

**Table of Contents**

<b>Table of Contents</b> .....	<b>1</b>
<b>Background</b> .....	<b>2</b>
<b>Who we asked?</b> .....	<b>2</b>
<b>Respondents' PKI Experience</b> .....	<b>3</b>
<b>Institutions PKI uptake</b> .....	<b>4</b>
<b>PKI supported applications</b> .....	<b>5</b>
<b>Application/Infrastructure software packages currently in use</b> .....	<b>21</b>
<b>Additional Comments</b> .....	<b>23</b>
<b>Conclusion</b> .....	<b>23</b>

## **Background**

The eSecurity Framework project is part of a larger effort from Australian Higher Education Sector with support from AusCERT, CAUDIT, The University of Queensland, the Australian government and other universities to develop an environment in which universities can collaborate with each other at low cost and low risk.

This project builds on projects such as CAUDIT PKI and MAMS to establish a production Public Key Infrastructure (PKI) for the University and Research Sectors. This project seeks to develop standards and guidelines under a federation model, which leverages the PKI infrastructure in aligning the trust arrangements between institutions to support the implementation of Shibboleth across the sector. It also seeks to lower the barriers of entry to PKI using open source software. This project endeavours to enable the secure sharing of resources and research infrastructure across the domestic sector and with international partners.

The 'Application survey' main objective is to understand current and anticipated use of PKI enabled applications. The responses will influence the makeup of the certificate interoperability test matrix being developed by this project.

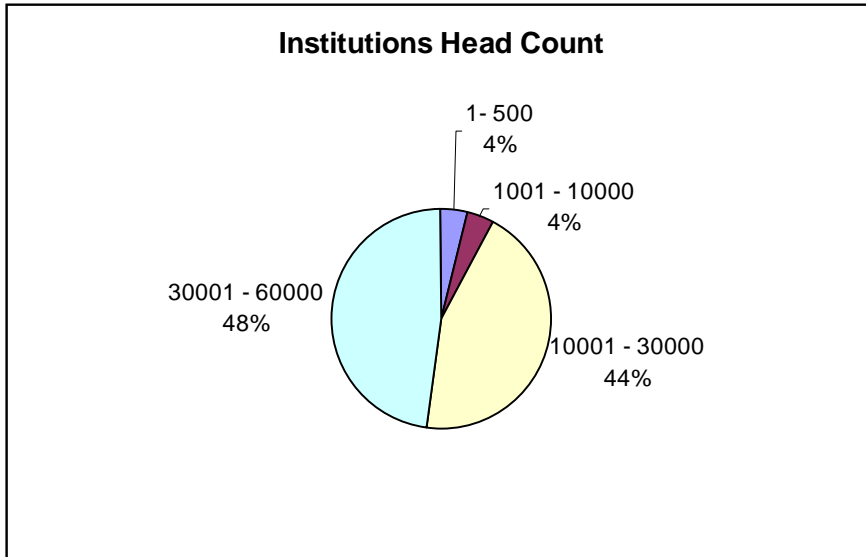
## **Who we asked?**

This survey was available at the CAUDIT web site. CAUDIT and AusCERT member universities were invited to provide their input. We targeted those who were involved in or have a stake in end user applications.

28 respondents representing a number of universities in Australia and New Zealand participated in this survey.

Participant institutions included Australian National University, Charles Stuart University, Curtin University of Technology, Deakin University, Flinders University, Griffith University, James Cook University, LaTrobe University, Murdoch University, Queensland University of Technology, RMIT University, The University of Queensland, The University of Sydney, The University of Waikato, The University of Wollongong, University of Melbourne, University of Otago, University of Southern Queensland, University of Western Australia and University of Western Sydney.

