International Symposium on Grid Computing 2008

An Experience in Developing Common Certificate Policy

9 April 2008, Academia Sinica, Taipei, Taiwan

Shinichi Mineo
(RIKEN)

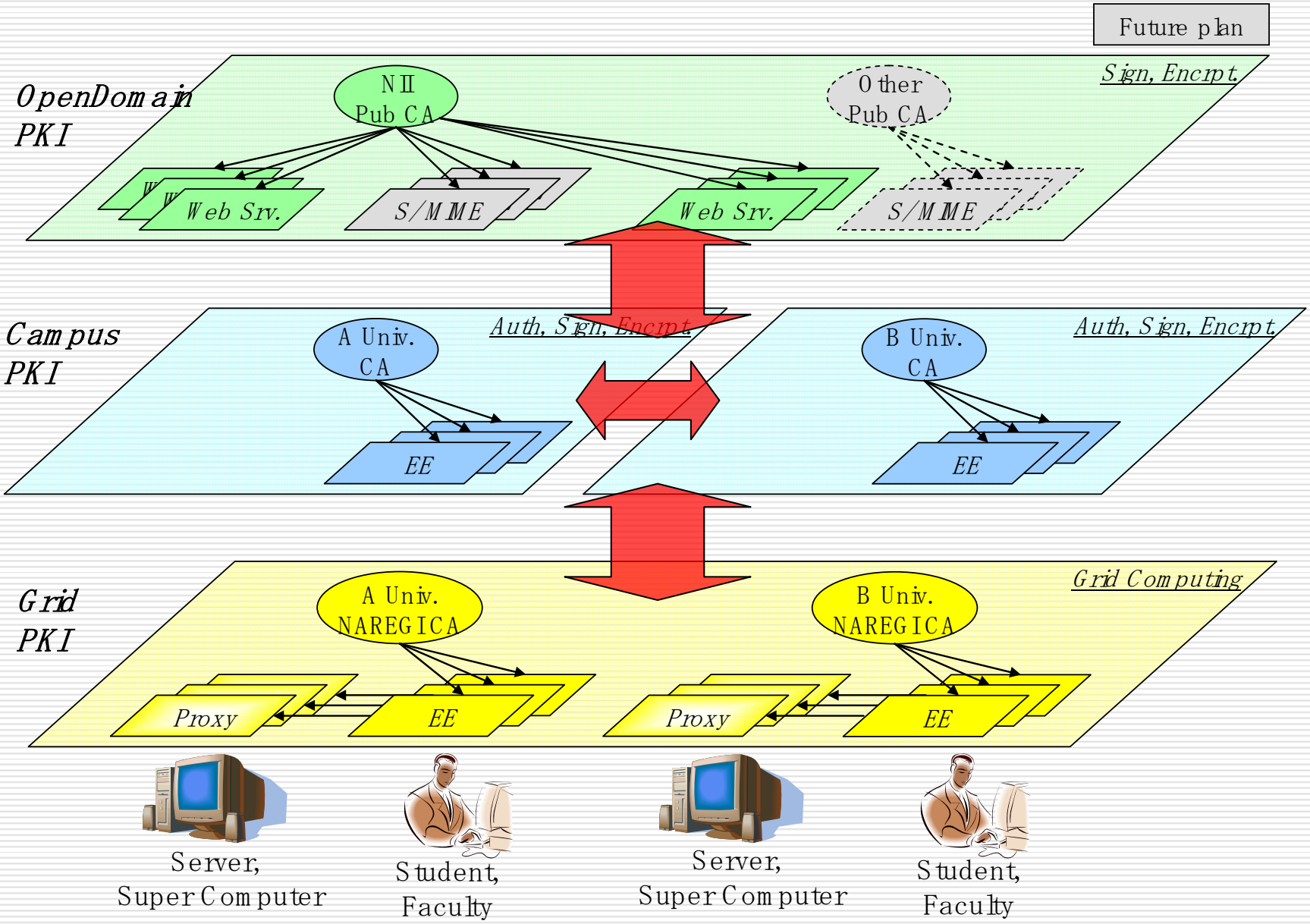
Outline

- MOTIVATION
- FEATURES OF RFC3647
- A CASE IN NAREGI
- DRAFTING A COMMON CP
- OPEN ISSUES
- SUMMARY

MOTIVATION

- Preparation for CA operations based on RFC 3647
  - NAREGI CA plans to restart operation with a new CP/CPS
- Deployment Plan of Grid CAs by UPKI
