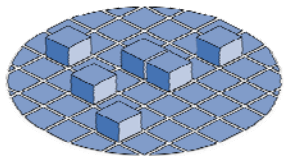
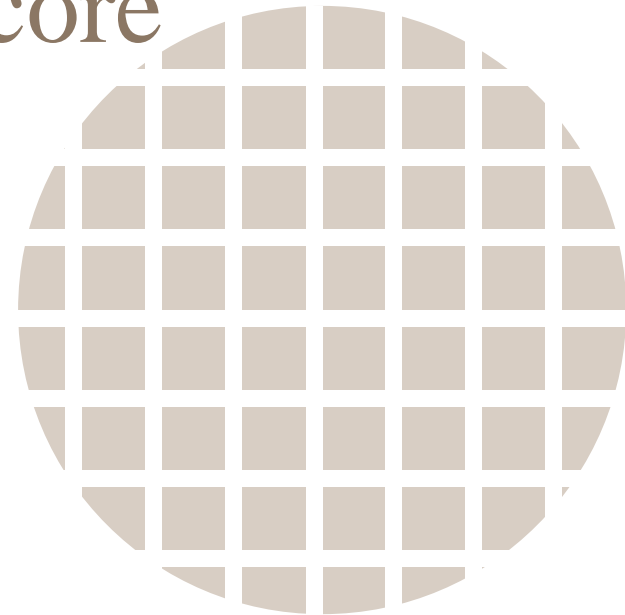


Explicit Trust Delegation: Dynamic Security in Unicore

Dr. David Snelling
Fujitsu Laboratories of Europe



UniGrids



Motivation

- Static Delegation
 - Allows Grid agents to perform specified tasks for users
 - The tasks must be defined statically
 - The user need not be contacted directly for authorization at the time the task is performed
- Dynamic Delegation
 - Grid agents create tasks dynamically on the user's behalf
 - Authorization is implicit in the Grid architecture
 - e.g. Proxy certificate infrastructure
- Traditional Unicore Supports only Static Delegation
 - No dynamic creation of tasks
 - Schedulers cannot “rewrite” resource requests
 - No support for remote portals
 - Not sufficient for WS integration in Unicore/GS

Outline

- Principles of Unicore Security
- Static Unicore Security
- Explicit Trust Delegation
- Comparison to GSI

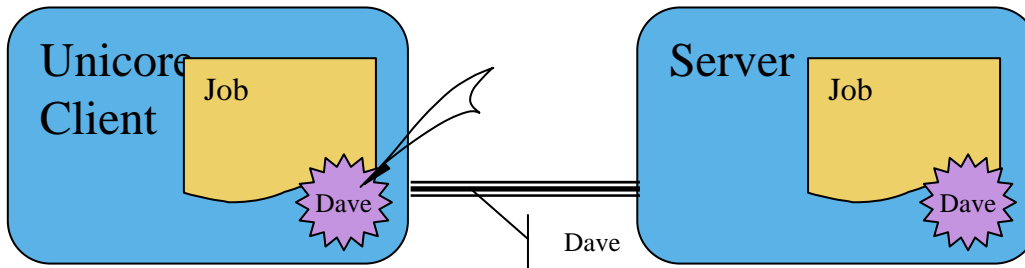
Principles of Unicore Security

- Maintain the Separation of Security Concepts
 - Authentication
 - Authorization
 - Integrity
 - Confidentiality
 - Trust Management




This talk focuses on the binding between these.

All managed independently in Unicore/GS
- Abstraction versus Dynamics
 - Use abstract concepts for tasks
 - User authorizes the abstract task (signed by user directly)
 - Incarnate abstract task into site specific rendering.
- Addresses most but not all use cases
 - Primary motivation for change was to simplify WS integration.

