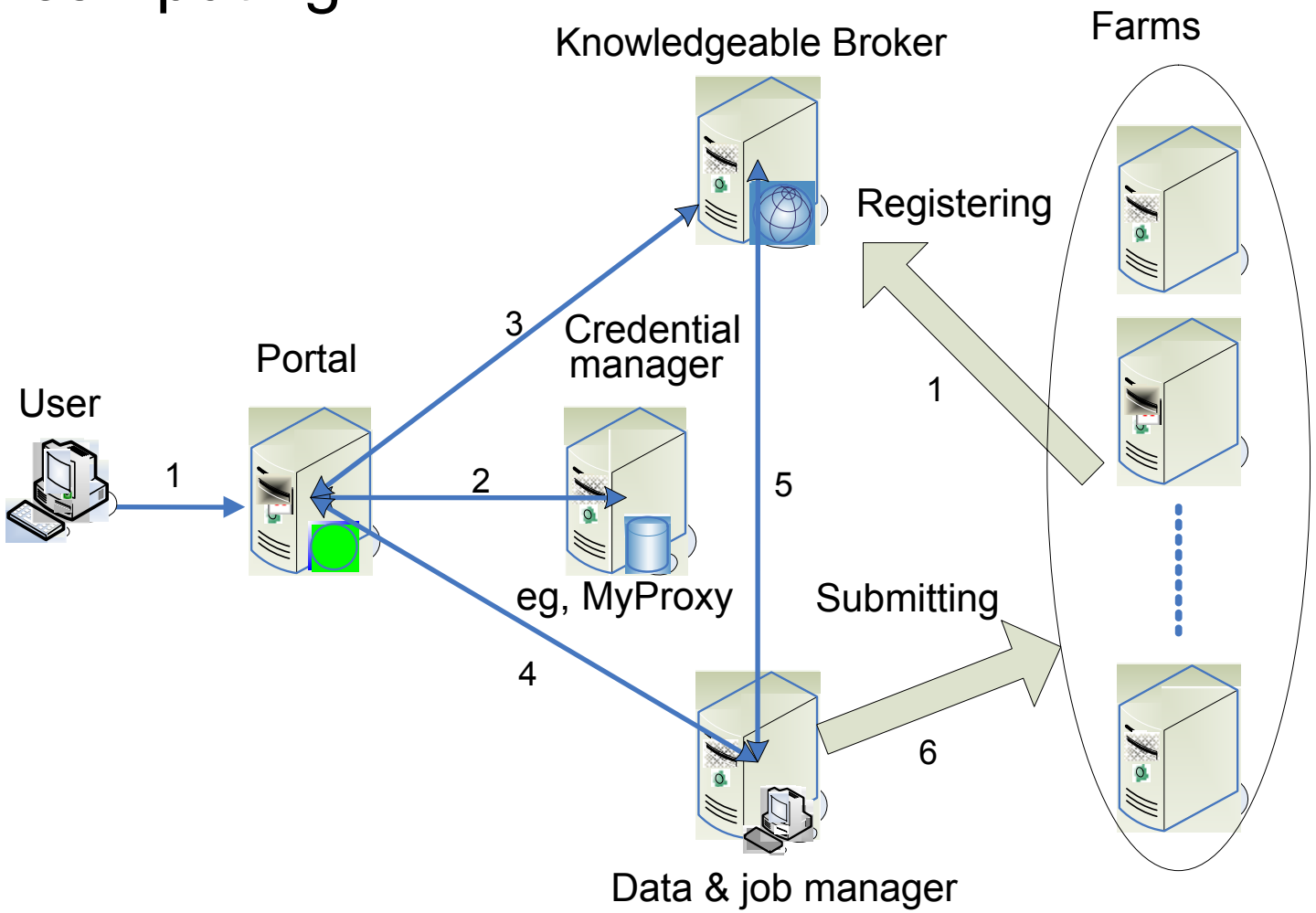
Daonity: Grid Security with Behaviour Conformity from Trusted Computing

The Daonity Team

- HP Laboratories China
- Wuhan University
- Huazhong University of Science and Technology
- Fudan University