  - Increasing complexity for trust federation
- CP Sensitive Application
  - Possibility of flexible authorization for Grid Applications

UPKI as a basis of Cyber Science Infrastructure



FEATURES OF RFC3647 (1)

- Easy to transform CP/CPS based on RFC 2527 to RFC 3647
  - (7) “Comparison to RFC 2527”
  - Just adding (4.9) “Other Business and Legal Maters”, etc
- It’s OK, but…
  - Another idea is to develop a new CP split from CPS

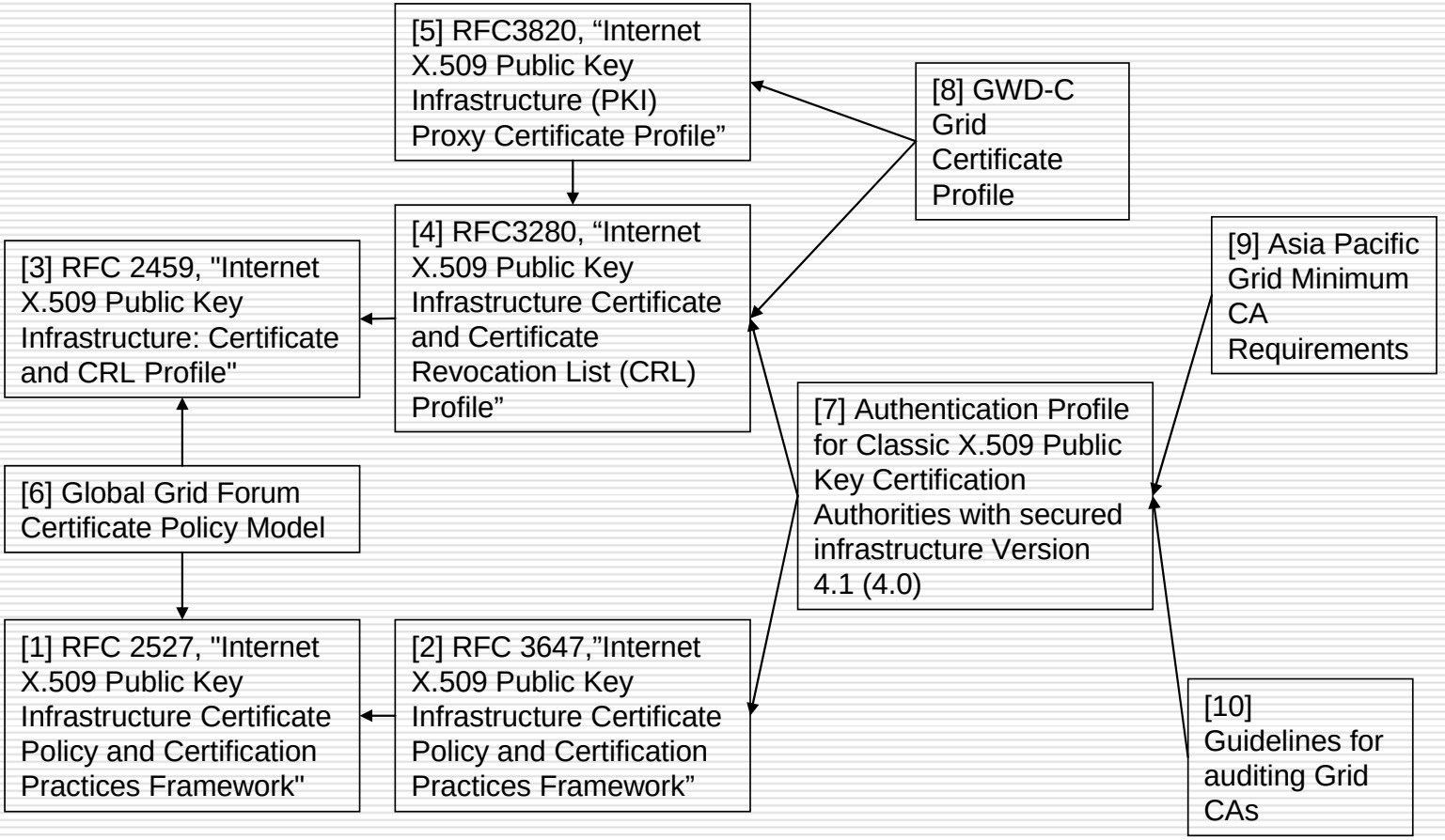
FEATURES OF RFC3647 (2)

- CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements, and CPS is a statement of the practices which a certification authority employs in issuing certificates.(1.1)
- A CP generally applies to multiple CAs, and a CPS applies only to a single CA. (3.5)
- CP and CPS have the same structure and ordering of topics, thereby facilitating comparisons and mappings among these documents (3.7)
- Document framework is the same in CP and CPS, but their objectives are different.

A CASE IN NAREGI (1)

- A traditional X.509 Public Key CA
  - issues long-term credentials to end-entities
  - conforms to the Asia Pacific Grid Minimum CA Requirements
- An Analysis of the documentation structure regarding to accreditation of ApGrid PMA

An Analysis of Documentation Structure



NOTE) Arrows show relations of conformity to each other

A CASE IN NAREGI (2)

- Why split CP from CPS?
  - Grid CAs can concentrate on designing CPS based on the common CP, which will save money and time.
  - The regional PMA can concentrate on analyzing CPS to accredit Grid CAs, which will decrease a lot of work load.
  - The Grid CAs can enforce mutual audit based on the common policy, which will make the work simple and efficient.

A CASE IN NAREGI (3)

- A Trial to design a Common CP
  - Collection of common security requirements for Grid applications
    - excluding descriptions peculiar to CAs or organizations.
  - The CP demands a CA to describe individual information in CPS
    - the Demands themselves are treated as a part of the Certificate Policy
  - For items with no special requirements either in CP or CPS, “No requirements” is described
    - These items can be described at discretion of the CA

DRAFTING A COMMON CP

- We have analyzed all the sections of RFC3647 framework, and classified them into groups of:
  - CP: To be described in CP
  - CPS: To be described in CPS conforming to the requirements of this CP
  - None: No Requirements

A Table of Classification (1)

RFC3647 section				RFC25	IGTF ClassicAP	CP	CPS
1			Introduction	1	1		
	1.1		Overview	1.1	2 4.2	レ	レ
	1.2		Document Name and Indentification	1.2	4.2	レ	レ
	1.3		PKI Participants	1.3			
		1.3.1	Certification authorities	1.3.1	2	レ	レ
		1.3.2	Registration authorities	1.3.2	2	レ	レ
		1.3.3	Subscribers	1.3.3			レ
		1.3.4	Relying parties	1.3.3			レ
		1.3.5	Other participants	N/A			
	1.4		Certificate usage	1.3.4			
		1.4.1	Appropriate Certificate Uses	1.3.4		レ	レ
		1.4.2	Prohibites Certificate Uses	1.3.4			
	1.5		Policy Administration	1.4			
		1.5.1	Organization Administering the Document	1.4.1		レ	レ
		1.5.2	Contact Person	1.4.2		レ	レ
		1.5.3	Person Determining CPS Suitability for the Policy	1.4.3		レ	レ
		1.5.4	CPS Approval Procedures	8.3		レ	レ
	1.6		Definition and Acronyms	N/A		レ	レ
2			Publication and Repository Responsibilities	2.1.5,2.6			
	2.1		Repositories	2.6.4	6	レ	レ
	2.2		Publication of certification information	2.6.1,8.2	4.2 4.3 4.4 6	レ	レ
	2.3		Time or frequency of publication	2.6.2,8.2			レ
	2.4		Access controls on repositories	2.6.3			レ