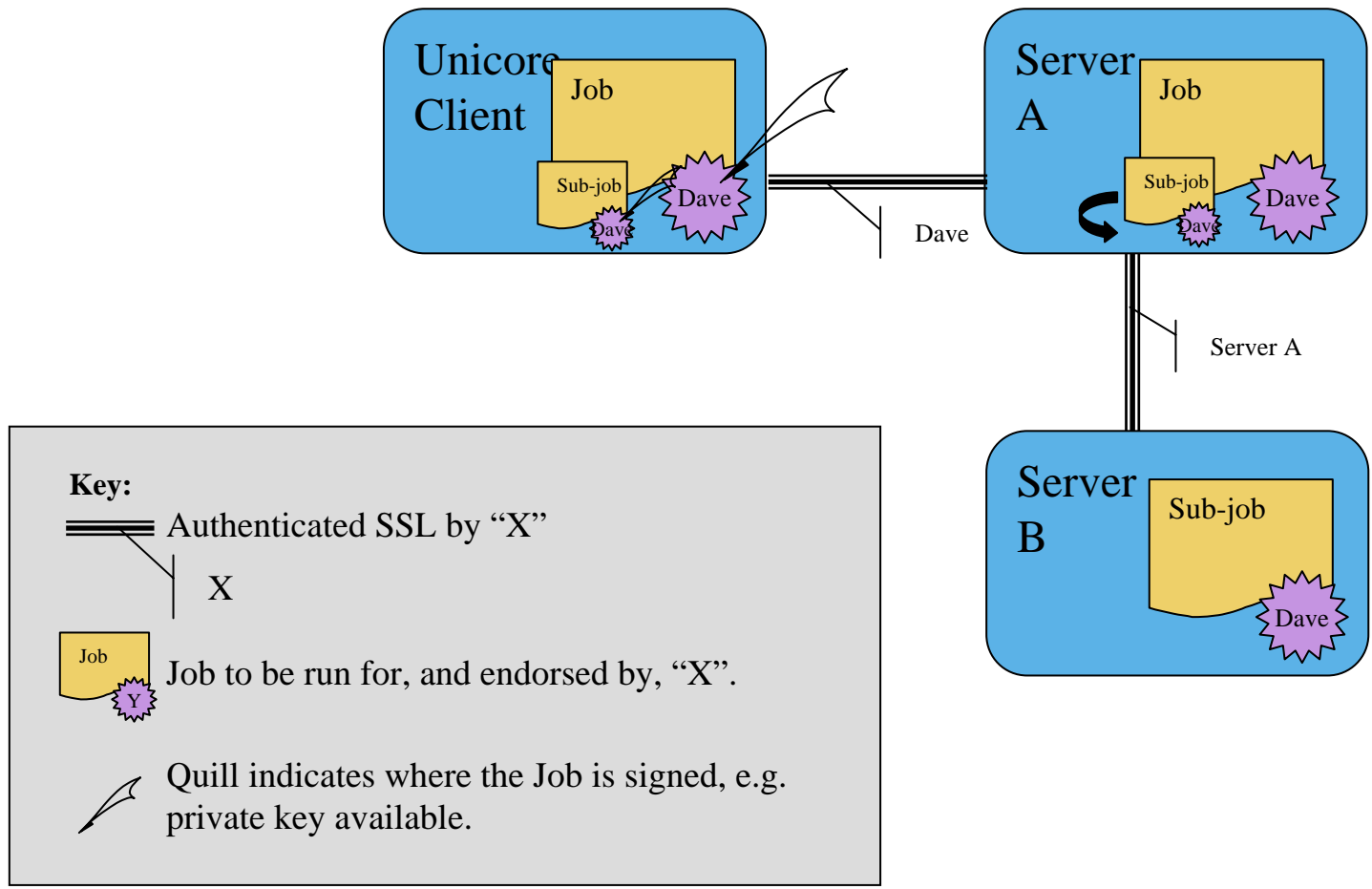
Unicore Static Security: Single-Site Job



Key:

-  Authenticated SSL by "X"
X
-  Job to be run for, and endorsed by, "X".
-  Quill indicates where the Job is signed, e.g. private key available.

