

## Position Statement on Network Security in a Collaborative Environment (‘Grid’ Security)

Neil Clarke  
Manager, Monash e-Research Centre  
15 June 2006

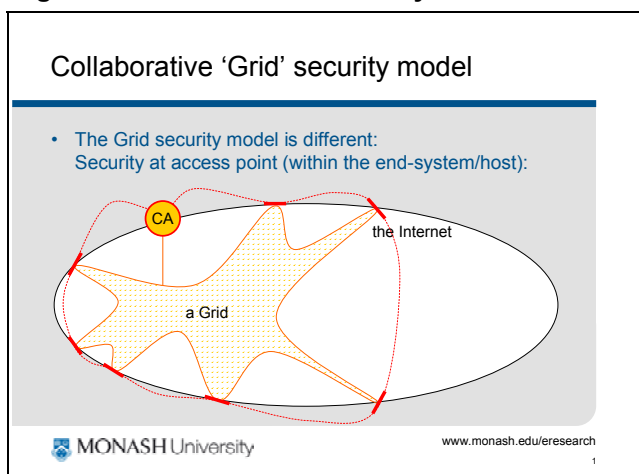
### Definition

A ‘Grid’ is a **collaborative protected virtual working environment**, constructed between **consenting authorized participants and facilities**. A ‘Grid’ is generally constructed over the public internet. A ‘Grid’ is not a physically separate network. There is in existence a multiplicity of overlapping and non-overlapping ‘Grids’. A key differentiating feature of a ‘Grid’ virtual workgroup is that it **spans organizational boundaries**, across either internal and/or external organizational units.

### Network security

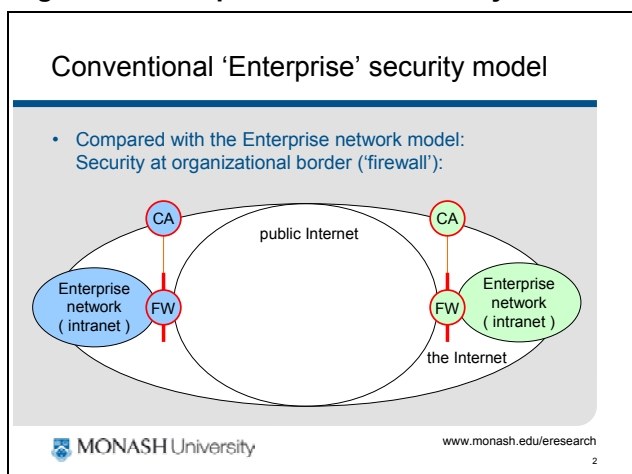
The collaborative (‘Grid’) network security model and the ‘enterprise’ network security model are fundamentally different (Figures 1 and 2).

Figure 1: ‘Grid’ network security model



*Host-based-security: Security is controlled at the access point within the end-system, host computer or application server, under the supervision of a trusted Certificate Authority (CA).*

Figure 2: ‘Enterprise’ network security model



*Border security: Institution’s network is protected by security elements at the border, and for large organizations between divisional ‘subnets’. In the case of Monash, this means between: faculties; staff and students; workstations and servers.*

*‘CA’ is interpreted broadly and is taken to include any device that hands out access rights on any basis.  
‘FW’ is interpreted broadly and is taken to include any security element.*

ITS Division operates various network security and access control elements (NSAACEs) within the Monash network (routers; ‘ACLs’; ‘firewalls’; intrusion detection, logging and response systems; ingress controls; proxy servers; application-layer gateways; etc.).

The role of these NSAACE security elements is to **enable high-speed connectivity** between the departments, faculties, campuses and other parts of the University and externally to other universities and organizations via the public internet. Under Network Infrastructure Services’ ‘Wire-Speed Everything’ (WiSE) Programme, all of the network security elements should be considered to operate at gigabit line rates.

