# Securing Grid and Cooperative Computing :

## OGSA, Globus, Vega Experiences and Research Frontiers on Grid Security

**Kai Hwang**
kaihwang@usc.edu
**Internet and Wireless Security Laboratory**
**University of Southern California**
**Los Angeles, CA. 90089 USA**

**Keynote Address at the**
**International Workshop on Grid and**
**Cooperative Computing (GCC2002)**
**Sanya, China, Dec. 26, 2002**

# Presentation Outline:

- **Grid Projects and Security Issues**
  - National Projects in US, Europe, and China
  - Grid Security Issues and Approaches
- **OGSA and Globus Security Architecture**
  - The Open Grid Service Architecture (OGSA)
  - The Globus Security Infrastructure (GSI)
- **Grid Security Research Frontiers**
  - Mobile IPv6 and WTLS for the mobile world
  - Wireless PKI Architecture and Interoperability
  - XML for Security in Internet, Web, and Grid services
  - DRM for protecting copyrights in digital contents
  - Automated intrusion detection and response systems

# What is Grid Computing?

- An information infrastructure that couples
  - Computers (PCs, workstations, clusters, traditional supercomputers, and even laptops, notebooks, mobile computers, PDA, and so on)
  - Software ? (e.g., renting expensive special purpose applications on demand)
  - Databases (e.g., transparent access to human genome database)
  - Special Instruments (e.g., searching for Life in galaxy)
  - People (may be sensors or even animals who knows ?)
- Across the local/wide-area networks (enterprise, organizations, or the Internet) and presents them as an unified integrated computing resource.

# GRID Projects and Initiatives

**http://www.gridcomputing.com/**

- Public Forum
  - Computing Portals
  - Grid Forum
  - European Grid Forum
  - IEEE TFCC
- Australia
  - Nimrod/G
  - EcoGrid and GRACE
  - DISCWorld
- Europe
  - UNICORE
  - MOL
  - METODIS
  - Globe
  - Poznan Metacomputing
  - CERN Data Grid
  - MetaMPI
  - DAS
  - JaWS

- Public Grid Initiatives
  - Distributed.net
  - SETI@Home
  - Compute Power Grid
- USA
  - Globus
  - Legion
  - JAVELIN
  - AppLes
  - NASA IPG
  - Condor
  - Harness
  - NetSolve
  - NCSA Workbench
  - WebFlow
  - EveryWhere
- Japan
  - Ninf
  - Bricks
- China
  - Vega
  - ChinaGrid

# National Grid Projects in The USA

| Grid Project | Launch | Sponsor | Main Purpose |
|---|---|---|---|
| **Access Grid** | 1999 | DoE and NSF www-fp.mcs.anl. gov / fl/ accessgrid | Internet-based collaboration among scientists at facilities worldwide |
| **GriPhyN** (Grid Physics Network) | 2000 | NSF | Data analysis for 4 physics projects in CERN's collider and other sites |
| **Information Power Grid** | 1999 | NASA | Computing support for aerospace, planetary, and NASA applications |
| **iVDGL** (Int'l Virtual DataGrid Lab) | 2002 | NSF and counterparts in Europe, Austrialia, and Japan | World's first global grid linking computer centers in Europe, US, Australia, and Japan |
| **NEESgrid** (Network for Earthquake Engr. and Simulation) | 2001 | NSF www.neesgrid.org | Integrated computing environment for 20 earthquake engineering labs |
| **TeraGrid** | 2002 | NSF www.teragrid.org | Science grid by linking 4 sites at 4 Gbps and up-to 13.6 Tflops in speed |

# Grid Projects in Europe and China

| Grid Project | Launch | Sponsor | Main Purpose |
|---|---|---|---|
| European Data Grid | 2001 | European Union www.eu-datagrid.org | Data analysis in high-energy physics, environmental science and bioinformatics |
| UK National Grid | 2001 | UK Office of Science and Technology | Support for grid projects within Britain |
| Unicore | 2000 | German Ministry for Education and Research | A seamless interface to computer centers at 9 govovernment, industry and academic labs |
| China National Grid | 2002 | Ministry of Science and Technology, China | A national service grid for science, environment, resources, manufacturing, and industry |
| Vega | 2001 | Chinese Academy of Science, Beijing www.grid.org.cn | A scientific computing grid built around the Dawning superserver series |
| ChinaGrid | 2002 | Ministry of Education, China | An educational computing grid linking more than 100 Chinese universities |

# Increasing Security Demands in Internet and Grid Computing Applications

- LANs, clusters, Intranets, Web, Grids, and Internet all demand security protection hacker-proof operations, crucial to the acceptance of a trust-based digital society

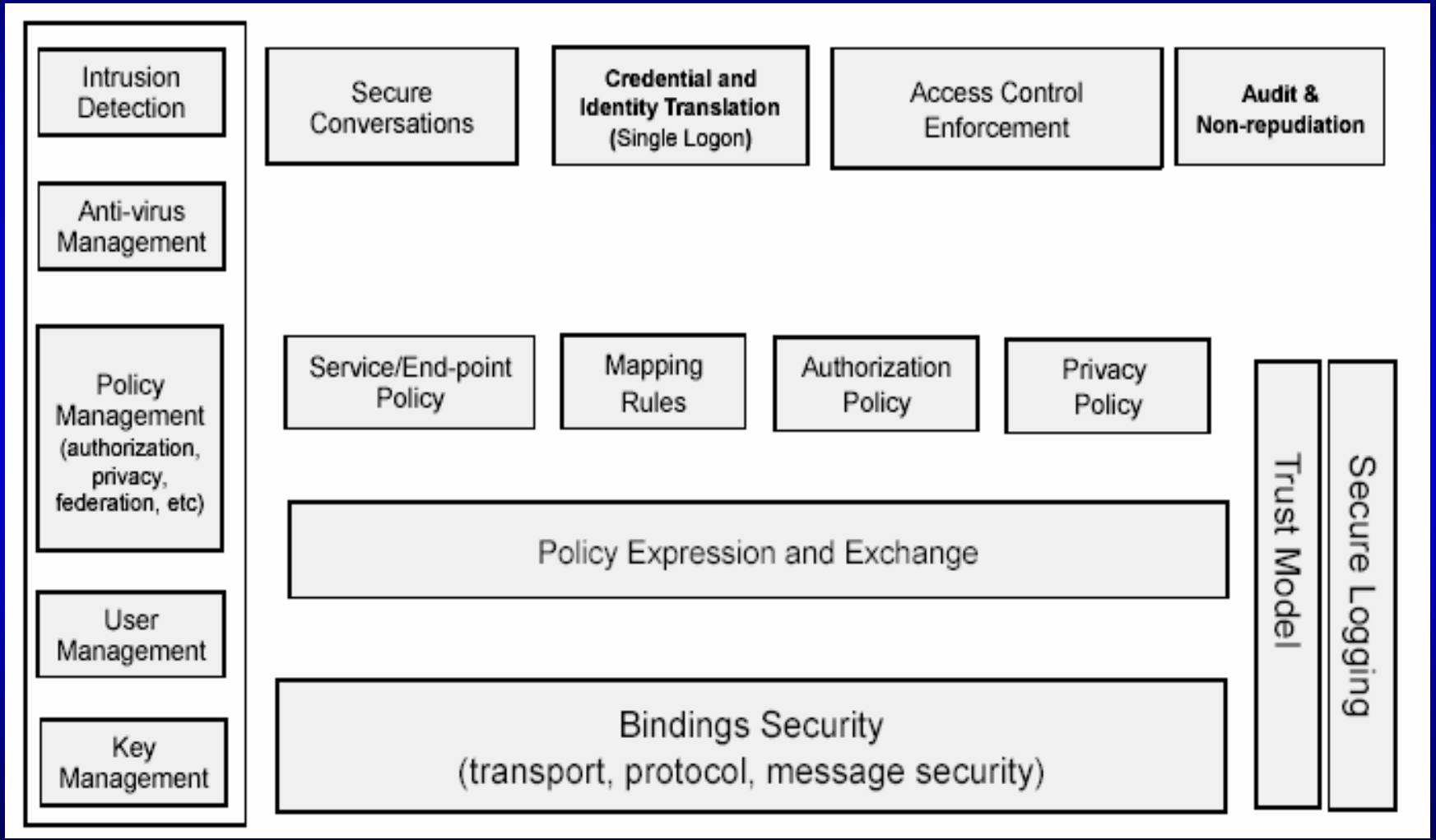
- Innovative grid computing services: E- transactions, M-commerce, telemedicine, and digital government, all demand high security and privacy protection

