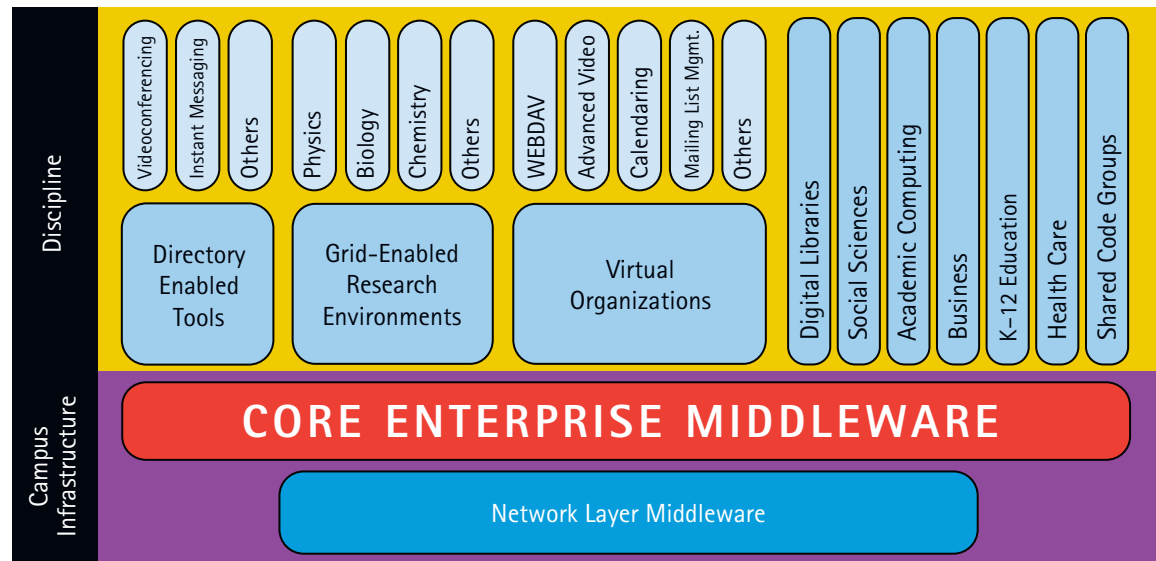




www.internet2.edu

Middleware is a layer of software between a network and the applications that use it. Middleware is an infrastructure that manages security, access, and information exchange on behalf of applications to make it easier and more secure for people to communicate and collaborate. It is used both to find people and things, as with directory services, and to keep them confidential, as with security services.



Why Middleware?

The absence of common, standard middleware solutions is a big problem for today's research and education networks. Addressing the opposing challenges of ensuring security and access, availability and privacy, a technology infrastructure—generically called "enterprise middleware"—is emerging throughout higher education, government, and corporate sectors.

Many of the online services and applications that campuses offer have similar requirements, which this infrastructure addresses:

- Are the people using these services who they claim to be?
- Are they members of our campus community?
- Do they have permission to use these services?
- Is their privacy being protected?

Applications either make do without these core middleware functions—in which case usability, security, and efficiency suffer—or applications perform middleware functions themselves, leading to competing and incompatible standards.

What is the Internet2 Middleware Initiative?

The goal of the Internet2 Middleware Initiative is to contribute to the building of an international interoperable middleware infrastructure for research and education.

The Middleware Architecture Committee for Education (MACE), a group of leading higher education IT architects, provides overall direction and vision for the Initiative. Their working agenda is set by campus CIOs and partners and includes:

- Researching and developing architectures, software, methodologies, practices, and standards for campus IT middleware infrastructure.
- Encouraging the establishment of community-based middleware policy and technology infrastructures.
- Working with government, corporate, and other national and international communities to ensure integration.
- Promulgating the findings and deliverables to catalyze deployment across the research and education communities.

Middleware Working Groups

While the vision is supplied by MACE, the research details are addressed by the Internet2 Middleware working groups. MACE forms these as needed to explore specific issues; below is a sampling of the many working groups (with their core enterprise middleware foci).

MACE-Dir (Directories)

The MACE-Dir Working Group researches and develops architectures and common practices to facilitate intra- and inter-institutional information exchange about people and services stored in an enterprise directory.

MACE-Shibboleth (Authentication and Authorization)

The MACE-Shibboleth Working Group develops architectures and corresponding software to support intra- or inter-institutional authentication and authorization for access to restricted electronic resources.

HEPKI-TAG (PKI)

The Higher Education Public Key Infrastructure-Technical Activities Group (HEPKI-TAG) is a collaboration between the Internet2 Middleware Initiative and EDUCAUSE and was formed to investigate technical issues related to the deployment of PKI in higher education.

MACE-WebISO (Authentication)

The MACE-WebISO Working Group investigates "web initial sign-on" (WebISO) software, which leverages campus authentication services to allow users with standard web browsers to authenticate to web-based services across many web servers.

VidMid (Directories and Authentication)

Video Middleware (VidMid) furthers the development of middleware for videoconferencing and related areas and is a collaboration between Internet2 Middleware Initiative and the Video Development Initiative (ViDe). The working group focuses on resource discovery and authentication for point-to-point and multi-point videoconferencing, and similar middleware requirements for video-on-demand, data collaboration, and voice over IP.

Core Enterprise Middleware components enable "transparent use," providing consistent infrastructure for security, privacy and access to protected resources:

- **Identity**—unique markers of person, machine, service, or group
- **Authentication**—how you prove or establish your identity
- **Authorization**—what an identity is permitted to do
- **Directories**—where an identity's basic characteristics (attributes) are kept
- **Public Key Infrastructure (PKI)**—set of security technologies that relies on the exchange of electronic credentials called certificates

NSF Middleware Initiative

The Internet2 Middleware Initiative also works in coordination with several other middleware-oriented efforts. The most important of these is the NSF Middleware Initiative (NMI) in which Internet2 partners with EDUCAUSE and the Southeastern Universities Research Association (SURA) under the consortium banner of NMI-EDIT. Funded with the GRIDS Center, these two teams work together on integrating campus and grid research infrastructures.

To Learn More

Visit middleware.internet2.edu for information about working group activities, architectures, implementation practices and guidelines, software downloads, email lists, and software demonstrations.

Contact mw-info@internet2.edu with specific questions.

Some of these activities are supported by the National Science Foundation (NSF) under the NSF Middleware Initiative-NSF 02-028, Grant No. ANI-0123937.