Grid: Architected for High Dependability

A Grid Virtual Organization for high performance computing



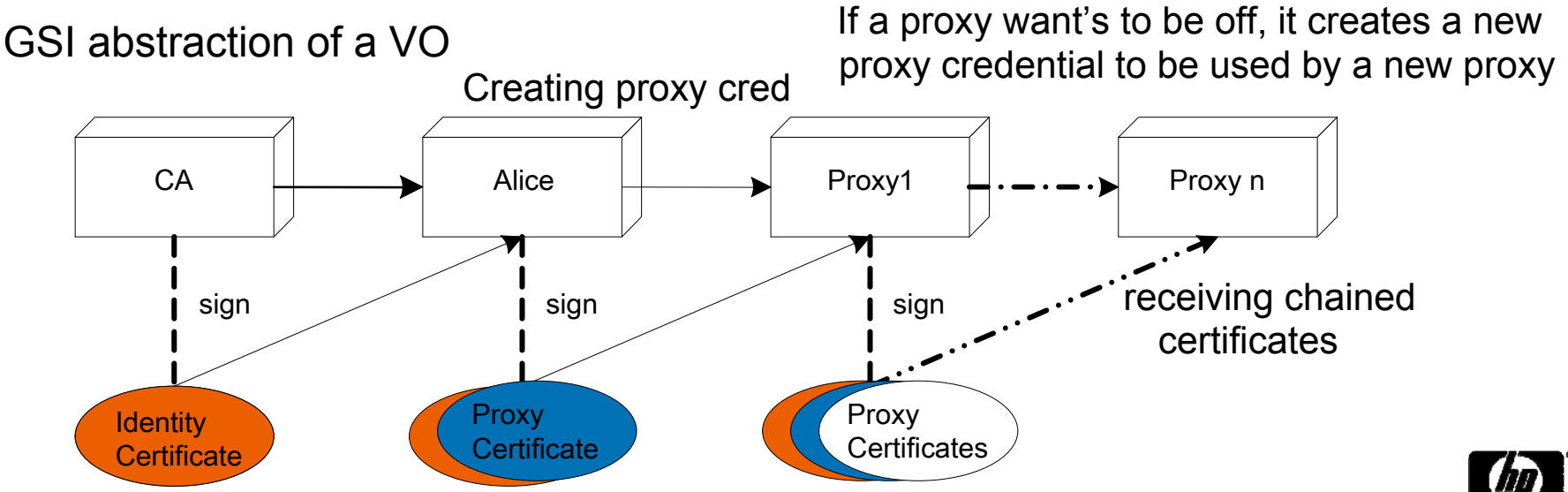
Grid Security Infrastructure (GSI) – Proxy Credentials for “Always-On-Science”

User Alice begins with creating a “Proxy Credential” and certifying its public part (then submits jobs and is off)

A “Proxy Credential” is to be used by a server (can be any servers in the preceding slide) to execute jobs on Alice’s behalf

If a broker or a farm needs to be off, it will create another proxy credential and certify its public part for a further level of delegation …

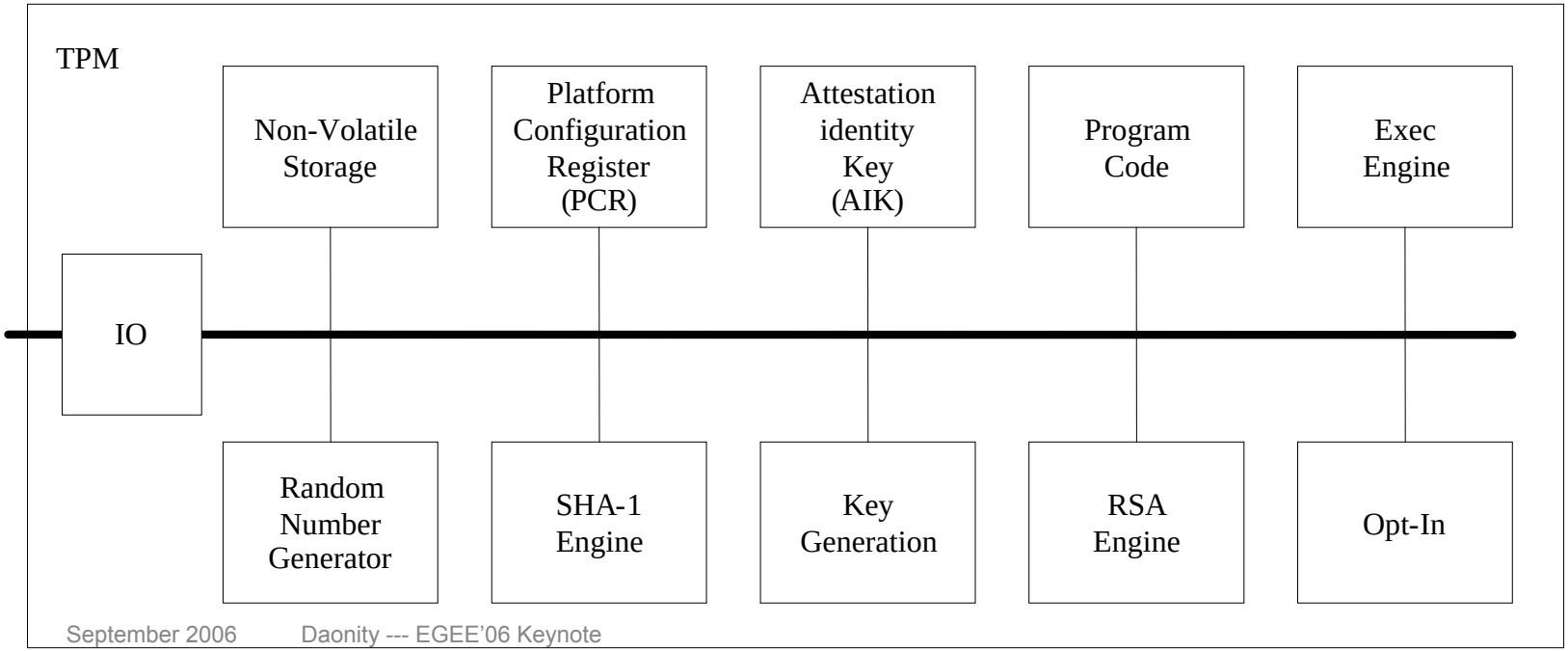
So anybody can be off, but Alice’s science is always on …



