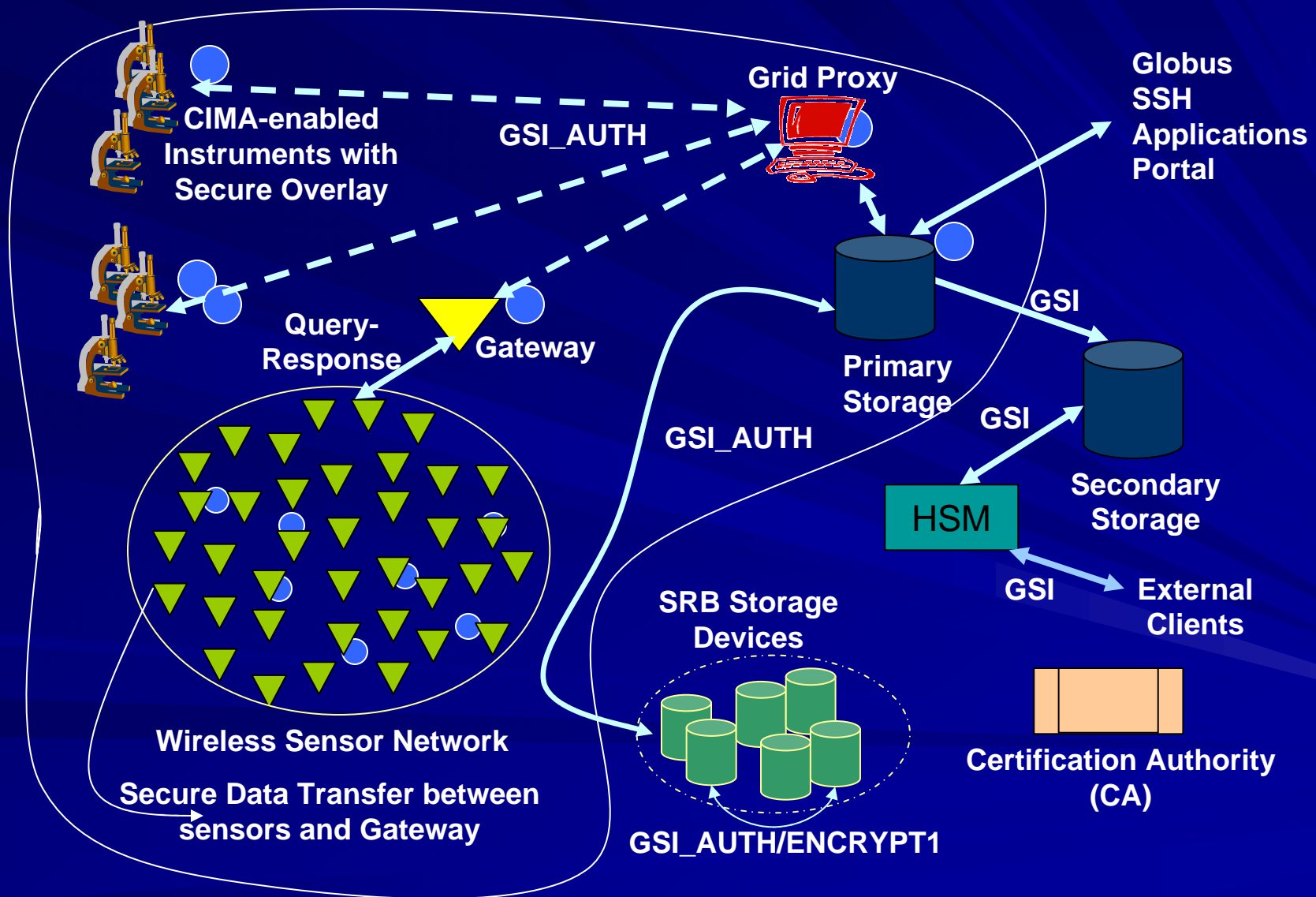# SI4: Secure data transfer facility between sensors/instruments and Grid