The role of the NSAACE security elements is to **facilitate all aspects of the University’s business**, while **protecting the University** from internal and external security threats emanating from accidental and malicious

bad behaviour of other network users and systems. The security elements should not be viewed as 'blocking-agents' that interfere with the smooth operation of any aspects of the business of the University. Research collaboration is one such important aspect of the University's activities.

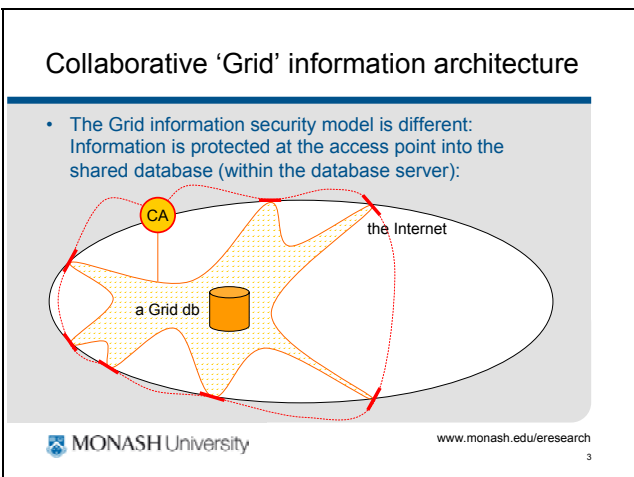
The Monash IT Security Manager, the Monash e-Research Centre Manager and the ITS Network Infrastructure Services (NIS) Manager work together to ensure that the various security elements do not impede any aspects of the University's operations. A collaborative process has been established in which these three groups work closely together to resolve any issues that arise. **Should any difficulties arise in the area of research collaboration or any communications between researchers or research systems, please contact e-Research Centre Manager (Neil Clarke) in the first instance.**

*In practice*, Figure 1 (the 'Grid' layer) is **layered** on top of Figure 2 (the underlying physical 'enterprise' infrastructure layer). Thus 'Grid' activities gain the added protection afforded by the 'enterprise' security elements.

### Information architecture

Similarly, the collaborative ('Grid') information security model and the 'enterprise' information security model are fundamentally different (Figures 3 and 4).

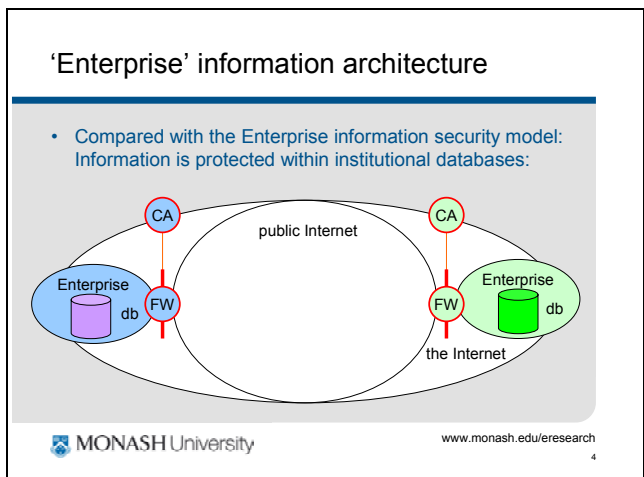
**Figure 3: 'Grid' information architecture**



*Information is held in a shared database, possibly a distributed database, that inhabits a Grid 'middle-ground' space. Information is protected at the access point/s into the shared database, under the supervision of a trusted Certificate Authority (CA).*

*'CA' is interpreted broadly and is taken to include any device that hands out access rights on any basis. 'FW' is interpreted broadly and is taken to include any security element.*

**Figure 4: 'Enterprise' information architecture**



*Information is protected by the institution that owns the data, under the supervision of the institution's Certificate Authority (CA). Responsibility and control of the information rests with the institution.*

Figure 3 introduces significant non-trivial and unresolved issues in the areas of Intellectual Property (IP) rights, copyright, information ownership, authoring, attribution, access rights, and responsibility for data integrity, protection, preservation and curation. Different jurisdictions, and even different individual contractual circumstances, take different positions on these issues. For example, Monash currently leads a major R&D activity on these topics (DART Project).

