

December 8, 2003

Tom Arons, Data Center and Client Services
Brian Monroe, Agronomy and Range Science
Robert Ono, Information and Educational Technology, Workgroup Chair
Beau Patrette, Data Center and Client Services
Sharie Sprague, Offices of the Chancellor and Provost
Elizabeth St.Goar, Data Center and Client Services
Andrew Walker, Student Housing
David Zavatson, Data Center and Client Services

SUBJECT: FILE ENCRYPTION SERVICES

The Internet provides global electronic connectivity that is critical to the UC Davis mission to teach students, advance knowledge and deliver public services. While the Internet provides a mechanism for sharing information, the Internet also increases the risks to information privacy and security. In recognition of these growing risks, new federal and state laws have mandated personal information residing on computers be protected from unauthorized access and disclosure.

A few campus units have made initial inquiries with several vendors of file and disk encryption products. However, an encryption methodology and product for a single campus unit or group of campus units may not scale well or be cost effective for broader campus needs. An encryption system that could be used throughout the campus and by campus affiliates would provide maximum benefits to UC Davis.

Any campus use of file and disk encryption services must also be consistent with the University of California Electronic Communications Policy. The intent of this policy is to ensure that records subject to disclosure under the Public Records Act remain accessible to authorized individuals.

Charge

A workgroup is being formed to assist the campus to define the functions and requirements for a file and disk encryption system that can support academic, research and administrative needs. The functional requirements will serve as the basis for a formal request for information or proposal to be released in early 2004. The workgroup will define requirements addressing, but not necessarily be limited to:

- key functional target of campus encryption services
- campus heterogeneous computing environment,
- use of industry accepted encryption standards,
- cryptographic key management,
- security of encryption infrastructure,
- robust and reliable operation,
- cost effectiveness,
- administration requirements,
- access revocation requirements,
- continued university access to archived encrypted information,
- ease of use and transparency of operation to end users, and
- scalability to students, staff, faculty and university affiliates

The workgroup findings and recommendations should be summarized and complete by March 31, 2004.

I appreciate your willingness to serve on this workgroup and look forward to receiving your report at the end of March. Please don't hesitate to consult with me if you have any questions.

Sincerely,

John Bruno
Vice Provost—Information and Educational Technology

c: Tracy Bennett, Student Housing
Leslye Hays, Offices of the Chancellor and Provost
Morna Mellor, Data Center and Client Services
Chris van Kessel, Agronomy and Range Science