One Slide Description of Trusted Computing

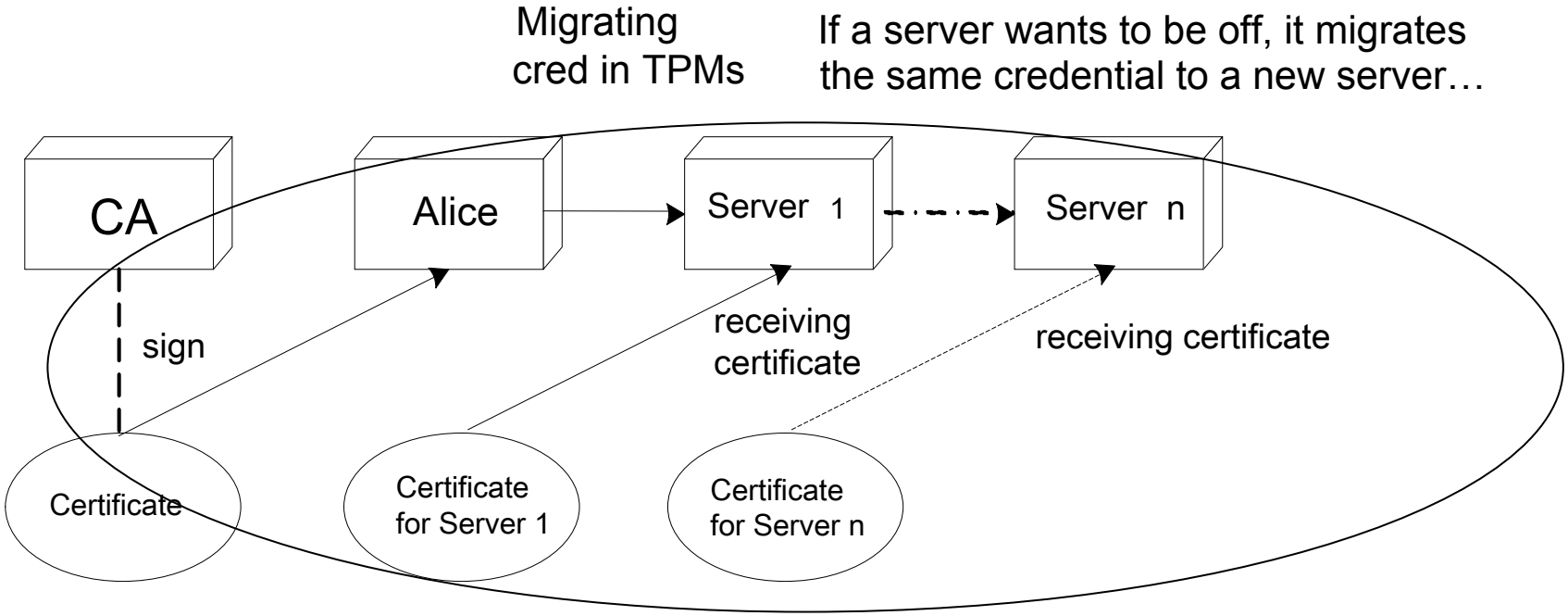
Trusted Computing Group (TCG)
www.trustedcomputinggroup.org

- Hardware based solutions to creating a Trusted Computing Base (TCB) in an open-platform computer
- Hardware: Trusted Platform Module (TPM)
- Roots of Trust for Measurement, Storage and Reporting



