



THE UNIVERSITY OF MICHIGAN
COMPUTER PURCHASING

7071 WOLVERINE TOWER
3003 S. STATE STREET
ANN ARBOR, MI 48109-1282
PHONE: 734-615-5700 FAX: 734-615-6235

The University of Michigan
Information Technologies Central Services
Secure Remote Access Project

Request for Information
C-0514-04-A

April 26, 2004

RFI Table of Contents:

Section 1: The University of Michigan Overview

Section 2: Scope of Interest

Section 3: RFI Logistics

Section 4: General Terms and Condition

Section 5: Company Information

Section 6: Price Model

Section 7: Technical Details

Section 1: The University of Michigan Overview

The University of Michigan Information Technology Central Services (ITCS) is an auxiliary unit that provides communication services to U of M campus at large. The Network Working Group, with membership drawn from campus IT service providers, is charged with the development of networking standards and practices for the campus community.

The University is in an ongoing process of enhancing and upgrading its network security infrastructure. ITCS, the Network Working Group, and other working groups are investigating numerous options to provide a secure environment for campus users and a number of projects have been initiated. This RFI is in regards to secure access to campus computing resources for the numerous members of the University community who work off-campus. This section describes the customer base served and provides an overview of current services. The diverse requirements of our faculty, staff, and students demand a flexible solution to secure access issues.

ITCS maintains much of the University's communication infrastructure for voice, video and data networks. The entire University of Michigan backbone network is made of up three separate backbones. IT Communications (ITCom), a unit within ITCS, provides the Ann Arbor campus backbone network, UMnet. The College of Engineering and the University of Michigan Health System each have a backbone network as well. This infrastructure supports three geographically dispersed campuses and connects in excess of 200 departmental LANs.

There are, in addition, numerous remote offices, distance learning facilities, health clinics, and other facilities located in the surrounding communities, throughout the USA, and worldwide.

The University has over 80,000 faculty, staff, and students that use the networking infrastructure. From a recent survey, over half reported that they have a laptop or other mobile device. This continues an increasing trend over the last few years of mobile computing, in which the faculty, staff, and students not only expect to work from their desk, but from any location that is convenient for them.

Secure access requirements therefore include access to the enterprise network for a large number of individual clients; remote office access for dispersed sites; and highly protected access to sensitive financial, clinical, and student data.

ITCS will need to work closely with all campus units to coordinate an integration that meets the entire user population's diverse locale, operating platform, and usability needs.

Section 2: Scope of Interest

With such a large possible user base, the University of Michigan's remote secure access needs range from a single user to remote office locations that need to connect to the campus backbone. Our decentralized model allows, but does not necessarily encourage, schools, colleges, and other units to choose their own solution. With this in mind, the ability of the solution to scale to all needs is a key concern. The following are a few possibilities for deployment.

1. A single user who wants to connect to the main campus while traveling. The possibility of machine OS range greatly.
2. A home office user who wants to connect not just a single machine, but also peripheral devices such as a VoIP phone.
3. A remote office with a range of users. They will want to appear as an extension to the main campus.

With so many variations, the needs for a standards based solution that can scale to the many uses and requirements is imperative. The added functionality of a consistent control and management platform for cross-training among support staff is also a key component of what we are looking for.

Section 3: RFI Logistics

Request for Information Issuing Office:

This RFI is issued by the Department of Purchasing Services, The University of Michigan, on behalf of ITCS. The Department of Purchasing Services is the sole point of contact for this RFI.

Qualifications to respond:

ITCS is seeking a product(s) that meets the needs of most of the functionality requirements of a Secure Remote Access solution. The responding vendors must have a stable and proven product solution. ITCS is not currently assessing the viability of a customized developed solution.

The University of Michigan is not liable for any cost incurred by a Proposer in replying to this RFI.

RFI Schedule and Critical Dates:

RFI Issued: April 26, 2004
Response Due: May 14, 2004

RFI General Instructions:

1. Each Vendor is solely responsible for the timely delivery of its response. Responses received after the due date may not be used in the analysis being done by the ITCS.
2. Requests for Information Responses are due May 14th, 2004 no later than 4:00 pm. ET.

They should be sent to:

Andrew J. Supers
Room 7071 Wolverine Tower – 7th Floor
3003 South State Street
Ann Arbor, MI 48109-1282

3. Responses shall be submitted in **Microsoft Word format, one (1) original and one (1) electronic version**. Please include an executive summary and repeat each question before answering it.
4. All questions pertaining to this RFI should be submitted in writing to: computer.procurement@umich.edu.

Section 4: General Terms and Conditions

1. ITCS is releasing this Request for Information as a part of the Secure Remote Access Project. The Request for Information Responses will NOT be used to buy a product or solution from a vendor. At the discretion of ITCS, ITCS may decide to proceed at a future date with a Request for Proposal.
2. Any responses, materials, correspondence or documents provided to the ITCS are subject to the State of Michigan Freedom of Information Act and may be released to third parties in compliance with that Act. Subsequently, no information provided to the ITCS in responding to this Request for Information including pricing and delivery information, shall be considered proprietary or confidential information.
3. This request shall be governed by and construed in accordance with the laws of the State of Michigan. "The parties understand and expressly agree that any claims, demands, or actions asserted against the Regents of the University of Michigan, its agents or employees shall be brought only in the Michigan Court of Claims, as it is the only court of exclusive jurisdiction over claims against the University of Michigan, a Michigan constitutional corporation."
4. Vendor certifies that it is an independent contractor, licensed and bonded, and is solely responsible for employment, acts and omissions, control, and direction of its' employees.