The Monash IT Security Manager and the ITS Information Management (IMSP) Director can assist researchers in these regards.

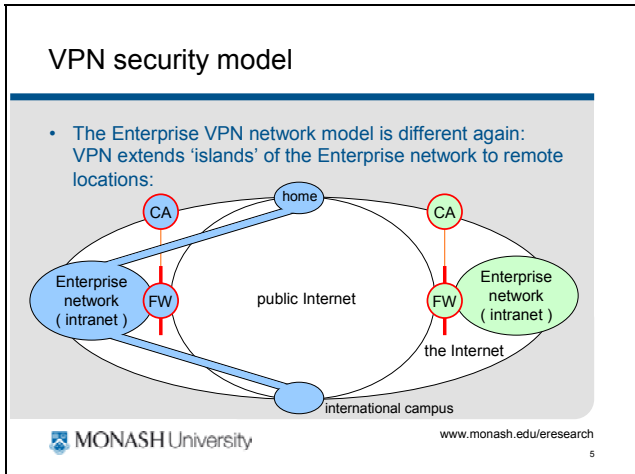
*In practice*, Figure 3 (data-base in a shared Grid 'middle-ground') is **simulated** using Figure 4 (conventional institutional repository). One (or more) host institution/s take responsibility for the data and make it available to others on a basis agreed between the contributors.

## Virtual Private Network

The term 'Virtual Private Network (VPN)' has been used to mean a variety of different things. In the broadest sense of the term, a Grid is a type of VPN. However, by common current usage convention, the term VPN normally refers to what is technically referred to as an 'Enterprise VPN'.

The Enterprise VPN model (Figure 5) is quite different from either the Grid (Figure 1) or Enterprise (Figure 2) network architectures.

**Figure 5: 'Enterprise' VPN network model**



VPN 'gateways' construct isolated 'tunnels' through the internet to remote 'islands'. These islands include remote campuses, people at home and people on the move. The islands become part of the Enterprise network ('intranet'). Access to the public internet from the islands is via the Enterprise network and its normal border controls (FW).

Note the asymmetry of this diagram cf Figure 1. The islands all become part of the (blue) Enterprise network. Users must be registered in the (blue) enterprise's CA. Whereas the Grid model symmetrically spans organizations, and people do not become extended members of other organizations' internal environments.

'CA' is interpreted broadly and is taken to include any device that hands out access rights on any basis. 'FW' is interpreted broadly and is taken to include any security element.

Therefore, the Grid and Enterprise VPN architectures are distinct. Whereas a Grid symmetrically **spans** organizations, a VPN joins remote users **into** an organization. A Grid does not have a central 'star' point (or hosting organization). Hence Enterprise VPN technology should not generally be considered to be suitable for implementing a Grid. An Enterprise VPN is not a Grid.

## Encryption

Whereas encryption normally comes as part of a VPN (virtually a side-effect of the way the isolating tunnel is constructed), there is not a 1-to-1 nexus between VPN and encryption. Nor is VPN-based encryption necessarily sufficient. VPN-based encryption provides protection only over the part of the path between the VPN gateways (i.e. within the 'tunnel').

The need for and level of encryption is an attribute of the quality of the data, i.e. the level of privacy and data integrity required. Hence there may or may not be a need for encryption within a particular Grid. If the nature of the data is such that there is a need for encryption, the level of encryption has 2 dimensions:

- The **robustness** of the encryption algorithm (how hard it is to break).
- The **geographic extent** of the encryption, e.g.:
  - network only
  - host-to-host
  - on-disk

If there is a real need for encryption, encryption over only the network path is rarely adequate, and on-disk encryption should be strongly considered. Encryption software rarely adds significant overhead.