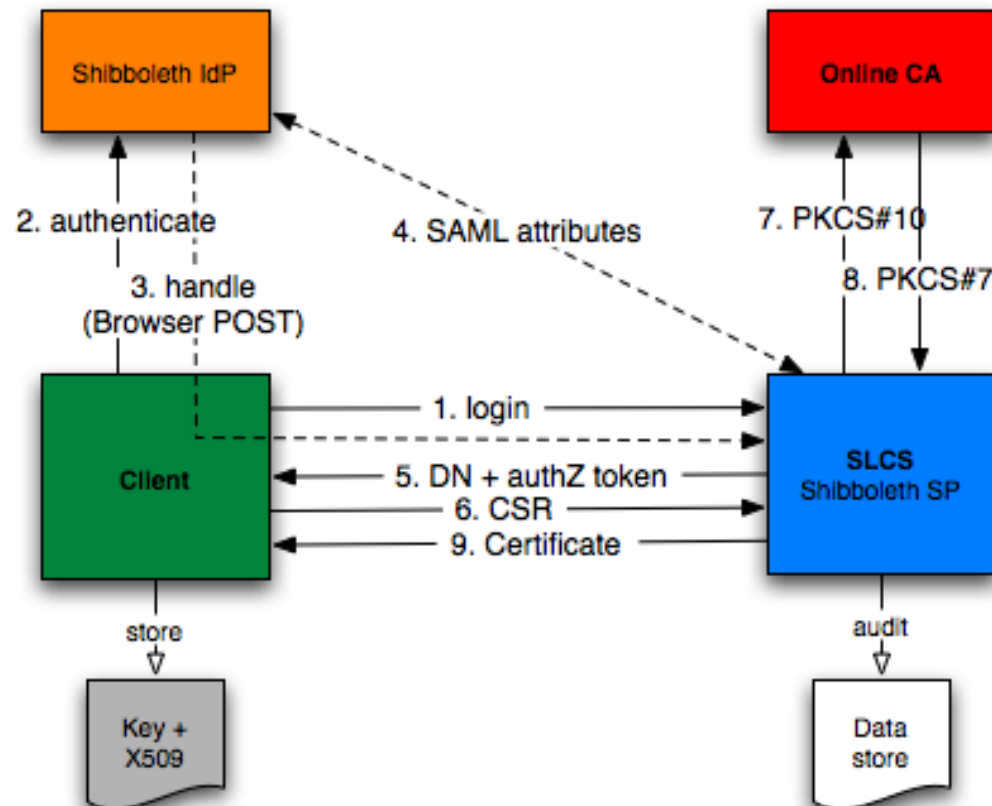
SWITCH

- EGEE (gLite) プロジェクトの一部
- SWITCHaai – a national Shibboleth - based AAIを構築、運用
 - 16万人の高等教育分野のメンバーの75%がSWITCHaaiのアカウントを保有
 - 100個程度のリソースへのアクセスのうち10%がSWITCHaai経由
- Shibbolethと相互運用する2つのSPを開発
 - SLCS (Short Lived Credential Service)
 - VASH (VOMS Attributes from Shibboleth)
 - できるだけ固有のミドルウェアの依存を排除する方針
- Shibboleth以外のFederationもターゲット



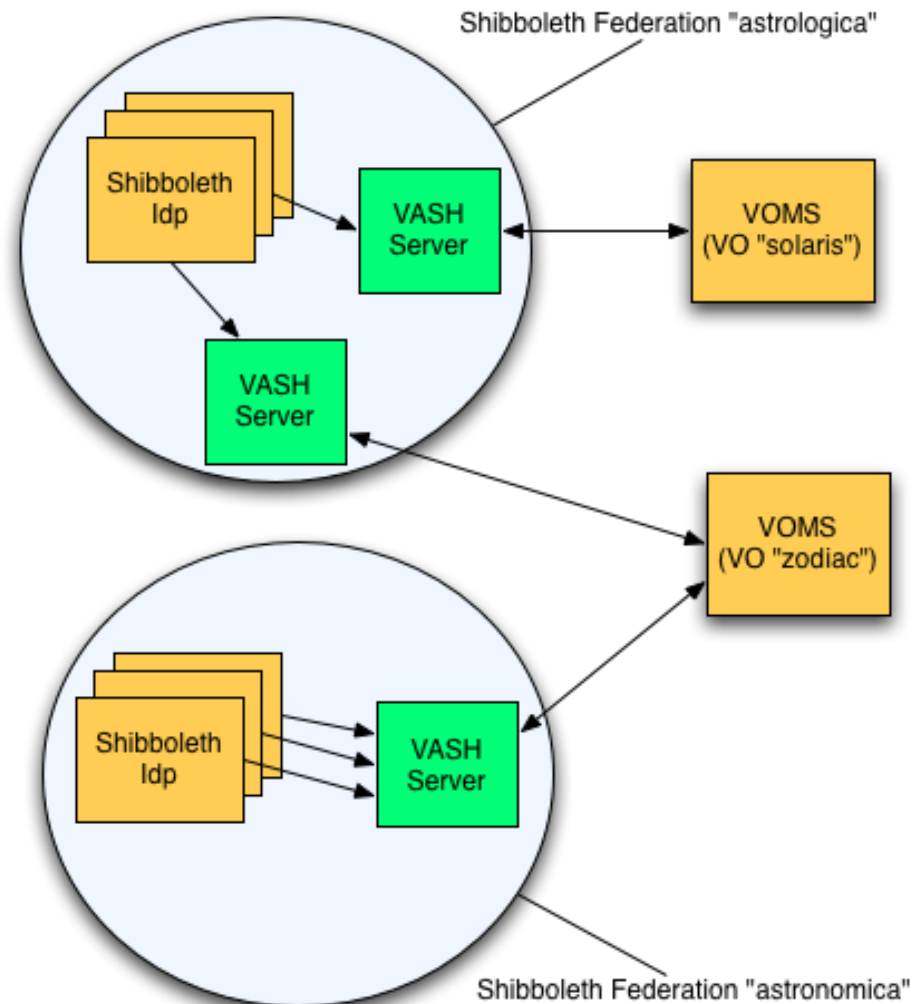
Slide courtesy of Christoph Witzig@SWITCH