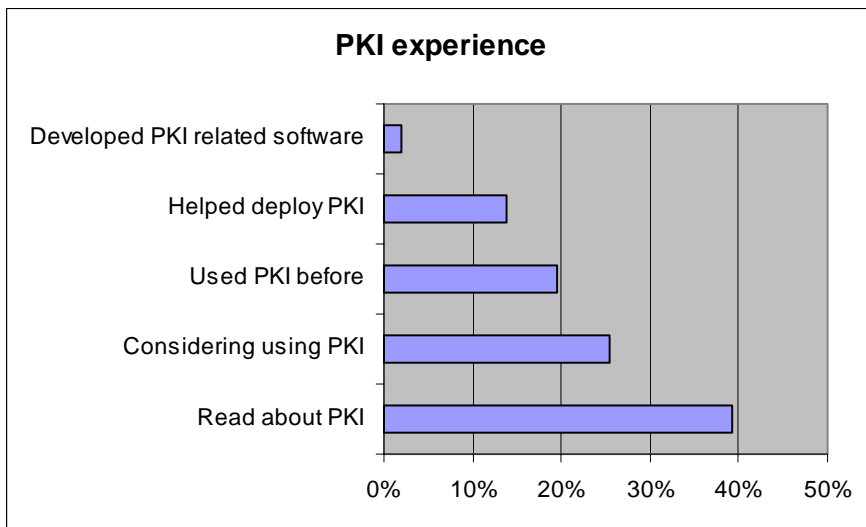
Respondents were asked to provide the total head count of their institutions. Their responses are illustrated in the chart below.



### Respondents' PKI Experience

In an attempt to better understand the expertise of the respondents we asked what involvement they have had with PKI. 39% of respondents responded that they have read about PKI, 25% were considering using PKI, 20% have used PKI, 14% helped deploy a PKI infrastructure and 2% have developed PKI related software.

The chart below illustrates these responses.

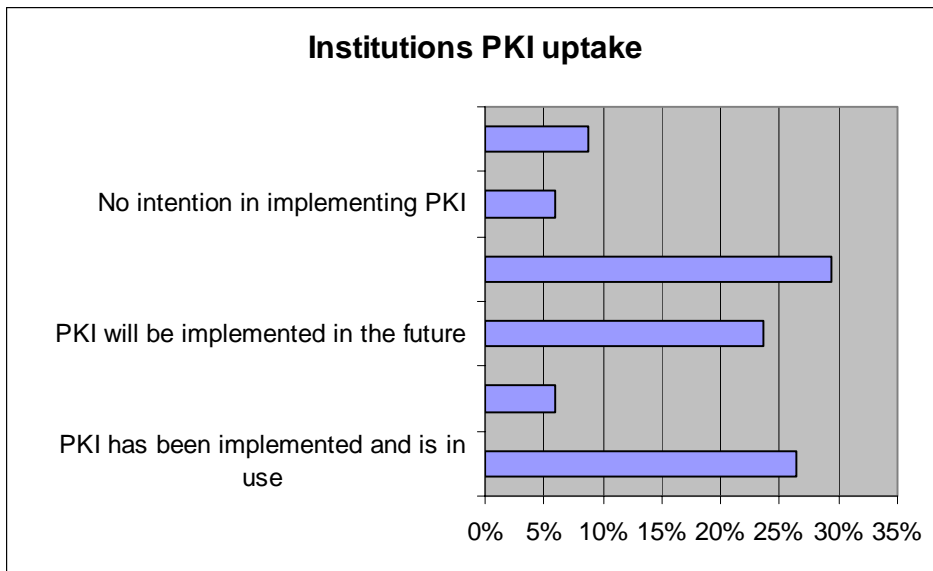


### **Institutions PKI uptake**

Respondents were asked to express their institution's interest in deploying PKI.