Responses must be submitted to:

The University of Michigan
Purchasing Services
Andrew J. Supers
7071 Wolverine Tower- 7th Floor
3003 S. State Street
Ann Arbor, MI 48109-1282

Vendors may email all questions to computer.procurement@umich.edu
(For all inquiries please include the response number and project name in the subject line.)

Section 5: Company Information

1. Provide complete address for the national main office and local branch office and the number of employees at each location.
2. Identify the sales person (s) that would be responsible for the ITCS installation. Include address and telephone number.
3. Provide information on your company history including profitability figures for the last five years. Include number of years in business and client growth patterns.
4. What differentiates your company and its product from competitor products? What are your company's core competencies? What are your support model and support services?
5. Provide the name of your company's current higher education clients. Provide the name of three references (one higher education reference) that may be contacted including Company Name, Contact Title, Address, Phone Number, Brief description of what your company delivered and implementation date. Selected references should have similar project initiatives.
6. Describe an engagement that has been successfully implemented that has the most common attributes to the needs of the University of Michigan Secure Remote Access project. Include information regarding the size of the organization, the number of users, the functionality that was deployed and roll-out strategy, adoption rate statistics, the applications it integrated with, the key milestones and duration of the project and any other relevant information.
7. Briefly describe your roll-out strategy and methodology. Identify whether you provide the integration services or whether you partner with other vendors for the integration and rollout of your portal product.

Section 6: Price Model

1. Please describe your pricing model as it relates to the following:

- Licensing
 1. per server
 2. per user
- Training
- Maintenance
- Hosting Alternatives
- Support Services
- Travel
- Scalability
- Other Variables

Section 7: Technical Details

Please detail your solutions capabilities based on the following areas.

Hardware
Network Ports (type and how many)
Do you adhere to the IEEE 802.1Q/P standard?
Encryption methods (DES, 3DES, AES...)
Hash types (MD5, SHA...)
Diffe-Helman Groups
Authentication Methods (Preshared Keys, X.509, KX.509...)
Authorization (Active Directory, LDAP...)
Tunnel Protocol (IPSec, SSL, L2TP...)
Nat Transparency (TCP, UDP...)
Routing Protocols (OSPF, Static, ISIS...)
Simultaneous Tunnels
Throughput (please note if software or hardware encryption)
Key Management
Hardware Access (HTTPS, SSH, Telnet...)
Concentrator Management
Various levels of access?
Number of levels
Are levels user definable
Support remote authentication (RADIUS, TACCACS...)
Monitoring (SNMP, Syslog...)
Clustering
Expandability (please list how)
High Availability (please list how)
Failover (please list how)
Central Admin Client controller

Configure and distribute preconfigured client
Push Updates to clients
Remote Client Security Enforcement
Virus Scan included or enforceable
Personal Firewall included or enforceable
Patch Level checking enforceable

System Security	Yes	No
Does the system disconnect after three invalid attempts during remote login by the administrator?		
Can the system be accessed by the vendor technical assistance group without knowing the password?		

	Client available	3 rd Party Client	Licensing Agreement	Split Tunnel	Nat Traversal	Personal Firewall	Virus scan tool
Windows 98							
Windows ME							
Windows NT							
Windows 2000							
Windows XP							
Mac OSX							
Mac 9							
Mac 8							
Linux (List distribution)							
BSD							
PocketPC							
Palm							
Clientless (SSL)							
Others							

Please respond under each item the detailed information requested.

1. Describe how your architecture is positioned for scalability? Can the architecture be horizontally and vertically scaled?
2. Discuss in detail how the system will interface with the Kerberos authentication server.
3. Detail support of Kerberos version 5.
4. Identify system requirements to successfully integrate with University of Michigan Directory servers with LDAP interface. The University of Michigan uses OpenLDAP version 1.2.11.
5. Is simple bind over SSL supported?
6. Identify your willingness to work with the University of Michigan for future feature development and testing.
7. Identify the degree to which your company is willing to engage in joint development work to resolve authentication and integration issues with UM directory services.
8. Identify if additional hardware is required or not to meet the required hot failover.
9. Identify environmental, physical, power and network requirements for the proposed system.
10. Which versions of Simple Network Management Protocol does your system Support (1, 2, 3)?
11. Will your solution provide enterprise specific MIBS that can be parsed in the University of Michigan Network Management System (Aprisma, Spectrum) utilizing industry standard compilers.
12. Identify which SNMP traps are generated by the System.
13. Does your product support multiple levels of trapping and separate informational traps from warning/critical traps?
14. For which types of encryption is there hardware based acceleration?
15. Detail your implementation of 'role based access control'.
16. List all browsers which you have tested in secure mode for compatibility with your Concentrator (provide browser versions and OS tested with). All those not listed will be assumed to pass unsecured traffic.
17. Are any third party and / or proprietary software involved? Please identify the third parties and how the software is supported.
18. What options does your product have for authenticating a user? Does it use its own database? Can the users be authenticated against Radius/Kerberos/LDAP?

19. What options does your product provide for reading and storing user profile information (beyond authentication information)?
20. Please describe your system architecture by using a logical architecture diagram. Also provide a brief description of the modules/ components of your architecture. Please include which modules are required and which ones are optional.
21. What Authentication infrastructures are supported (RADIUS, Kerberos, Active Directory, Novell eDirectory...)?
22. Please detail what troubleshooting utilities (logs, applications...) that are on available on the concentrator.
23. Does your product support multiple logging locations? Can different user bases be logged to diverse locations?
24. Is IP Precedence (TOS, DSCP) supported? If so, does your product also support rewriting IP Precedence?