- Basic Security Requirements:
  - Confidentiality of exchanges – make sure that nobody can listen in.
  - Authentication – Certify the identities of all parties involved
  - Data Integrity - assurance that data is not tampered on its journey
  - Non-repudiation of transactions – assure agreements are legally binding

# Grid Security Functionalities

- Binding Security (SOAP, and IIOP)
- Policy Expression and Exchange (XML)
- Security Association
  (IPSec, SSL, IIOP, Kerberos)
- Identity and Credential Mapping
- Authorization Enforcement
- Privacy Enforcement
- Trust Management
- Secure Logging
- Manageability of Security

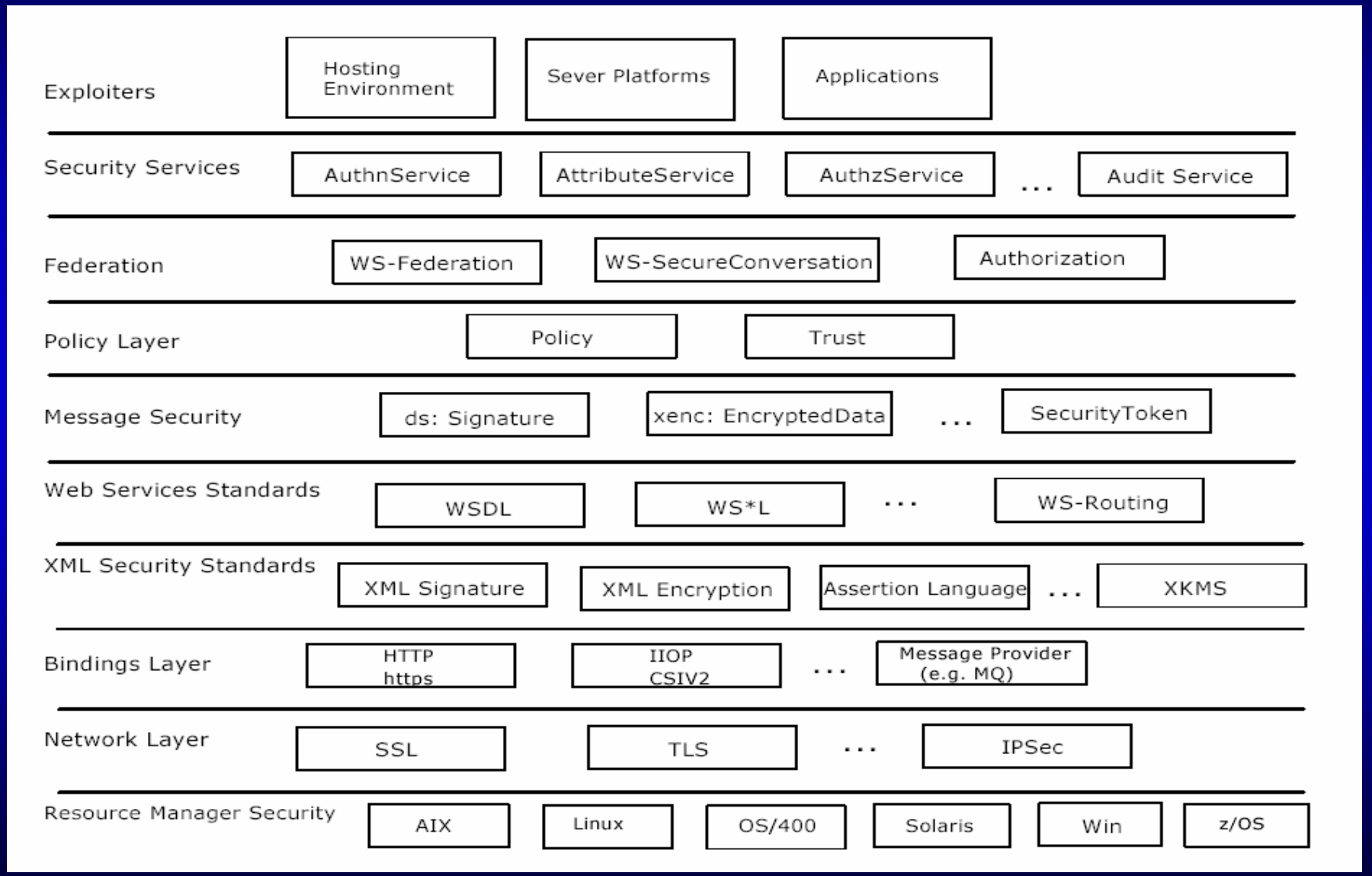
# Open Grid Service Architecture (The OGSA Security Model)



# OGSA Grid Security :

- Authentication
- Delegation
- Single Logon (Federation)
- Credential Lifespan and Renewal
- Authorization
- Privacy Protection
- Confidentiality
- Policy Exchange
- Secure Loggin
- Assurance
- Manageability
- Firewall Traversal
- Securing the OGSA Infrastructure

# OGSA Security Building Blocks



# Globus for Grid Computing

- **A software toolkit developed at Argonne Nat'l Lab and USC/ISI to promote the OGSA for Grid Computing**
  - **Offering a modular library of software tools**
  - **Enabling *incremental* development of grid-enabled tools and applications**
  - **Define and standardize grid protocols and APIs**
  - **Focus is on *inter-domain* issues, not clustering**
  - **Supports the ise of collaborative resources by spanning across multiple organizations**
  - **Integrates cleanly with intra-domain services**
  - **Creates a "collective" service layer**

# Major Globus Components

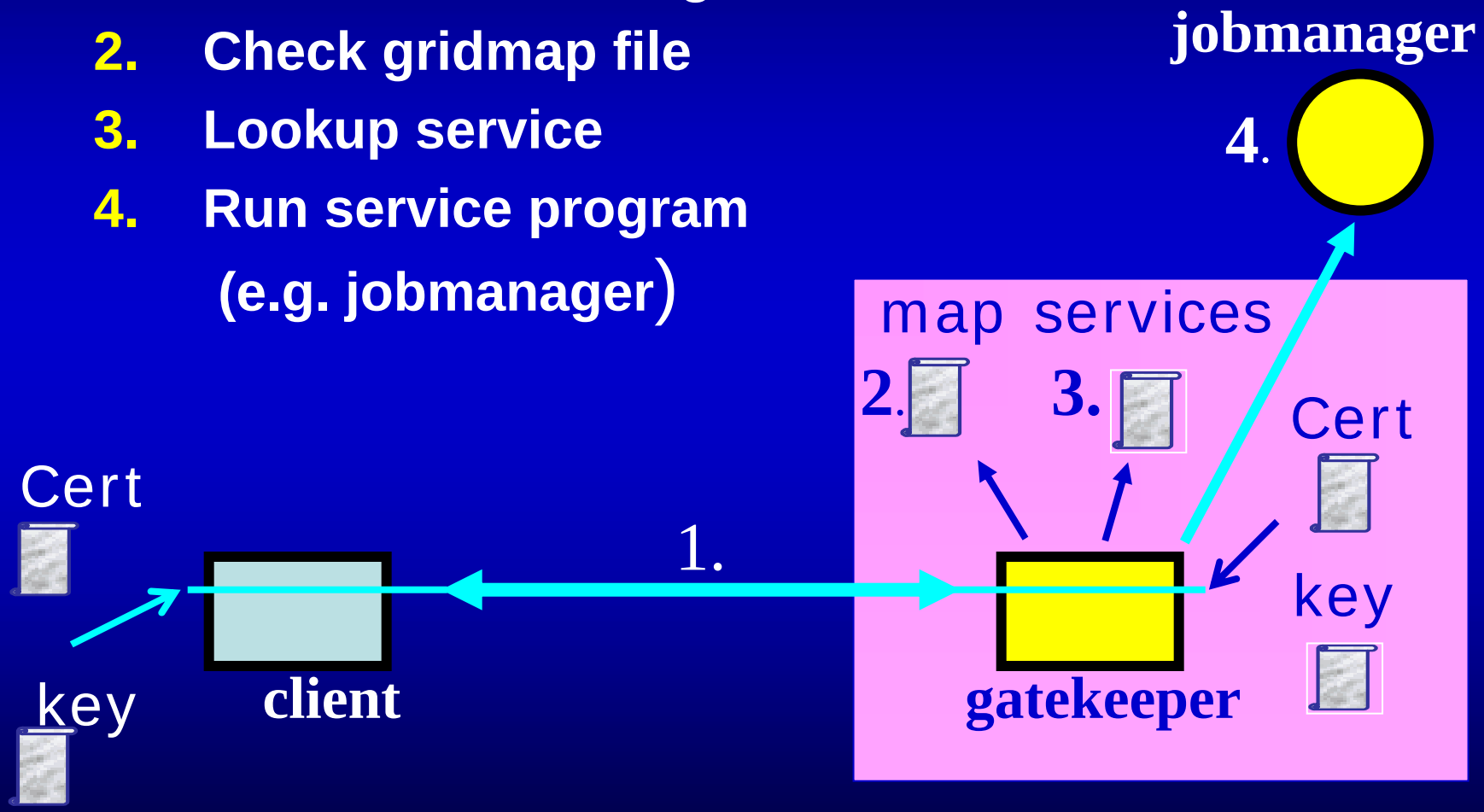
| Service Funtionality | Module Name | Functional Description |
|---|---|---|
| Resource management | GRAM | Grid Resource Access and Management (HTTP-based) |
| Communication | Nexus | Unicast and multicast communication |
| Security | GSI | Authentication and related security services |
| Information Service | MDS | Distributed access to structure and state information |
| Health and Status | HBM | Heartbeat monitoring of system components |
| Remote Data access | GASS | Grid Remote access to data |