- Design goals:
 - Private key is never transferred
 - Use commercial CA and only standard protocols
 - Modular design such that other people can use components



Slide courtesy of Christoph Witzig@SWITCH

- **VASH:**
 - VOMS Attributes from Shibboleth
- **Shibboleth SP**
 - Browser-based
 - Specific for
 - Federation
 - VO
- **“lightweight” SP**
 - No administrator duties
 - No management of attributes
 - Simply transfers attributes upon user request



Slide courtesy of Christoph Witzig@SWITCH

GridShibプロジェクト

- GridShib:
 - NSF(全米科学財団)が出資し、NCSA、シカゴ大、アルゴンヌ国立研究所が主導するプロジェクト
 - Shibbolethが発行する属性をGlobus Toolkitでの認可に利用することが狙い
- GridShibプロジェクトでの成果について簡単に紹介
 - Globus Toolkit拡張、Shibboleth IdP拡張、Shib-enabled CA、SAMLツール、IdP Proxy(myVocs)
- グリッドでShibbolethを利用する際の問題点について考察
 - NameIdentifierとグリッドでのIDのマッピングの問題
 - Attribute Pullの時のIdP発見、Attribute Pushの時のSP発見の問題
- 方向性としては...
 - Attribute Pushで、IdPからの属性を含め必要な属性をX509証明書へ埋め込み、既存のグリッド基盤で利用する?
 - 前提としてはリソース側がShibbolethのNameIdentifierを判別できる



Implemented Software

- Globus Toolkit extensions
 - ◆ Grid SP protects Grid resources
- Shib IdP extensions
 - ◆ Provides name mapping plugins and certificate registry UI
- Shib-enabled CA
 - ◆ Issues short-lived X.509 end-entity credentials to be stored on the desktop
- SAML Tools
 - ◆ Issues short-lived SAML and X.509 for VOs