A Table of Classification (2)

RFC3647 section				RFC25	IGTF ClassicAP	CP	CPS
3			Identification and Authentication (I&A)	3			
	3.1		Naming	3.1			
		3.1.1	Type of Names	3.1.1		レ	
		3.1.2	Need for Names to be Meaningful	3.1.2	4.3	レ	
		3.1.3	Anonymity or Pseudonymity of Subscribers	3.1.2			
		3.1.4	Rules for Interpreting Various Name Forms	3.1.3			
		3.1.5	Uniqueness of Names	3.1.4	3	レ	
		3.1.6	Recognition, Authentication,and Role of Trademarks	3.1.5,3.1.6			
	3.2		Initial Identity Validation	3.1	3.1		レ
		3.2.1	Method to Prove Possession of Private Key	3.1.7	3.1	レ	レ
		3.2.2	Authentication of Organization Identity	3.1.8			レ
		3.2.3	Authentication of Individual Identity	3.1.9	3.1	レ	レ
		3.2.4	Non-Verified Subscriber Information	N/A			レ
		3.2.5	Validation of Authority	3.1.9			レ
		3.2.6	Criteria for Interoperation	4.1			レ
	3.3		I&A for Re-key Requests	3.2,3.3			
		3.3.1	Identification and Authentication for Routine Re-Key	3.2	3.2	レ	レ
		3.3.2	Identification and Authentication for Re-Key After Revocation	3.3			レ
	3.4		I&A for revocation requests	3.4		レ	レ

The rest is omitted.