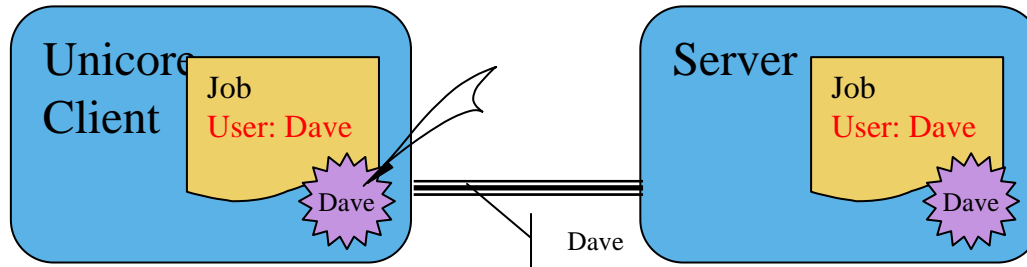
Unicore Static Security: Multi-Site Job



Explicit Trust Delegation

- Basic Principle of Delegation
 - One Grid entity (e.g. portal, scheduler, ...) signs tasks on behalf of other entities (e.g. users).
- Extend Unicore's Static approach with Explicit Trust of specific "Agents"
- Static Security Roles:
 - Consigner: The entity (client or server) that consigns a job or sub-job
 - Expressed through the identity of an authenticated SSL connection
 - Endorser: The entity (user) that authorizes the tasks to be performed
 - Expressed by signing of serialized task descriptions.
- Extension to Include User role for dynamic delegation
 - User: The entity (user) on who's behalf tasks will be performed.
 - "Trusted Agents" added explicitly to the authorization database
 - "Trusted Agents" allowed to endorse task descriptions on behalf of users
 - Many modes possible
 - E.g. Any consigner, Site trusted, User specified, VO Managed, ...

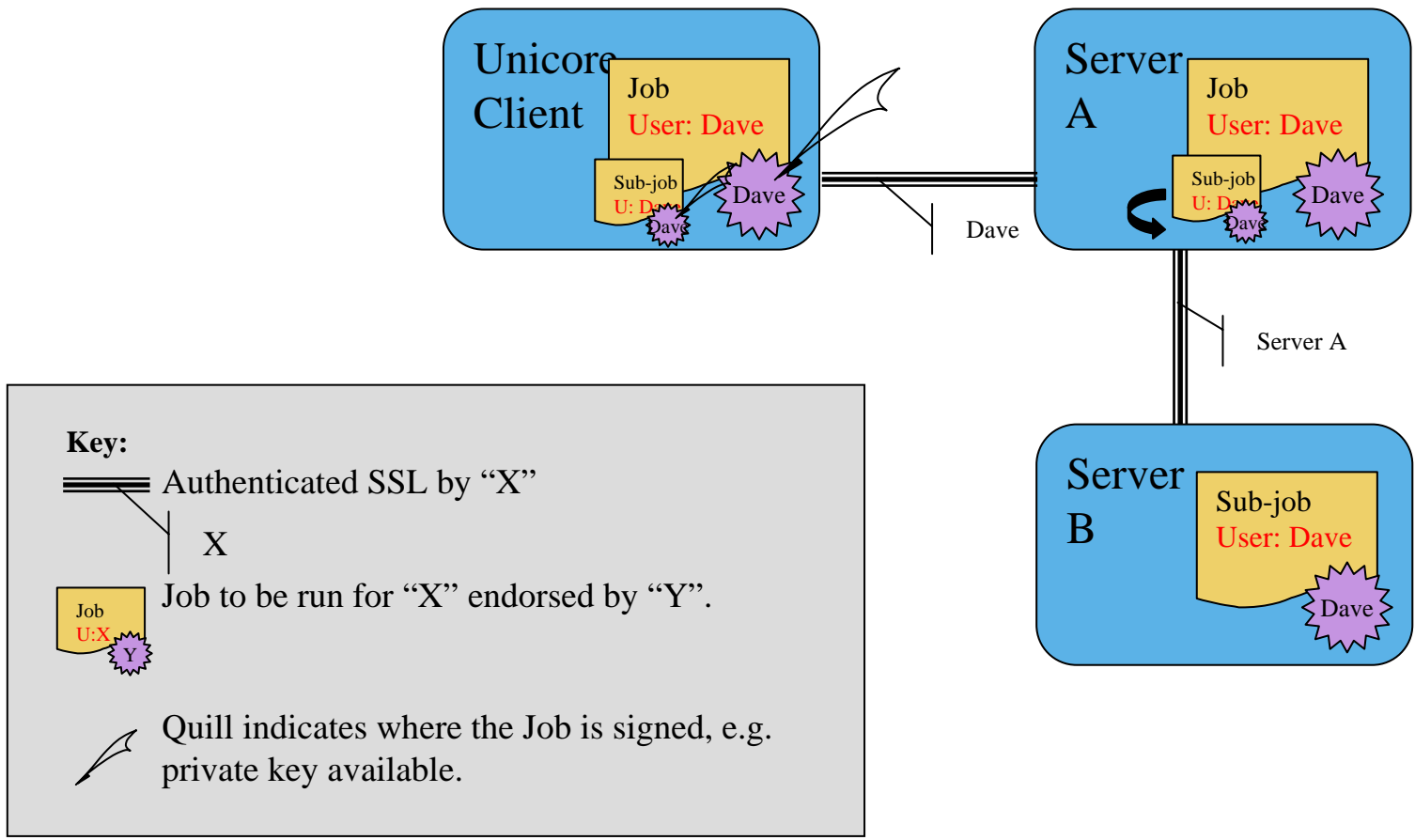
Unicore Dynamic Security: Single-Site Job