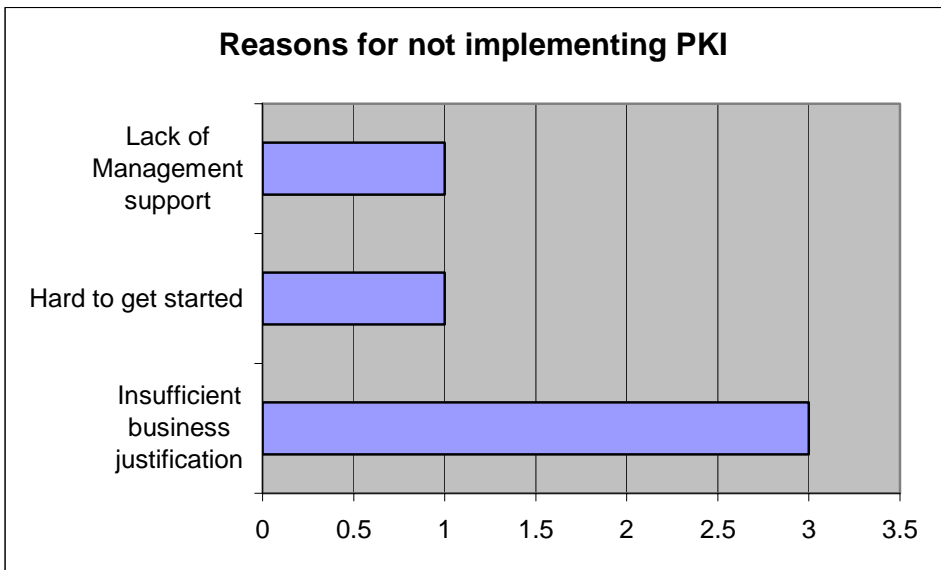
Based on respondents' answers it was noticed that PKI enabled applications are catching the interest of the higher education sector. The following charts support this assumption.

Out of 28 respondents 9 claim their institution have implemented PKI, 2 plan to implement PKI in 2007, 8 would like to implement PKI in the future, 12 have no intention in implementing PKI, however from these 10 would like to use certificates issued by another organisation, 1 is awaiting on a business case to decide on a course of action.



**We asked institutions that did not intend to implement PKI to explain their reasons.**

Only 5 responses were provided, which raised three main reasons for not implement PKI. These issues were insufficient business justification, insufficient management support and difficulty of implementation.



### **PKI supported applications**

Participants were asked to rate various PKI supported applications as ‘Most Important’, ‘Important’ and ‘Not Important’ in light of users population such as ‘General Staff’, ‘Research/Academic Staff’ and ‘Students’ for future use at their institutions.

*Web server* and *services security* were rated the ‘most important’ with *SSL* and *SSH* applications rated prominently. *Secure email* was identified as ‘important’ for research, academic and general staff.

A large number of respondents were unsure of the importance of *Grid*, *Eduroam*, *Globus* and *Shibboleth*.

**Australian Higher Education  
Application Survey Results**



The table below illustrates the number of responses in order of importance for each of the applications and infrastructure software packages.

	<b>Most Important</b>	<b>Important</b>	<b>Not Important</b>	<b>Don't Know</b>
<b>Document Signing</b>	3	15	3	4
<b>Secure Email</b>	8	14	3	1
<b>Code Signing</b>	0	7	13	7
<b>Single Sign On</b>	5	15	5	3
<b>Web Server Security</b>	13	10	1	1
<b>Web Services Security</b>	12	9	1	4
<b>Virtual Private Network</b>	6	14	1	3
<b>Electronic Commerce</b>	5	9	7	5
<b>Secure Wireless LAN</b>	7	10	4	4
<b>Secure RPC</b>	2	7	11	5
<b>SSL</b>	9	13	2	2
<b>SSH authentication</b>	9	13	2	2
<b>Kerberos</b>	3	11	6	5
<b>Windows login</b>	3	10	7	5
<b>A-Select</b>	0	1	7	17
<b>S/MIME</b>	3	7	6	9
<b>Dual Key</b>	1	1	7	16
<b>AuthN</b>	3	2	5	15
<b>Desktop Client authN</b>	3	2	5	15
<b>AuthN for EAP/TLS</b>	0	3	7	15
<b>Grid</b>	1	6	7	12
<b>Eduroam</b>	2	8	5	10
<b>Globus</b>	1	3	5	15
<b>Pubcookie</b>	0	2	5	17
<b>Shibboleth</b>	3	7	3	12
<b>Smart Cards</b>	2	4	7	12