# Globus Security Overview

- GSI extends existing Protocols & APIs
  - **Based on standards: SSL/TLS, X.509 & CA, GSS-API**
  - **Extensions for single sign-on and delegation**
- The Globus Toolkit provides:
  - **Generic Security Services API (GSS-API) on the GSI protocols**
    - **The GSS-API is the IETF standard for adding authentication, delegation, message integrity, and message confidentiality to applications.**
  - **Various tools for credential management, login/logout, etc.**

# Secure Remote Startup

1. Exchange certificates, authenticate, delegate
2. Check gridmap file
3. Lookup service
4. Run service program (e.g. jobmanager)



# Generic Security Service API

- The GSS-API is the IETF standard for adding authentication, delegation, message integrity and confidentiality to applications.
  - For secure communication between two parties over a reliable channel (e.g. TCP)
- GSS-API separates security from communication, allowing security to be easily added to existing communication code.
  - Effectively placing transformation filters on each end of the communication link
- Globus components use GSS-API to incorporate security
  - Globus Toolkit GSS-API speaks the GSI protocol

# Multisite Authentication in GSI

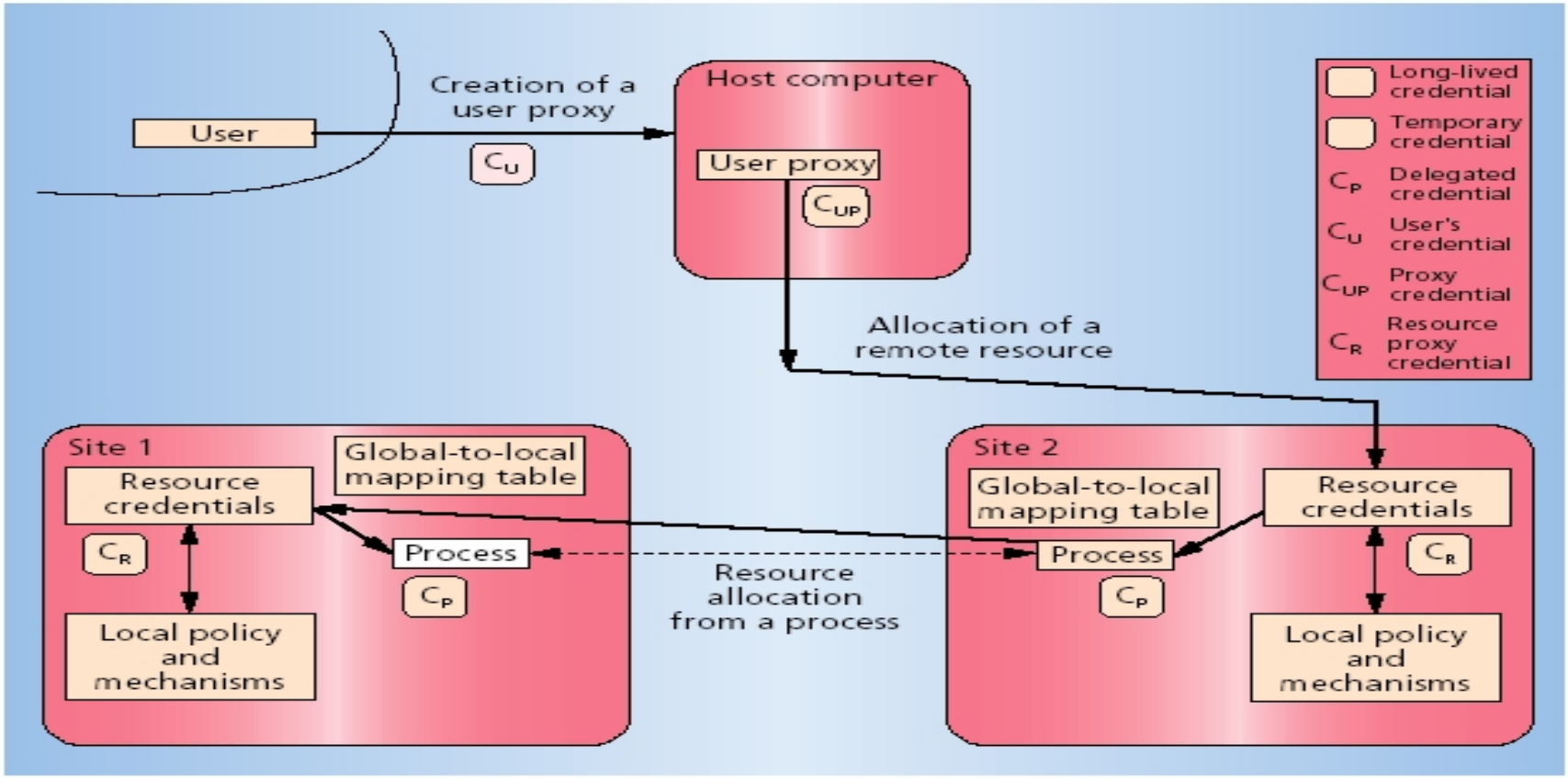
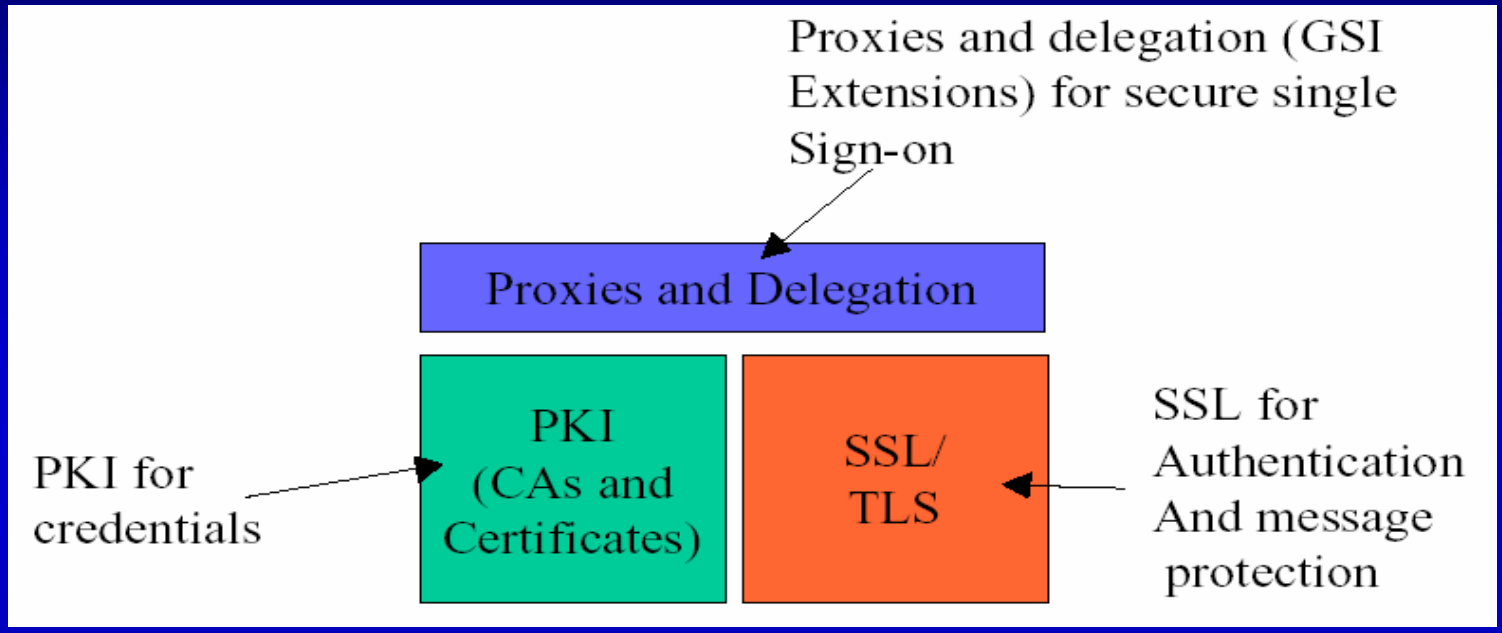