Same Architecture, New Realization

- Alice creates a VO credential and migrates it within TPMs of the VO members
- Behaviour conformity: a VO can satisfy given properties (e.g., distributed firewall, non-dissemination of VO data)

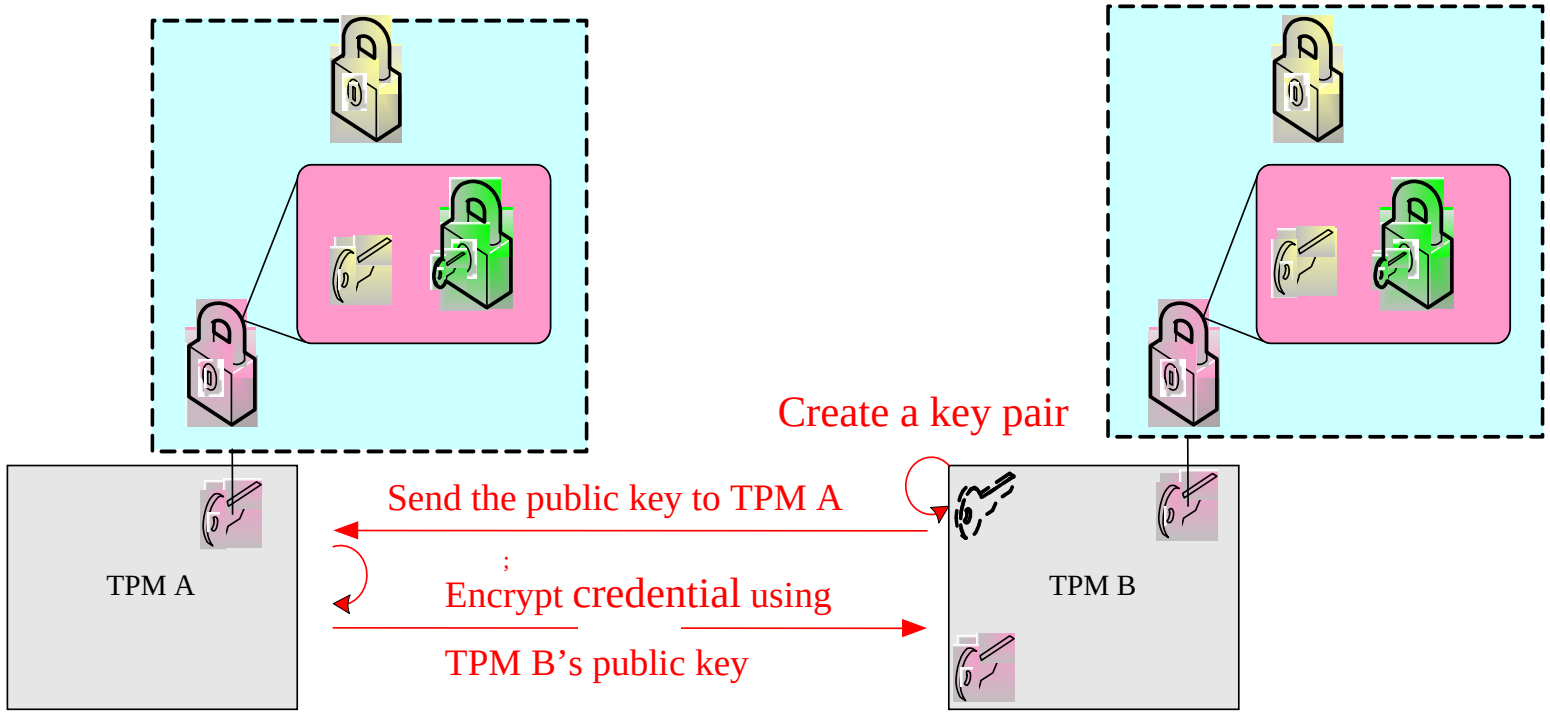


Credential Migration Know-How

A credential in a TPM can be migrated to another TPM

Separation of Roles: “TPM Owner” =/= “Credential Owner”

- a cred is owned by one who has created it IN an owned TPM
- a cred migrated TO a TPM is not owned by the owner of that TPM
- use of un-owned cred can be conditional, since TPM can act as a trusted 3rd party to enforce the usage for the credential owner



Daonity Project

- Project Goal: to improve security in Grids and SOAs using the TCG and TPM technologies
- Within Open Grid Forum (OGF) for standardization
- With ChinaGrid for software development
- Started in Aug 05; Released open-source system v.1 earlier this month (Sep 06, in GGF18)
- Led & architected by HP Labs China, R&D conducted with
  - Wuhan University (TCG technologies)
  - Huazhong University of Science and Technology (integration with Gird middleware)
  - Fudan University (secure virtualization for isolation and compartmentization)


invent