Chief Investigator: Dr. Asad Khan
Lead Investigator: Zubair Baig
DART Workshop on Infrastructure
April 12th, 2006
Sofitel Hotel, Melbourne

Goals

- To authenticate all data transfers on the following communication channels:
  - Sensors – grid
  - Instruments - grid
- To authorize access to sensors and instruments
- Verify data integrity for all such data transfers
- Provide data confidentiality using PKI standards supported by the GT4 Globus Security Infrastructure (GSI)

Details

Secure overlay on instruments and sensor gateways must use GSI standards:

– X.509 certificates

– Integrity check enabled by default – X.509 digital signatures

– Public key encryption option available

– Usage of state information on messages for protection against message replay attacks

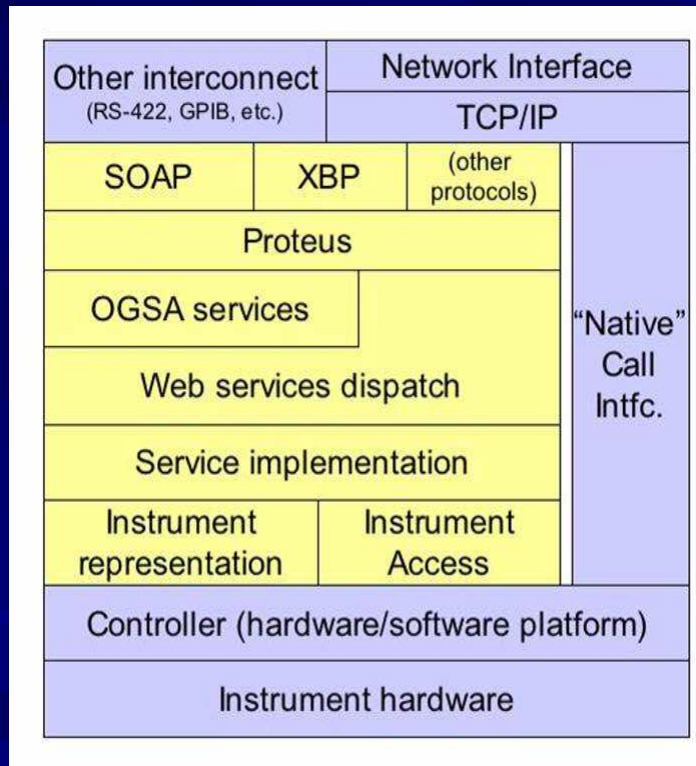   ■ NTP for time synchronization - LAN accuracy = 200us

GSI Security Infrastructure

	Message-level Security w/X.509 Credentials	Message-level Security w/Usernames and Passwords	Transport-level Security w/X.509 Credentials
Authorization	SAML and grid-mapfile	grid-mapfile	SAML and grid-mapfile
Delegation	X.509 Proxy Certificates/ WS-Trust		X.509 Proxy Certificates/ WS-Trust
Authentication	X.509 End Entity Certificates	Username/ Password	X.509 End Entity Certificates
Message Protection	WS-Security WS-SecureConversation	WS-Security	TLS
Message format	SOAP	SOAP	SOAP

- Transport layer security using SSL for efficient encryption of data using symmetric keys
- Application-layer Alternatives: WS-Security and WS-SecureConversation – high overhead

Grid-enabled Instruments

CIMA on Instruments

| Other interconnect (RS-422, GPIB, etc.) | Network Interface |
| | TCP/IP |

SOAP | XBP | (other protocols)
Proteus
OGSA services
Web services dispatch
Service implementation
Instrument representation | Instrument Access
"Native" Call Intfc.
Controller (hardware/software platform)
Instrument hardware

Security Add-ons

- GSI Authentication

- SSH for long-lived connections

- Security Assertion Markup Language (SAML)

- Shibboleth – inter-realm authentication

- IEEE 1451 standard

Note: A Gateway is essential for mapping of sensor addresses to IP for direct access of sensors by end-users of the Grid

Milestones

Meet the following security goals for the sensors/instruments to Grid communication channel:

- Data authentication
- Data integrity
- Data confidentiality
- Replay protection

Thank you for your attention!