*Figure 1. Schematic showing the basic operations that GSI supports. Following the dark line from the top left-hand corner, we first see user authentication via public-key mechanisms applied to the user's credential ($C_U$), followed by creation of a temporary user proxy credential ($C_{UP}$), then subsequent requests to remote resources, represented by resource proxies holding resource proxy credentials ($C_R$), and finally authorization and global-to-local identity mapping at an individual site, resulting in the creation of a remote process at Site 2, with its own delegated credential ($C_P$). We also see how such a remote process can use its delegated credential to initiate further requests to other sites (in this case, a process creation request to Site 1) and engage in authenticated interprocess communication (the dashed line).*

# Grid Research and Security Projects at USC and ISI

- The Globus Toolkits was jointly developed by Ian Foster Argonne Nation Lab and by USC Information Science Institute (Carl Kesselman )
- Kerberos 4 was co-developed by Clifford Neuman. His group at ISI has extended the package to Kerberos 5 and various APIs for access authorization
- Recently, an Internet and Wireless Security Lab was established by Kai Hwang to develop a WPKI and RADAR security testbed on USC main campus

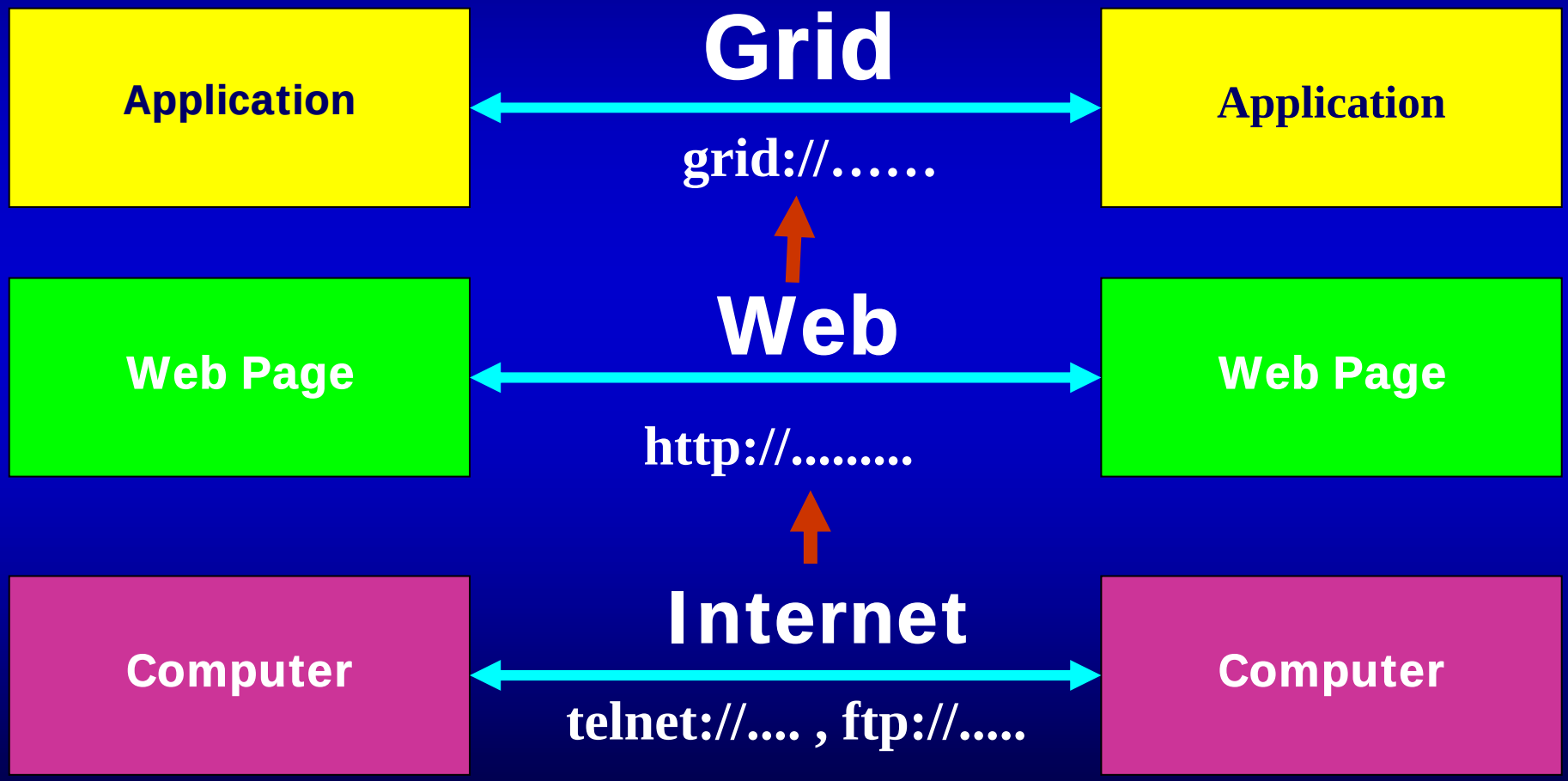
# Local vs. Global Grid Security Solutions