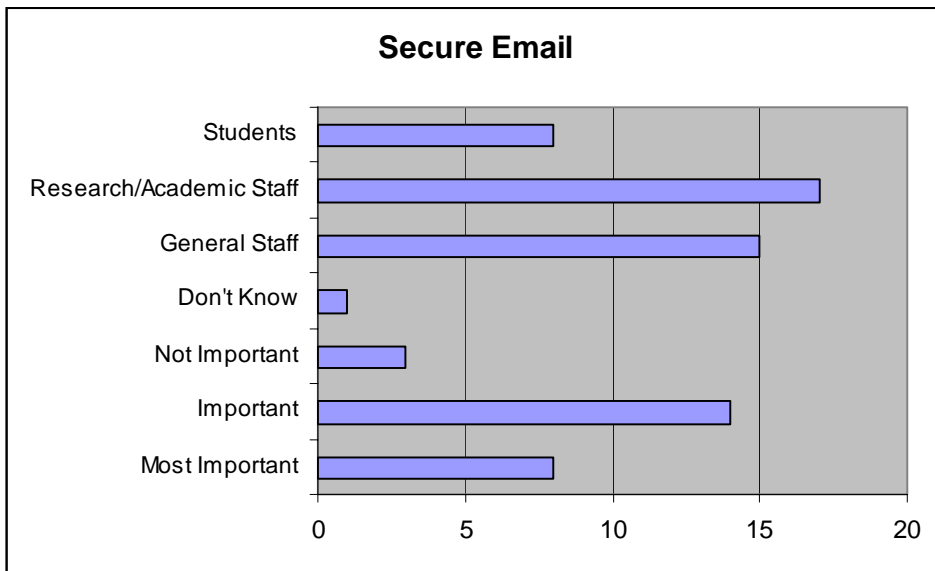
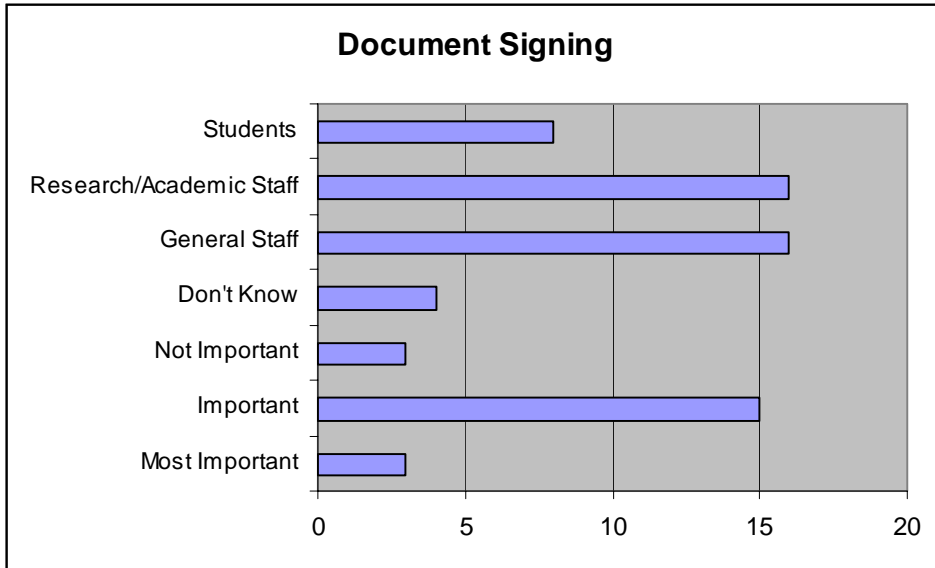
**Australian Higher Education  
Application Survey Results**