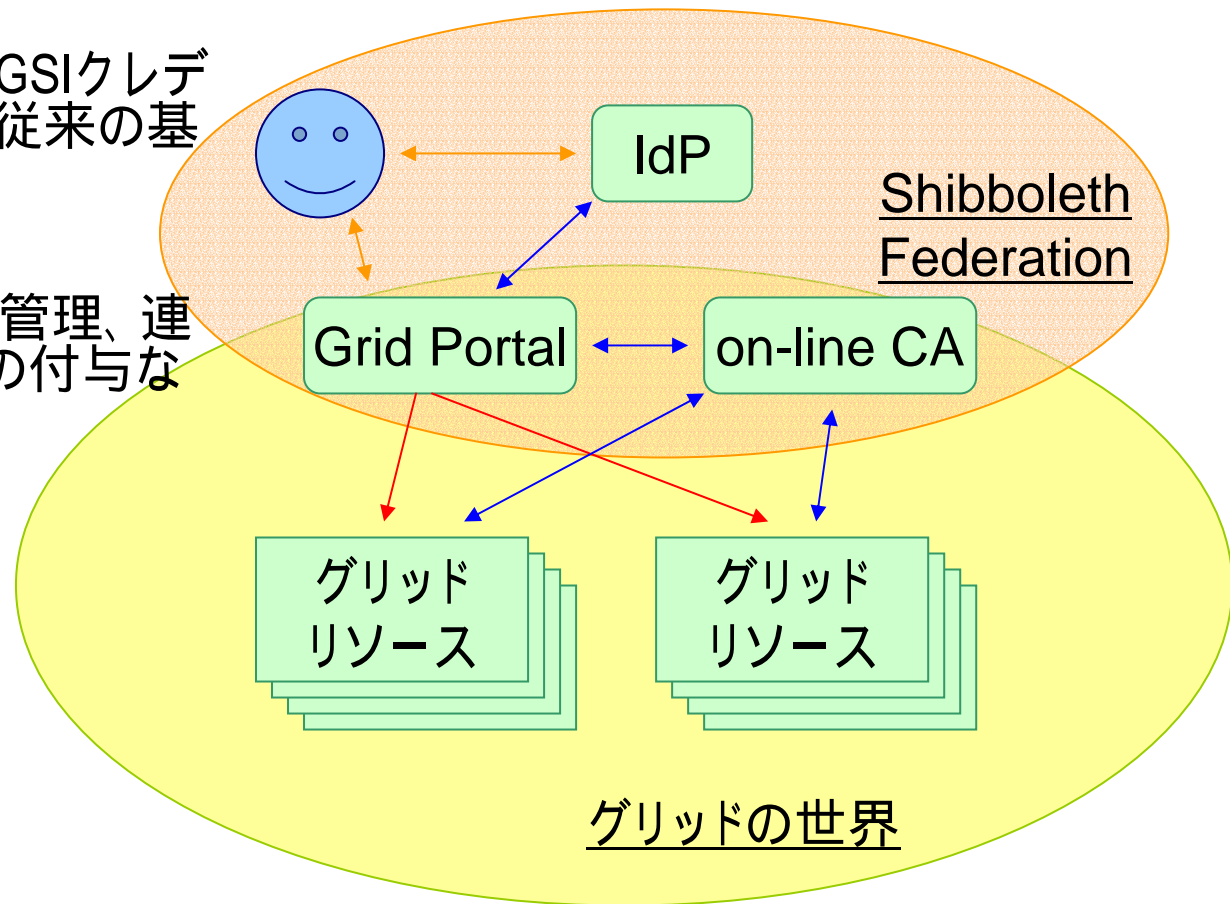


IdP Proxy

- Another essential VO middleware component is the *IdP Proxy* (e.g., myVocs)
- An IdP Proxy is useful because:
 - ◆ There is a paucity of campus attributes (and campus admins are loathe to add more)
 - ◆ VOs have unique attribute requirements
 - ◆ A layer of abstraction between the campus IdPs and the Grid SPs provides flexibility
- Much activity in this space (UAB, MAMS, USC, D-Grid)

Shibboleth - Grid連携について

- 方向性としては、
 - 認証と属性の管理は ShibbolethのFederationを利用
 - グリッドの世界ではGSIクレデンシャルを利用し、従来の基盤をそのまま利用
- あわせて、
 - グリッド側での属性管理、連携Idに対する権限の付与などの検討も



まとめ

- OGSA - AuthZ:
 - OGSIBベースのプロファイルから新たなプロファイルを作成する方向にあることを紹介した
 - プロファイルのうち、XACML Request Context ProfileとWS - Trust Profileの概要を紹介した
- OGSA - AuthN:
 - OGF19でのBoFセッションの動向を報告した
 - 数ヶ月のうちにユースケースとプロファイル、それより長期のスコープで複数のセキュリティトークンを用いた認証、より高機能な認証について見当
- Federated Identity Workshop
 - 欧米ではShibbolethを代表とするID連携の仕組みがR&E分野から公的分野へ広がりつつあることを紹介した
 - ShibbolethのID連携を用いたグリッド利用が欧米ではほぼ実現しつつあることを紹介した
 - 特にShibbolethとGridの相互運用では、on-line CAをShibboleth SPとして構築し、Shibbolethでの認証と属性の取得後は既存のグリッド基盤を利用する例を紹介した

References

- OGF19 Schedule Federated Identity (1 / 4):
http://www.ogf.org/gf/event_schedule/index.php?id=574
- The Basics of Federated Identity – Ken Klingenstein:
http://www.ogf.org/OGF19/materials/574/fedid_basics.ppt
- The Art of Federated Identity - Ken Klingenstein:
http://www.ogf.org/OGF19/materials/574/art_of_federations.ppt
- Adapting to the Federated Identity – Mike Jones:
http://www.ogf.org/OGF19/materials/574/adapting_to_federated_identity.ppt
- Interoperability Shibboleth – gLite - Christoph Witzig:
http://www.ogf.org/OGF19/materials/575/070130_OGF19_SWITCH.ppt
- Federated Identity for Grid Architects – Tom Scavo@NCSA:
<http://www.ogf.org/OGF19/materials/575/ogf19-fidm-architects.ppt>

Empowered by Innovation

NEC

著作権について

本資料中に引用しているスライドは下記記載の通りOGFが著作権を持つスライドです。

Full Copyright Notice



Copyright (C) Open Grid Forum (2007). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.

The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assignees.