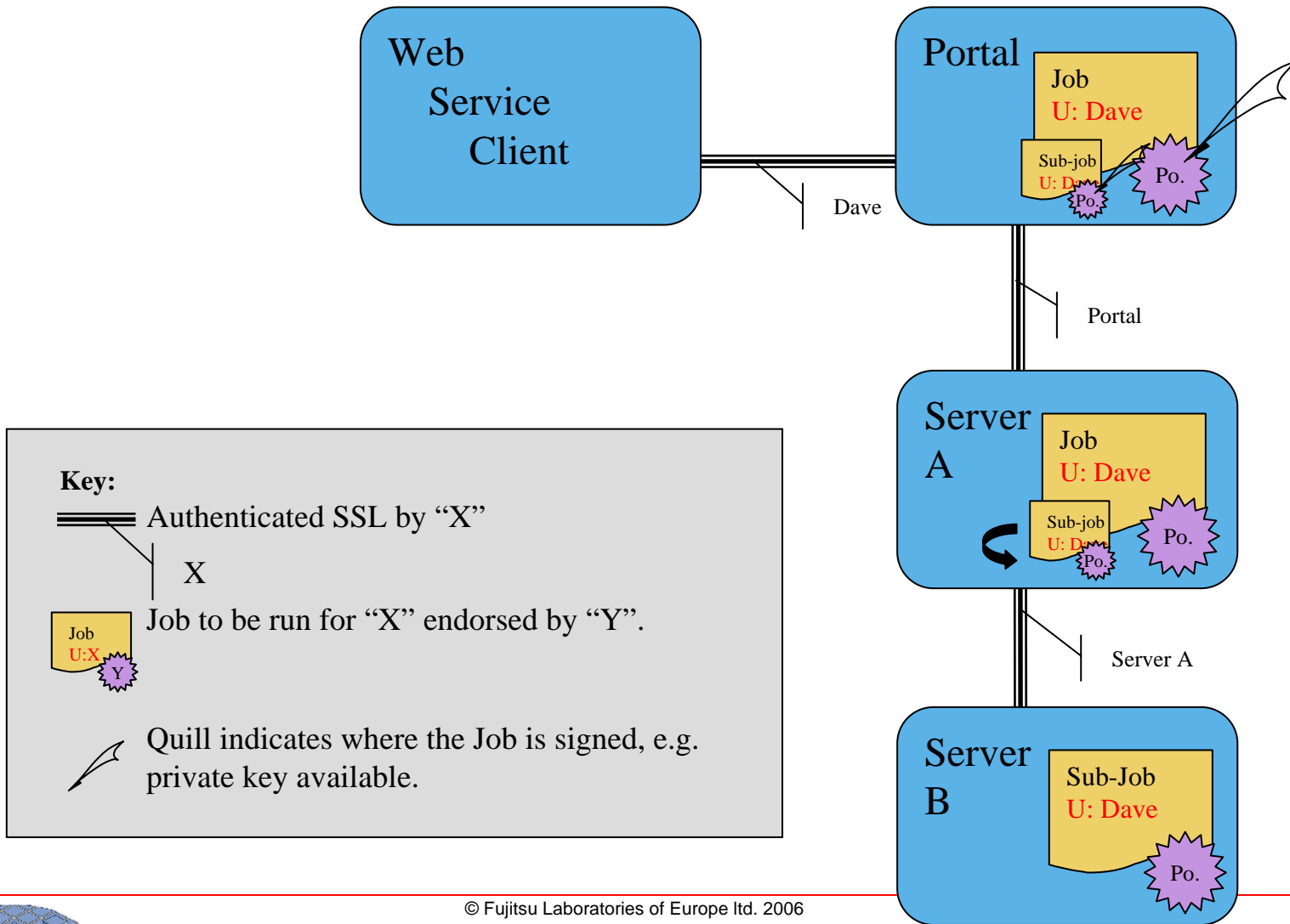
Key:

- Authenticated SSL by "X"
- X
- Job to be run for "X" endorsed by "Y".
- Quill indicates where the Job is signed, e.g. private key available.

Unicore Dynamic Security: Multi-Site Job



Multi-Site Job via a WS Portal



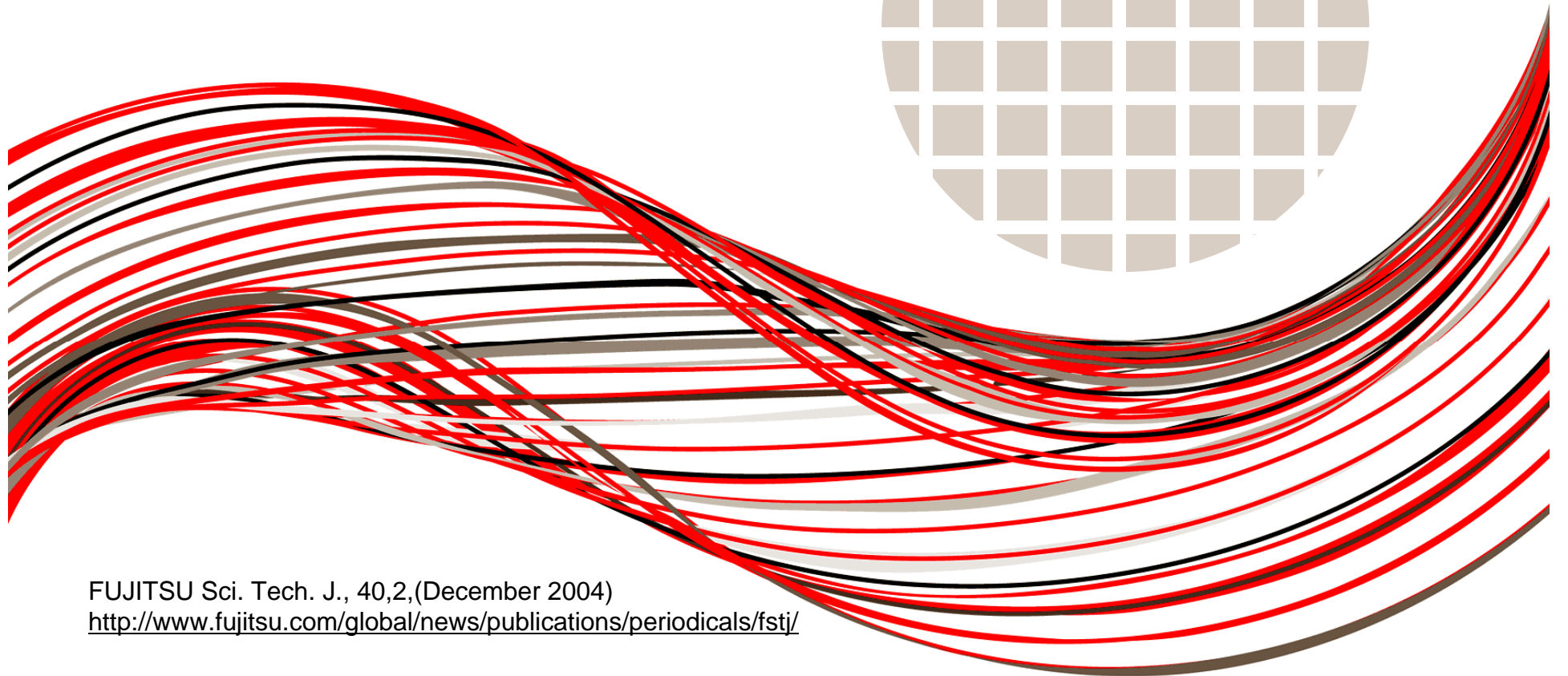
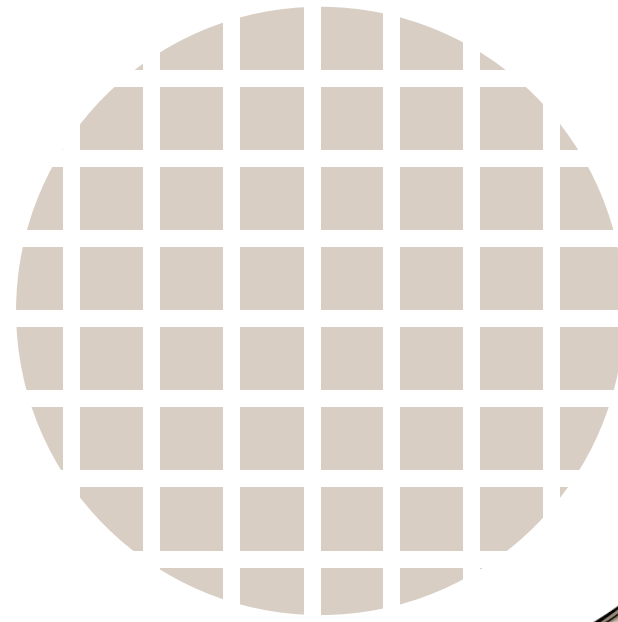
Comparison to GSI