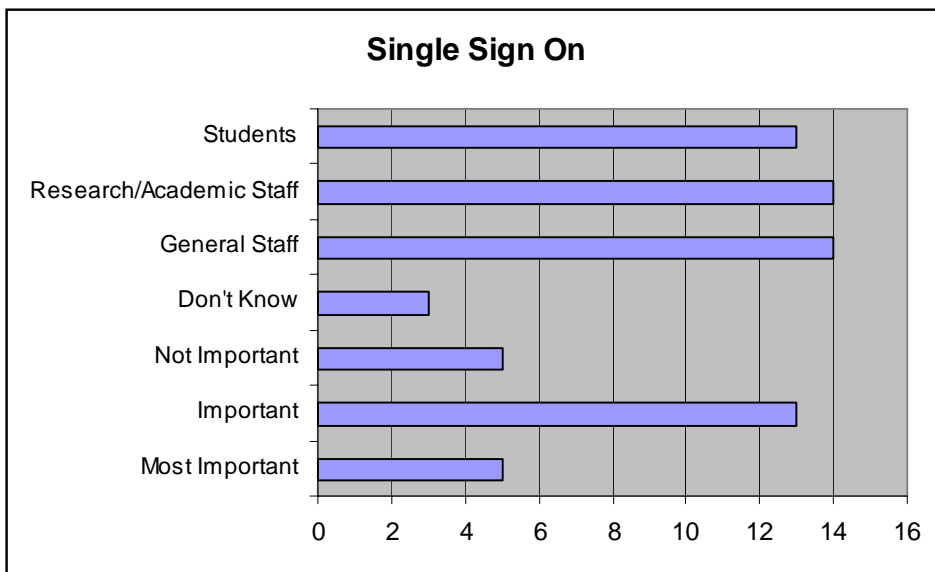
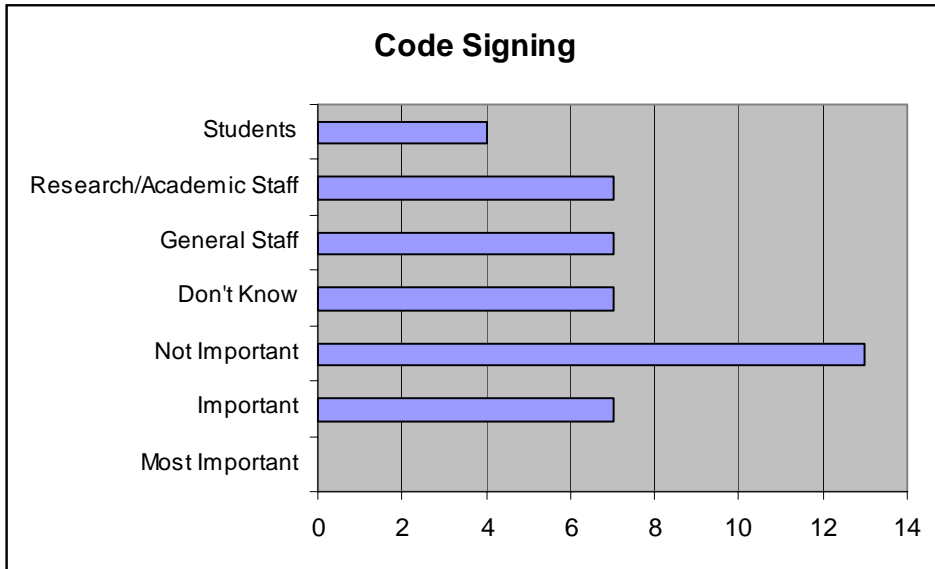