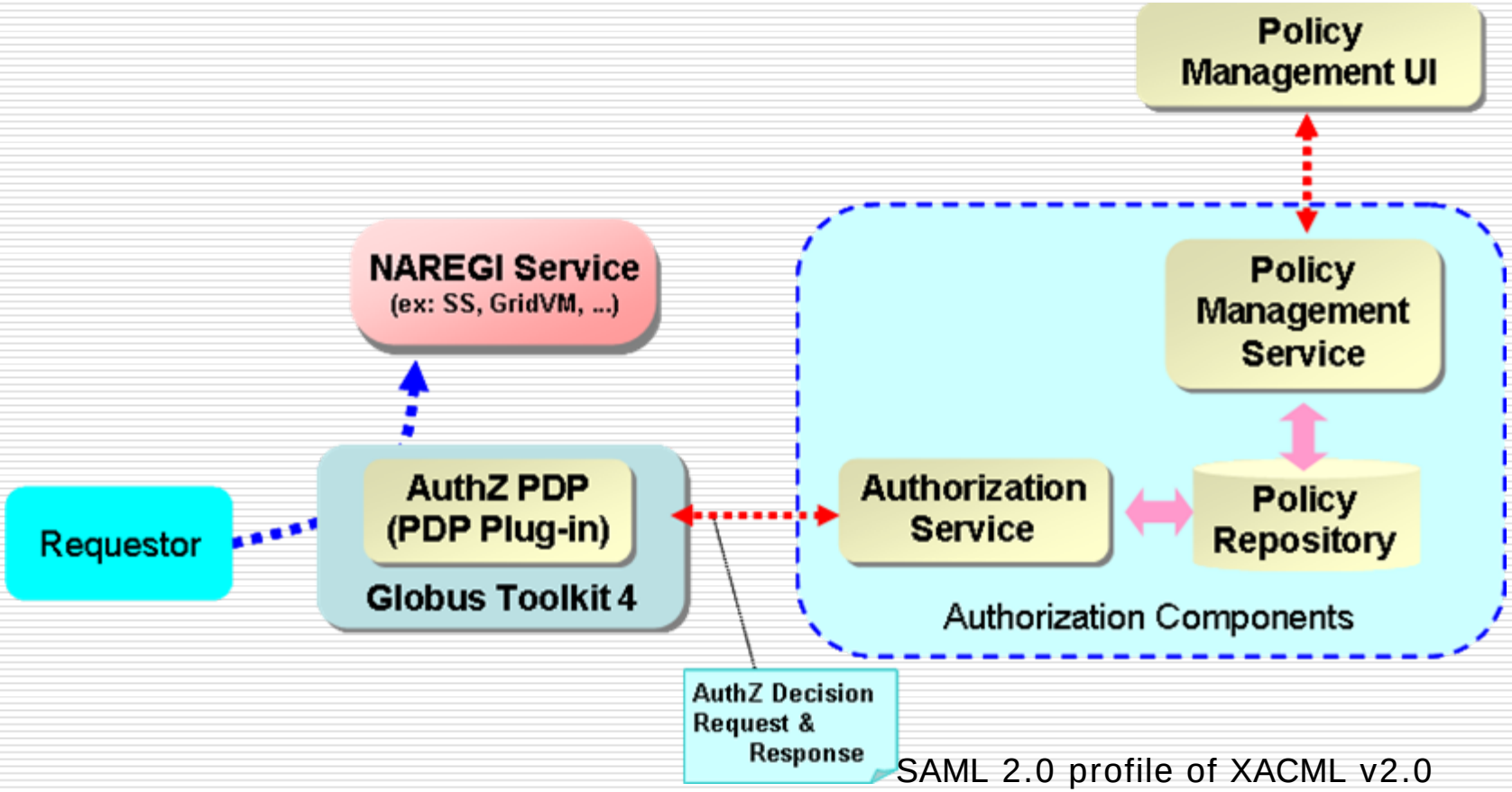
CertifatePolicies EXTENTION in ASN.1 NOTATION

```
CertifatePolicies EXTENTION ::= {
  SYNTAX CeritificatePoliciesSyntax
  IDENTIFIED BY id-ce-certificatePolicies }
CertifiatePoliciesSyntax ::= SEQUENCE SIZE(1..MAX) OF
PolicyInformation
PolicyInformation ::= SEQUENCE {
  PolicyIdentifier CertpolicyId,
  PolicyQalifiers PolicyQualifierInfo}
CertPolicyId ::= OBJECT IDENTIFIER
PolicyQalifierInfo ::= SET {pointerToCPS-Qualifier
pointerToCPS,
          noticeToUser-Qualifier noticeToUser OPTIONAL)}
pointerToCPS ::= {POLICY-QUALIFIER-ID  id-qt-cps
QUALIFIER-TYPE   CPSuri }
Id-qt-cps  OBJECT IDENTIFIER ::= { id-qt 1 }
CPSuri ::= IA5String
```

OPEN ISSUES

- Future Capability of the common CP
  - If this CP is proved operational and effective, it is worth to commonly used in the Grid community accredited by ApGrid or IGTF.
- CP Sensitivity
  - If the Grid application can recognize Certificate Policies, a Grid CA can issue certificates of different policies, with which Grid service providers will be able to change authorization decisions according to their service policies.
- Legal Matters
  - Legal matters tend to be different in nations. We need consensus on general conditions for Grid certificates.

An Example: CP Sensitive AuthZ Service



CONCLUSIONS

- We have described a possibility of a common certificate policy, which NAREGI is trying to develop and planning to use for the next generation CA operations.
- We believe a common CP concept is effective for both Grid CAs and the regional PMAs, and contributes to the Grid community.
- Further discussions will be necessary for consensus and the open issues in public place such as CAOPs working group in OGF.
- A draft of a common CP with a sample of CPS will be published by NAREGI project for open discussions.