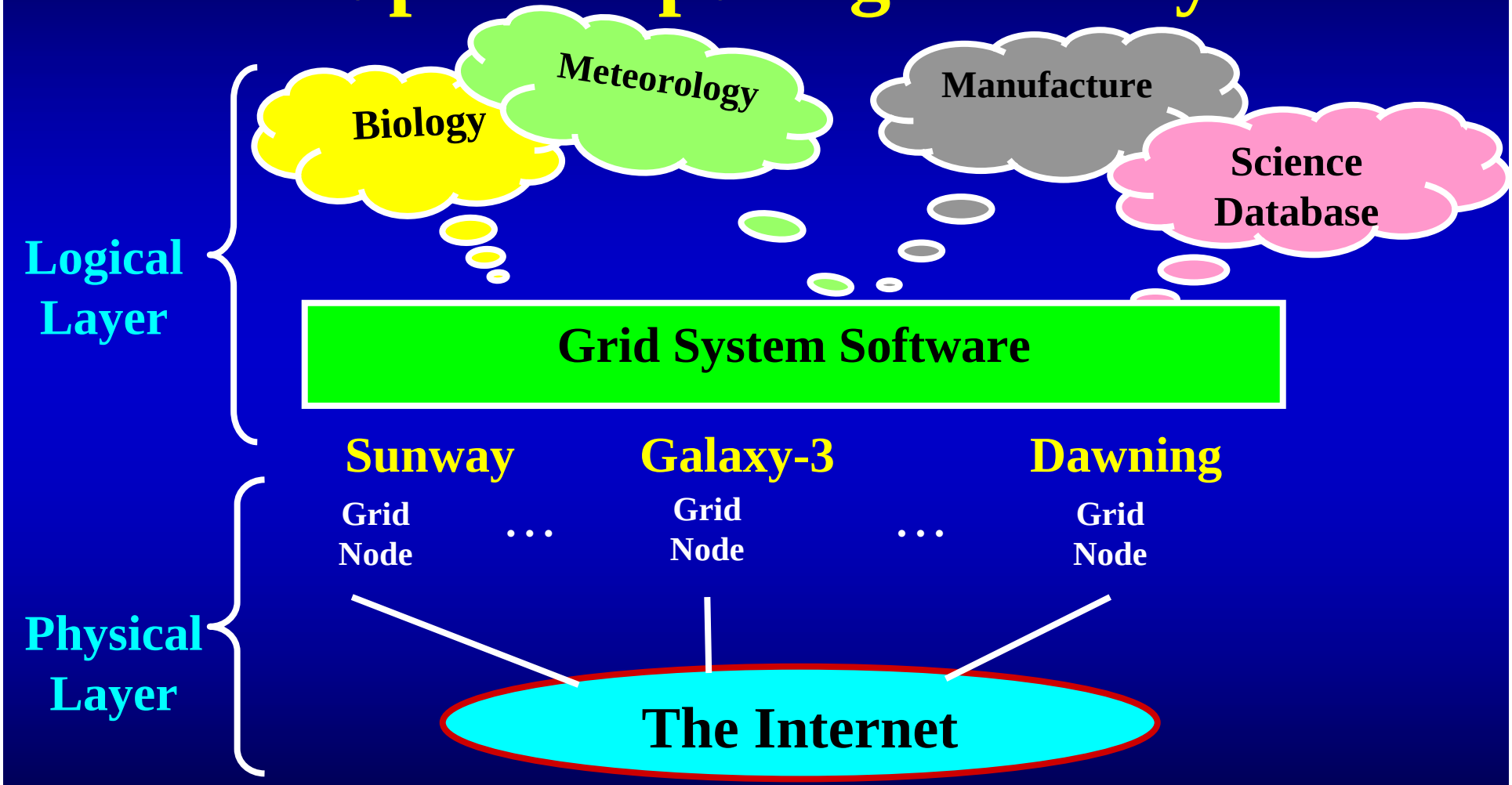

- Localized security solutions are easier to deploy, if the grid is not exposed to the general public
- National or global grid security is very difficult to enforce, unless multi-national effort works under a trust-based security system.

# Network Evolutional Path

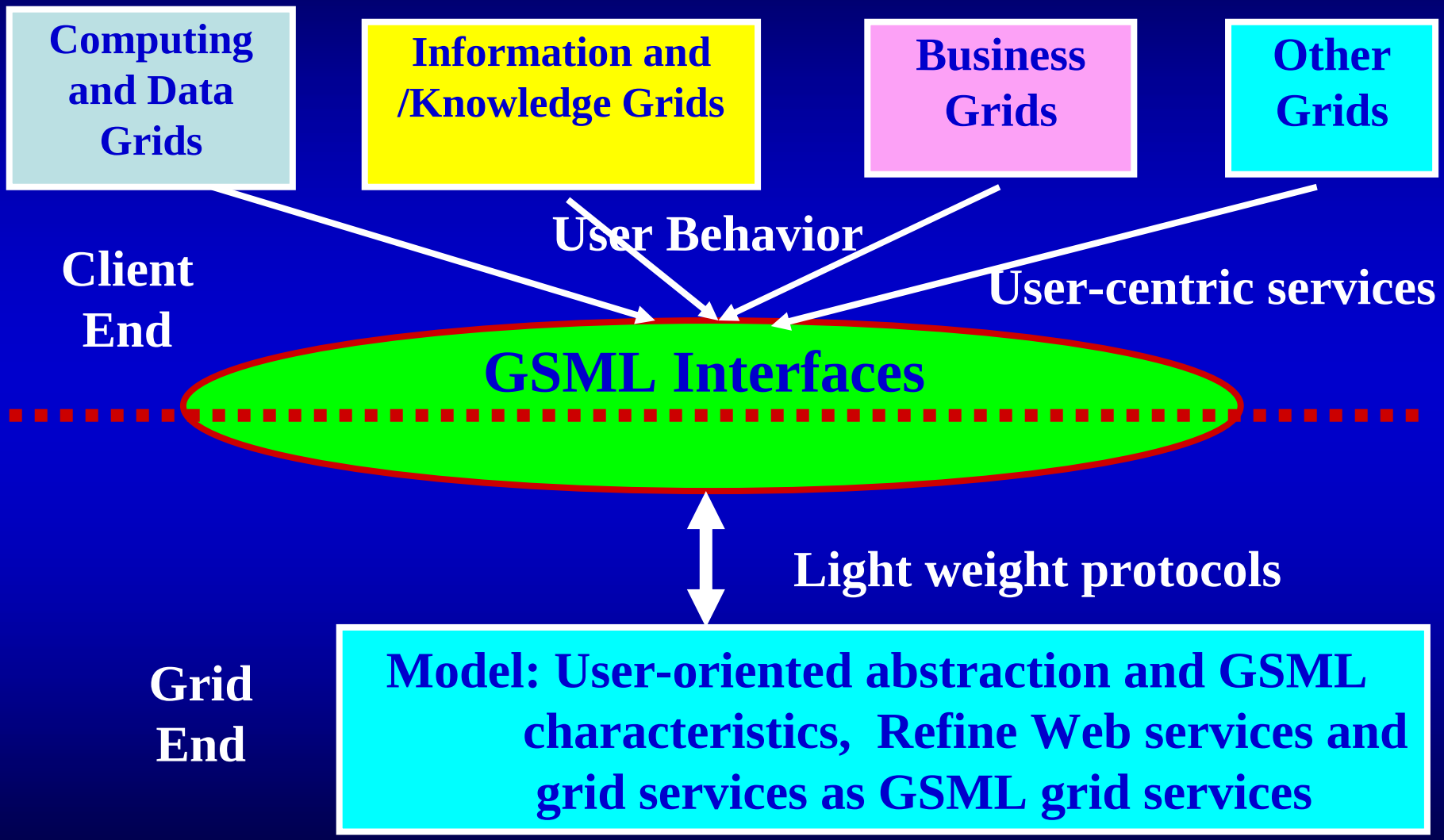
## to Eliminate Resource Islands (Dr. Zhiwei Xu, 2002)



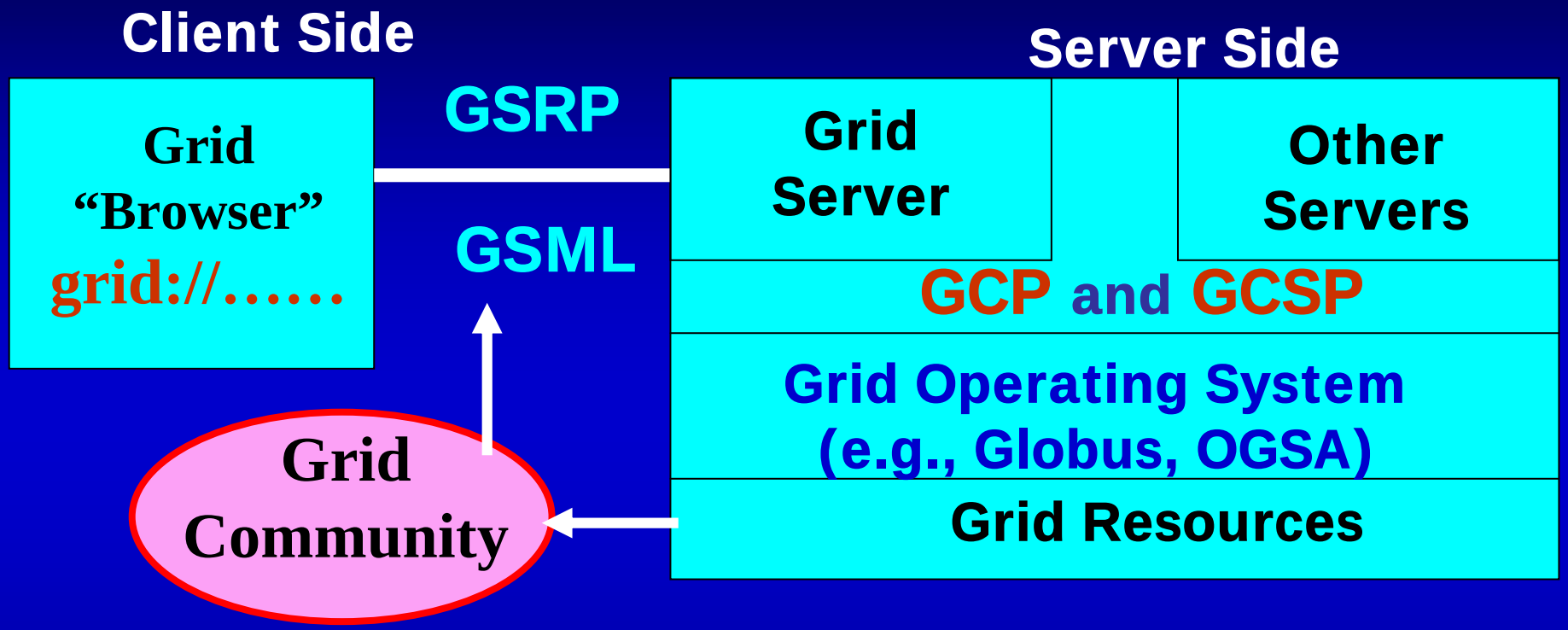
# China's Vega Grid for Scientific Supercomputing Initially