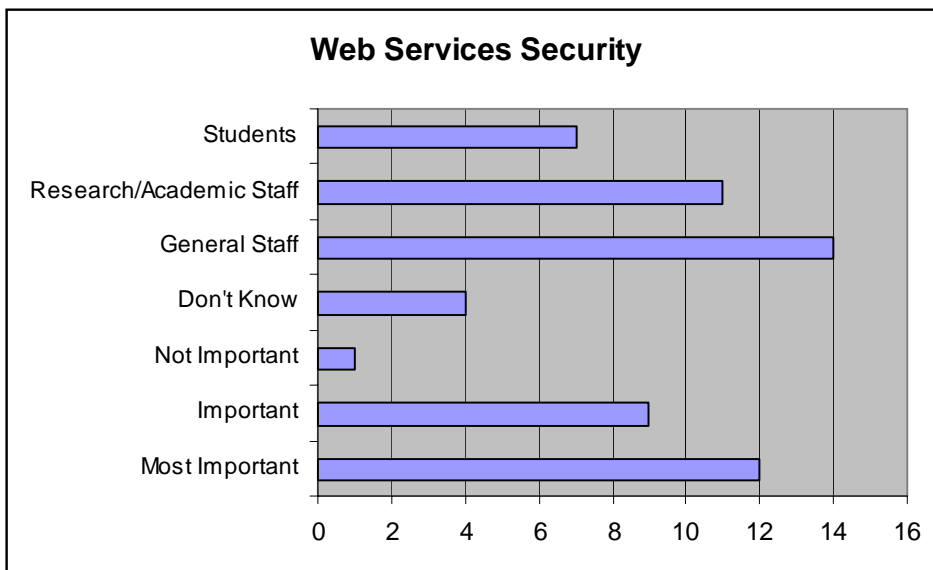
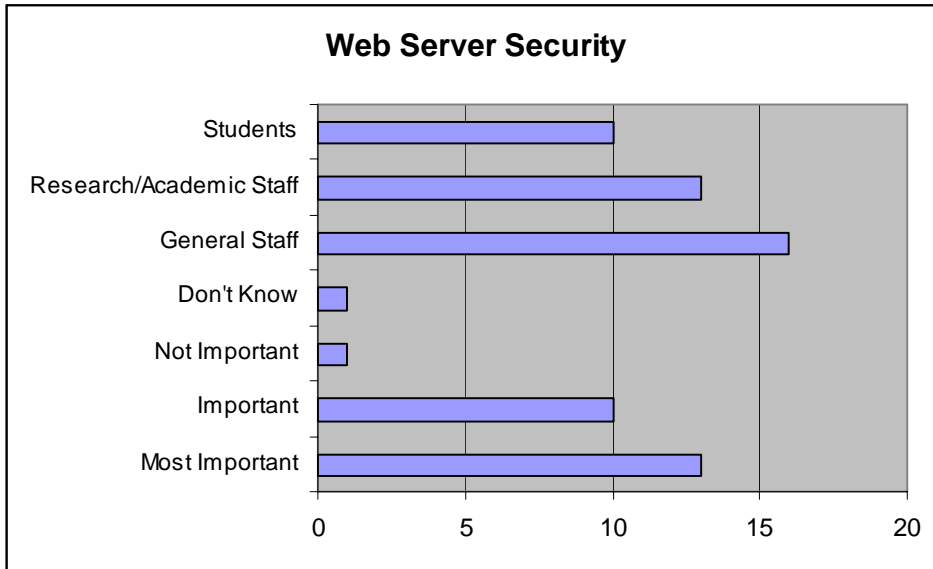
The table below illustrates the importance of each of the applications and infrastructure software packages for ‘general staff’, research and academic staff’ and ‘students’.