- Fusion of Authentication and Authorization
 - X509 certificates function is extended to Authorization
 - Proposals to add restrictions to proxies make it worse
- Extension to the Standard
 - Extension to allow “user” certificates to act as CA
 - Not widely supported
- Anonymity of delegating agent
 - No audit of who actually authorized the activity
- Security Issues
 - Forces trust between all sites in the Grid
 - Unencrypted private key
 - Private key protected only by local systems mechanisms and policy
- Time Limit Issue
 - Poor support for long running tasks (12-24 hours too short)
 - Artificial sense of security (50 ms is a long time to a hacker)

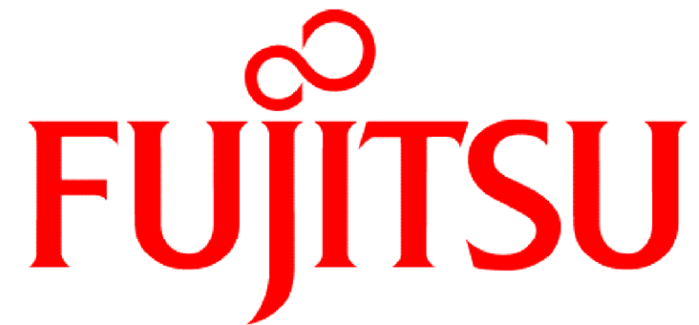


THE POSSIBILITIES ARE INFINITE

Thank you, and Questions



FUJITSU Sci. Tech. J., 40,2,(December 2004)
<http://www.fujitsu.com/global/news/publications/periodicals/fstj/>



FUJITSU

THE POSSIBILITIES ARE INFINITE

Trust Model Details

- Trust Relationships in Static Unicore
 - User trusts the sites at which they are registered
 - User trusts entities (e.g. portals) she contacts
 - Based on authenticated ssl.
 - Sites authenticate all incoming connections
 - Sites trust other sites to consign sub-jobs and retrieve outcomes of tasks.

Open Questions

- User Trust of “Trusted Agents”
 - The site trusts the agent and the user can authenticate the agent when she uses it.
 - The user can include that agent explicitly in the authorization database.
 - However, the agent could submit work on behalf a user without her knowledge.
- Include in the consign request a user-signed copy of the “Trusted Agent’s” certificate and bound in some way to the request.
 - Simple and lightweight
 - Easy to implement in Unicore, but ...
 - Adds complexity to Web Service interaction protocol.
 - It is also possible to include something like an “execute only once” signed tag enforced at the server.