# Grid Service Model in Vega



# Major Advances in Vega Project




**GSML :** Grid Service Markup Language
**GSRP :** Grid Service Request Protocol
**GCP :** Grid Computing Protocol
**GCSP :** Grid Common Service Platform

# Expected Innovations in Vega Grid

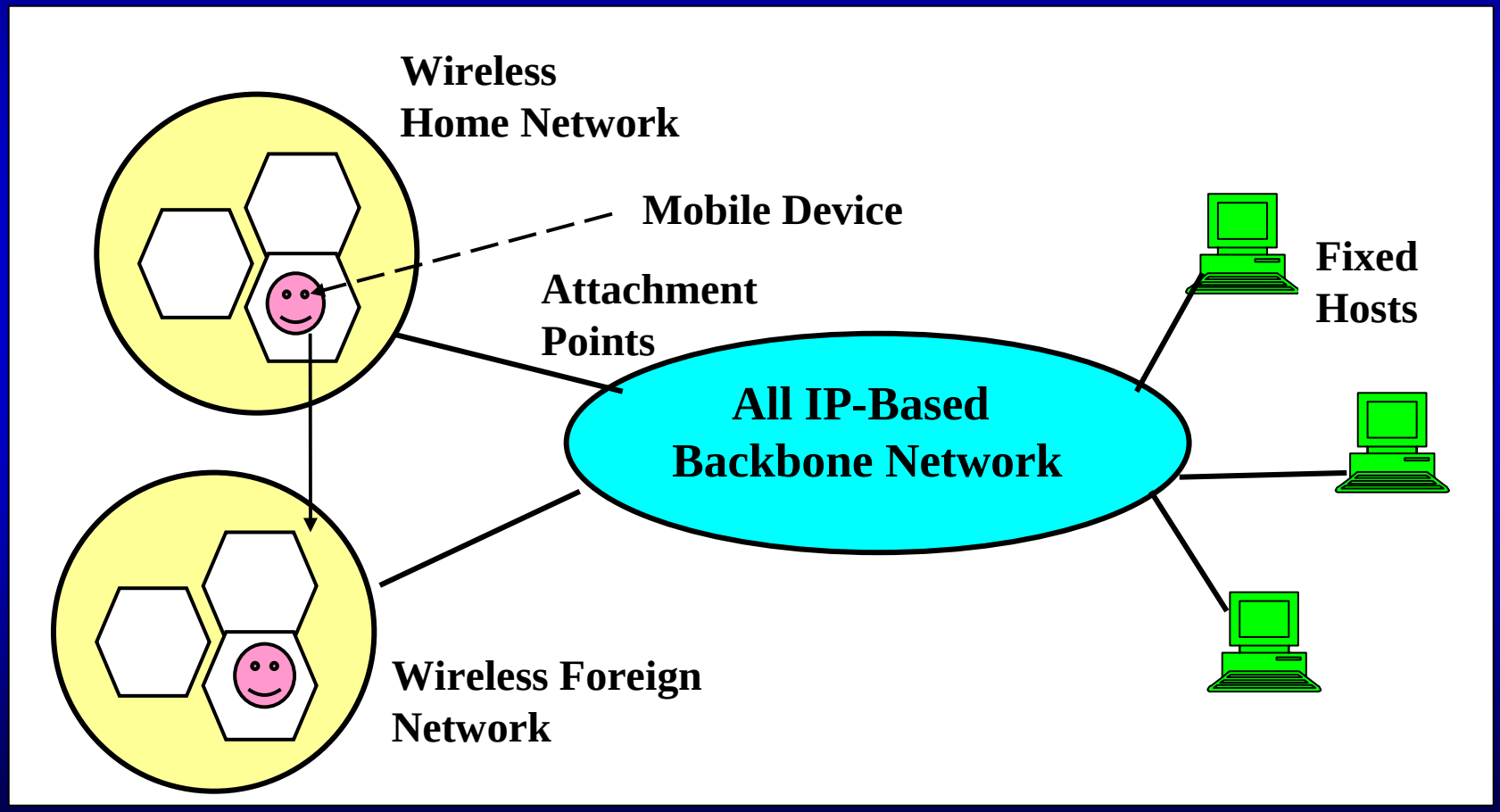
- Leverage on Dawning superserver cluster and storage server technology
- Vega-GFS: A grid document system
- Grid browsers and Grid servers
- GSML: Grid Service Markup Language
- GSRP : Grid Service Request Protocol
- Grid Service Routers and Monitors
- Vega-Miner : Grid datamining tools
- Resources Allocation and Routing
- Traversal Control and Dynamic Resources

# Grid Security Research Frontiers

## : A Call for Globalization from USC

1. Mobile IPv6 and WTLS for wireless Internet accessed by hybrid 3G/4G mobile telecom systems and wireless LANs
2. Architectural optimization of Wireless PKI and Interoperability with wired PKI for grid security
3. XML (eXtensible Markup Language) for PKI-based security, dynamic policy update, and key management
4. Digital Rights Management (DRM) for protecting intellectual property rights in digital media contents over the Internet download services
5. The RADAR system at USC for automated intrusion detection and response with minimized risks to clusters, Intranets, and grid resources in cooperative applications

# Research Thrust 1 : Developing Mobile IPv6 and WTLS Protocols for Security in Hybrid Wireless and All IP-Based Networks



# Security Features in IPv6

- Support five security Standards published by IETF
  - RFC 1825 - Security architecture for the IPv6
  - RFC 1826 - IP Authentication Header
  - RFC 1827 - IP Encapsulating Security Payload (ESP)
  - RFC 1828 – IP Authentication using keyed MD5
  - RFC 1829 - The ESP DES-CBC Transform
- IP security association and authentication are combined to transmit IP packets
- IPv6 offers options for future expansion in Mobile IPv6 for authentication, data integrity, and confidentiality. Some progress has already made in asymmetric key agreement (AKA) and lightweight handshaking for mutual authentication and confidentiality control.

# Research Thrust 2 : Extending Wired PKI to Wireless PKI through Infrastructure Enhancement

WPKI Protocol: WMLSCrypt, WPKI Certificate Format: ECC
WPKI Cryptographic Algorithm: ECC, Certificate Status: OCSP