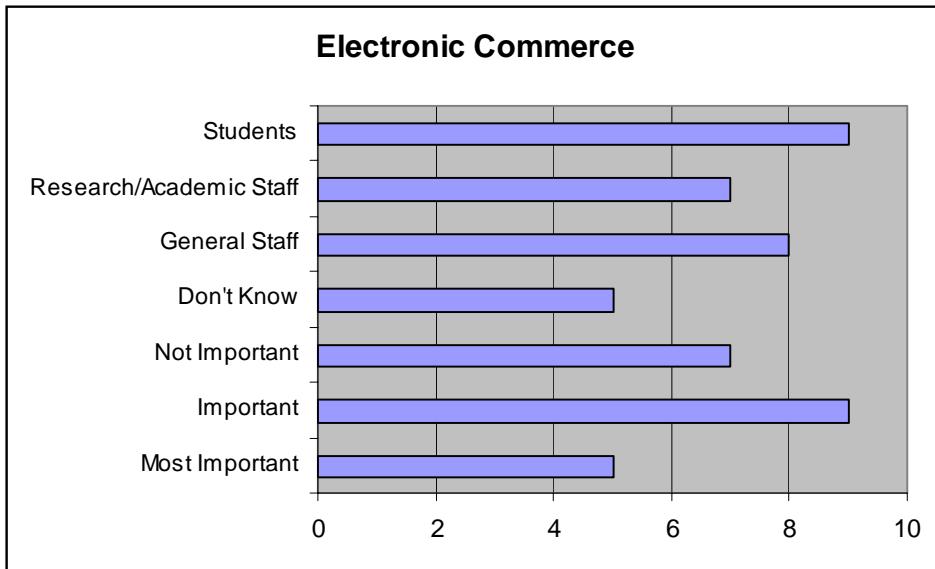
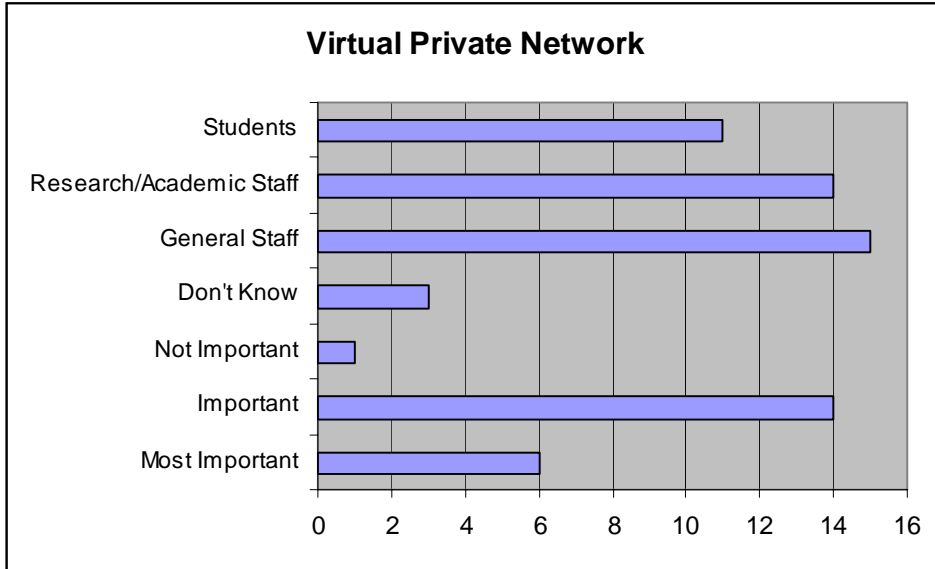
	<b>General Staff</b>	<b>Research/ Academic Staff</b>	<b>Students</b>
<b>Document Signing</b>	16	16	8
<b>Secure Email</b>	15	17	8
<b>Code Signing</b>	7	7	4
<b>Single Sign On</b>	14	14	13
<b>Web Server Security</b>	16	13	10
<b>Web Services Security</b>	14	11	7
<b>Virtual Private Network</b>	15	14	11
<b>Electronic Commerce</b>	8	7	9
<b>Secure Wireless LAN</b>	11	12	11
<b>Secure RPC</b>	6	7	4
<b>SSL</b>	16	13	12
<b>SSH authentication</b>	16	11	6
<b>Kerberos</b>	9	9	7
<b>Windows login</b>	10	9	7
<b>A-Select</b>	1	1	1
<b>S/MIME</b>	9	8	6
<b>Dual Key</b>	2	2	2
<b>AuthN</b>	4	4	4
<b>Desktop Client authN</b>	4	3	4
<b>AuthN for EAP/TLS</b>	2	2	3
<b>Grid</b>	3	6	3
<b>Eduroam</b>	6	6	4
<b>Globus</b>	2	3	3
<b>Pubcookie</b>	2	2	2
<b>Shibboleth</b>	6	8	5
<b>Smart Cards</b>	5	5	3