PKI

Optimizing

WPKI

Enhancing

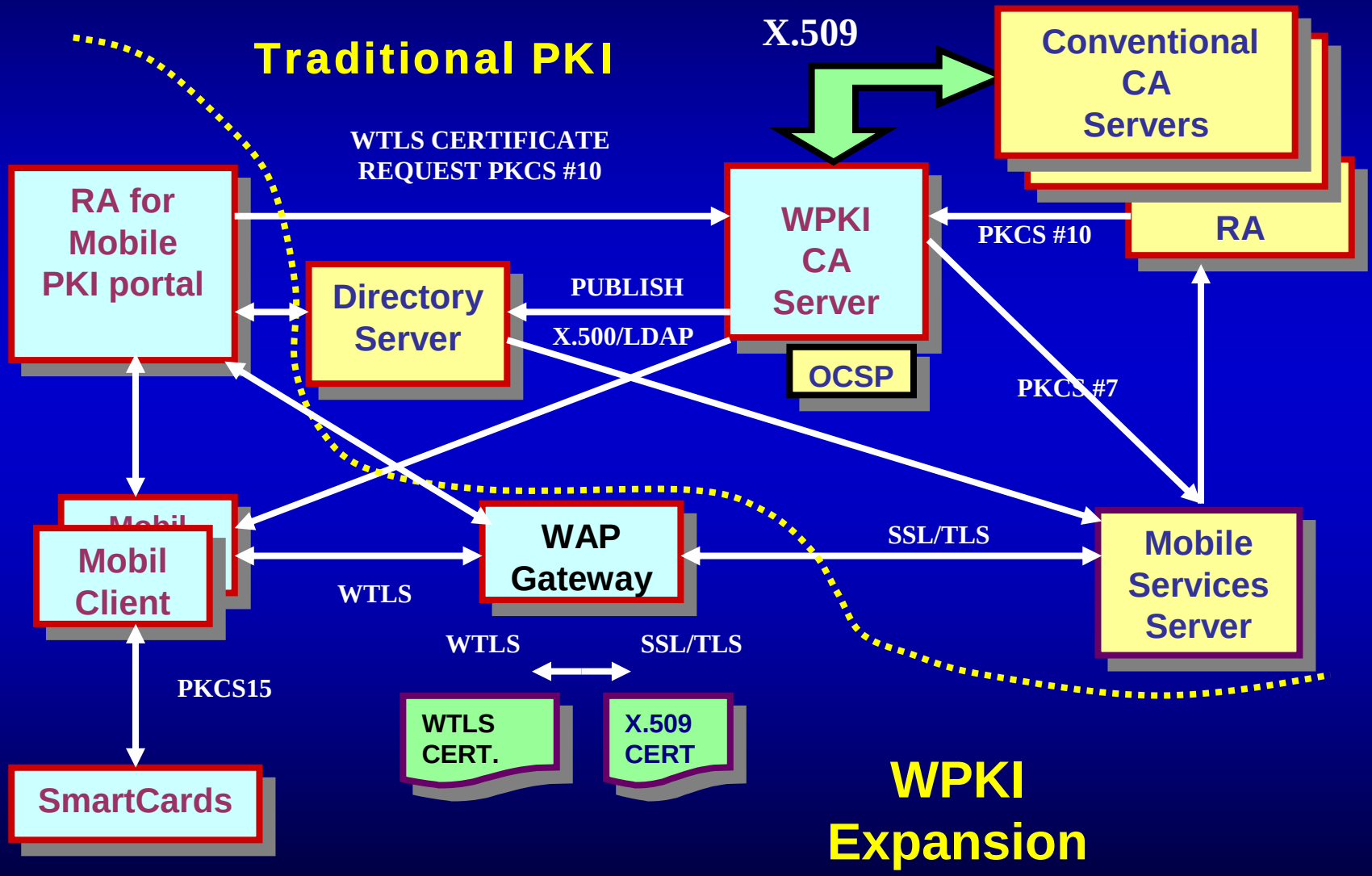
Limitation of Mobile Environment:

- Less CPU Power and Memory
- Low Battery Power, Small Display
- Limited Network Bandwidth
- High air loss and Error Rate
- Long Transmission Delay

Enhancement Techniques :

- WPKI architectural optimization
- Universal SIM standardization
- Mobile IPv6 and WTLS extensions
- Mutual authentication schemes
- Integrity and confidentiality protection

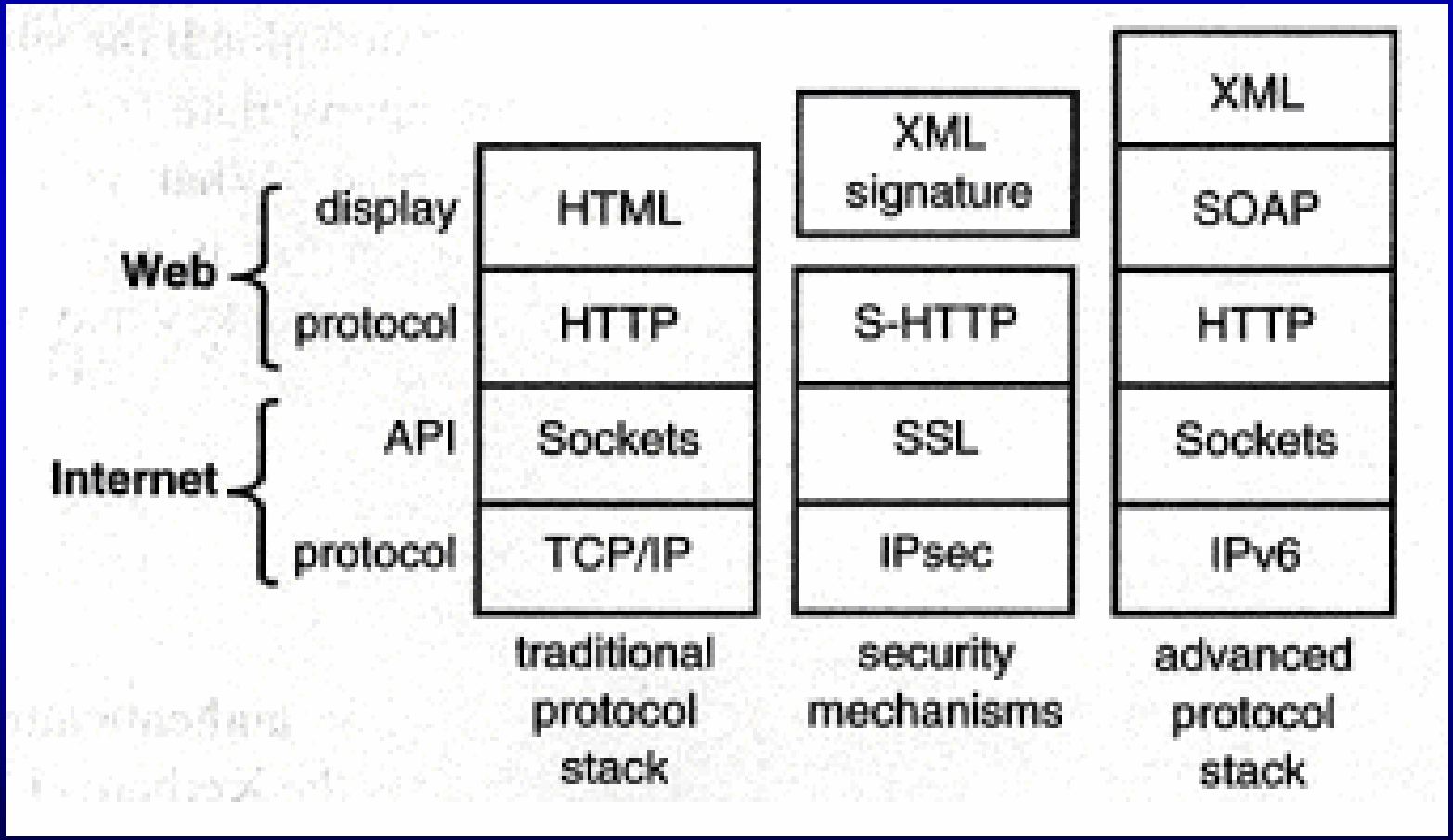
# Interoperability of WPKI with Traditional PKI



# Research Thrust 3 : XML for Internet and Grid Security

- **SOAP** (Simple Object Access Protocol) for 2-way XML communication (Request/Response)
- **WSDL** (Web Services Description Language)
- **UDDL** (Universal Description, Discovery and Integration)
- **XAML** (Transaction Authority Markup Language) for B2B
- **XML Signatures** : CA, Local RA, Certificates, Directory of Certificates, Registration of Certificates, Revocation, Short-Term Certificates, Attribute Certificates
- **XKMS** (XML Key Management Specification )
- **XACML** (XML Access Control Markup Language)
- **SAML** (Security Assertion Markup Language)

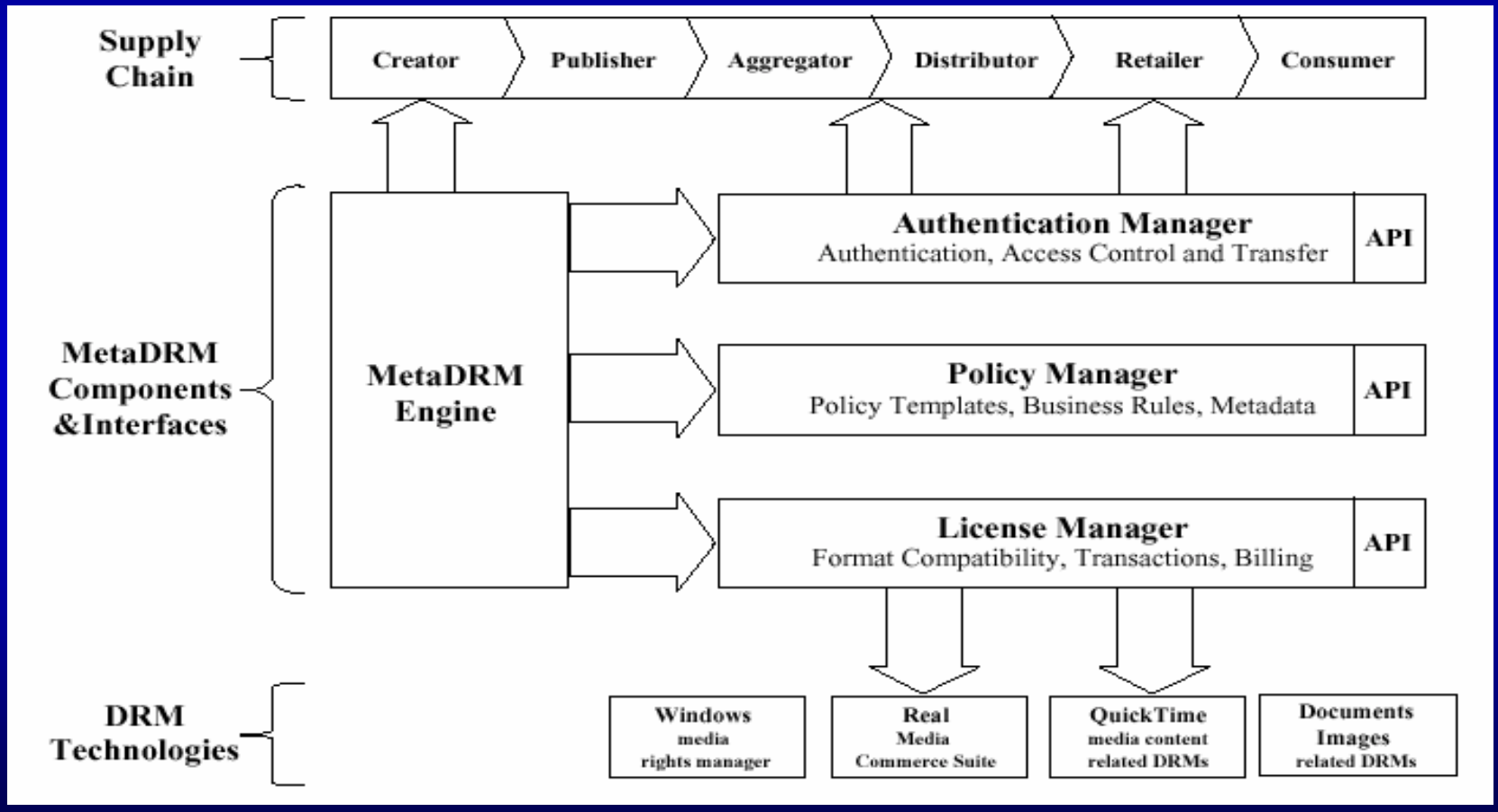
# Protocols and Security Mechanisms for Internet and Web Services



# Research Thrust 4 :Protecting Digital Contents from On-Line Piracy

- Digital Right Management (DRM) is the field for protecting digital contents (music, video, books, reports, etc.) from being stolen and reproduced (piracy) without consent from the copyright owners
- A violation example is the Napster incident by allowing people to download MP3 music files from third party sources who are not aware of the violations .
- Need DRM infrastructure at service providers, at large organizations or enterprises. Several commercial packages (MediaDRM from EnScaler, SeaChange, Microsoft Media Server, etc.) are available, but are not totally effective to cope with the problem

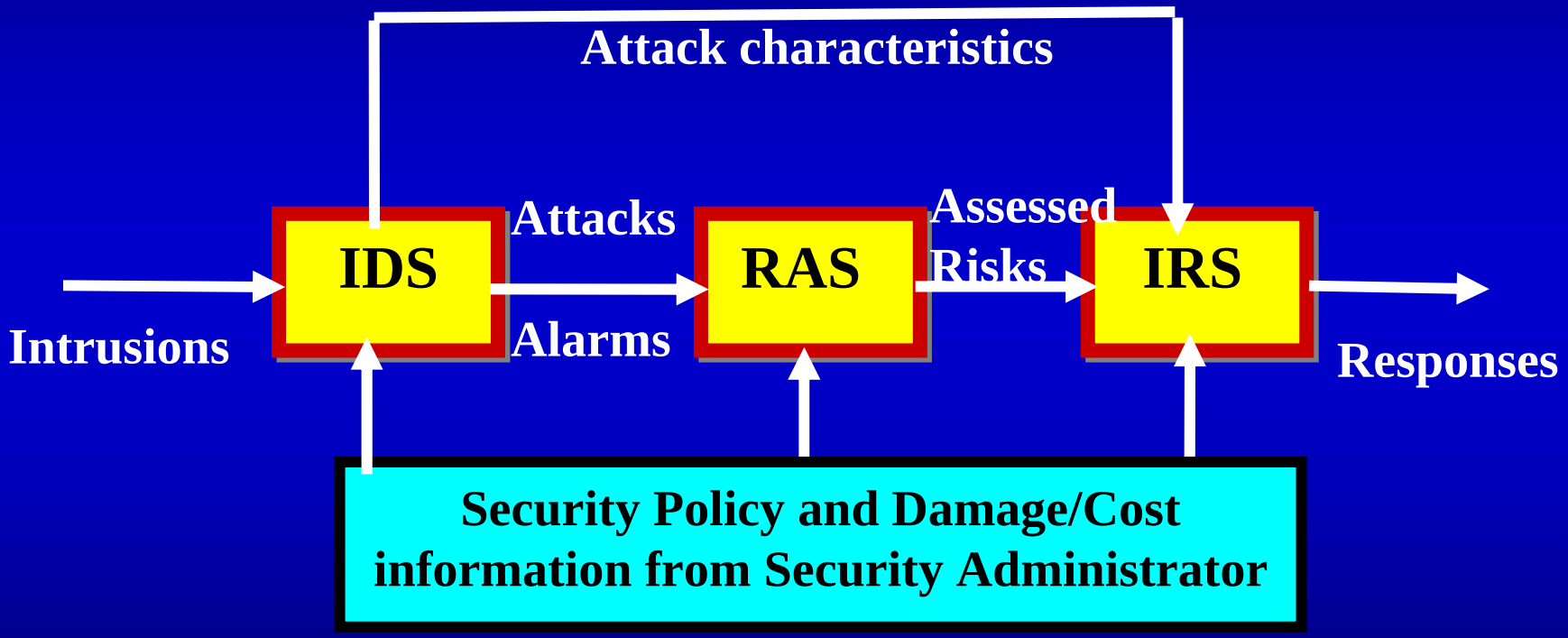
# Encryption, Authentication, Policy Management, and Licensing in The MediaDRM System from EnScaler, Inc.



# Research Thrust 5 : Securing Intranets and Grids by PKI Globalization and Automated Intrusion Response Systems

- Distributed security testbed being built at USC Internet and Wireless Security Laboratory
- XML, RMI, FTP, HTTP, SMTP, and AC are being evaluated for dynamic security updates
- Provide a full spectrum of VPN, pervasive, and grid-computing security infrastructures using the IPSec, XML, AAA, WPKI, DRM, and RADAR technologies

# The RADAR System at USC:
## Risk Assessment for Intrusion Detection with Armed Response




(IDS: intrusion detection system, RAS: risk assessment system, and IRS: intrusion response system)

# Conclusions:

- **Open grid service architecture (OGSA) specifies the grid software, protocol, and service standards**
- **Globus Toolkit opens up the real opportunities of grid applications through software deployment**
- **Grid security infrastructure (GSI), a core part of the Globus suite, awaits for linking to various PKI authorities**
- **Grid security solutions demand globalization and interoperability among various PKI authorities**
- **Very little progress being made in special networks, hardware, languages, and operating systems for grid computing**
- **No commercial grids are in place by 2002, but the Grid Service Providers (GSP) will gradually appear in the next few years**