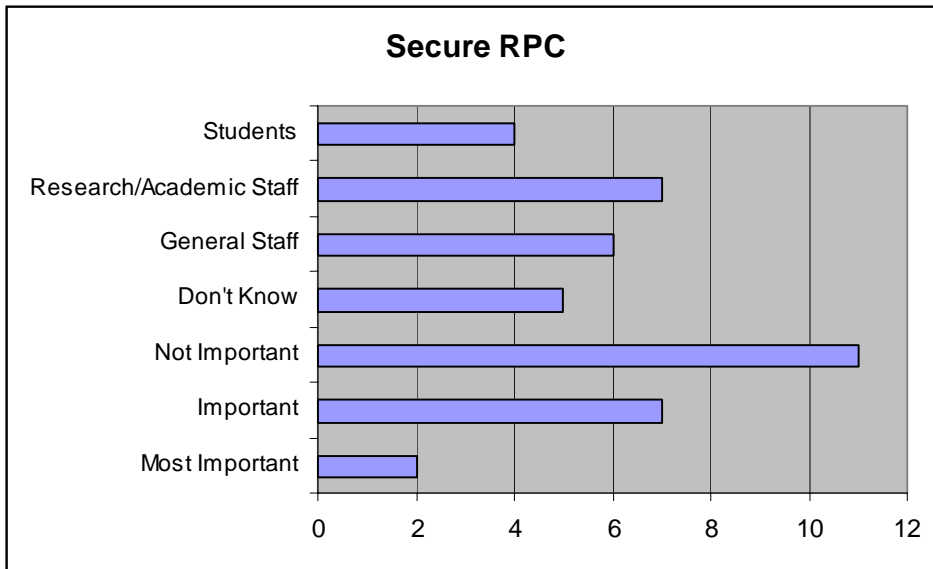
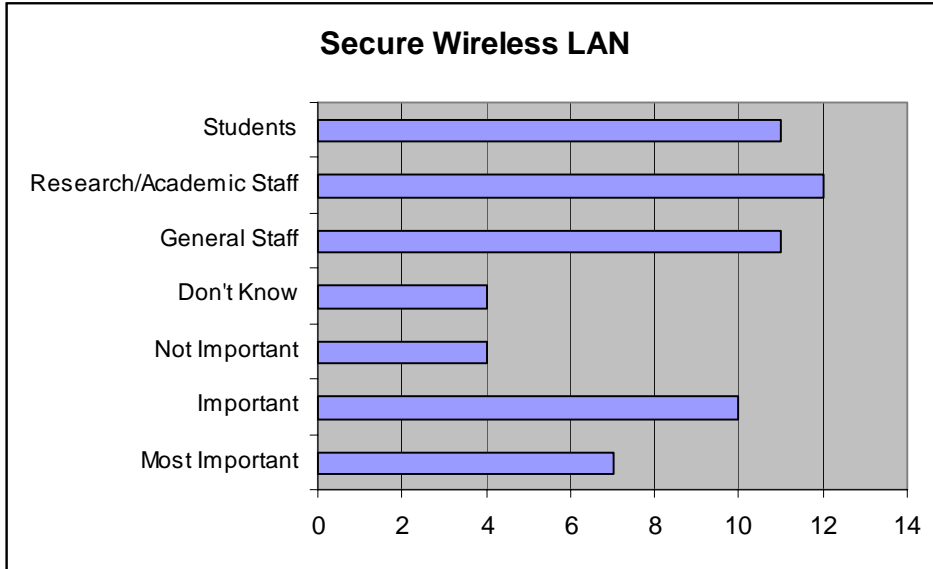
The following 26 charts illustrate the results of the table above, indicating the importance and utilization by application and/or infrastructure software package.

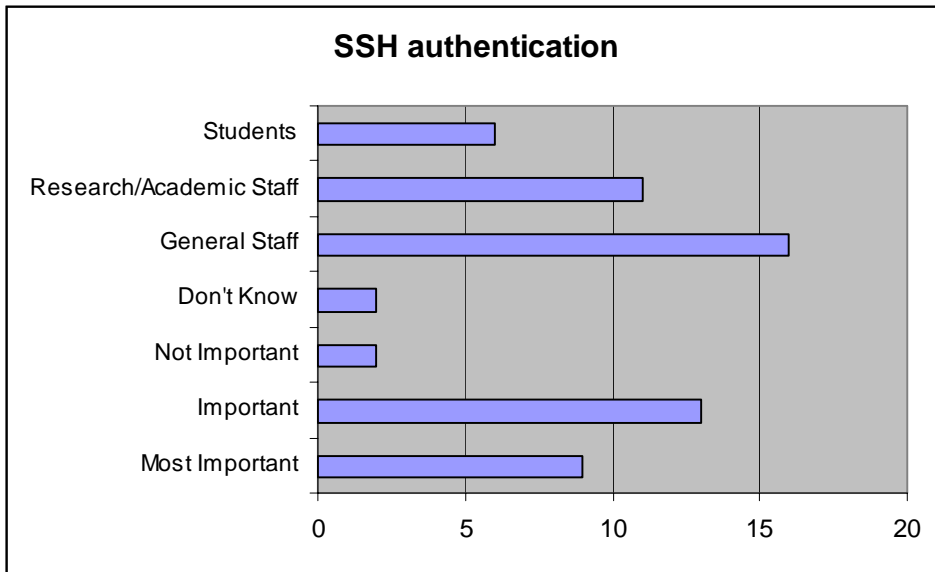
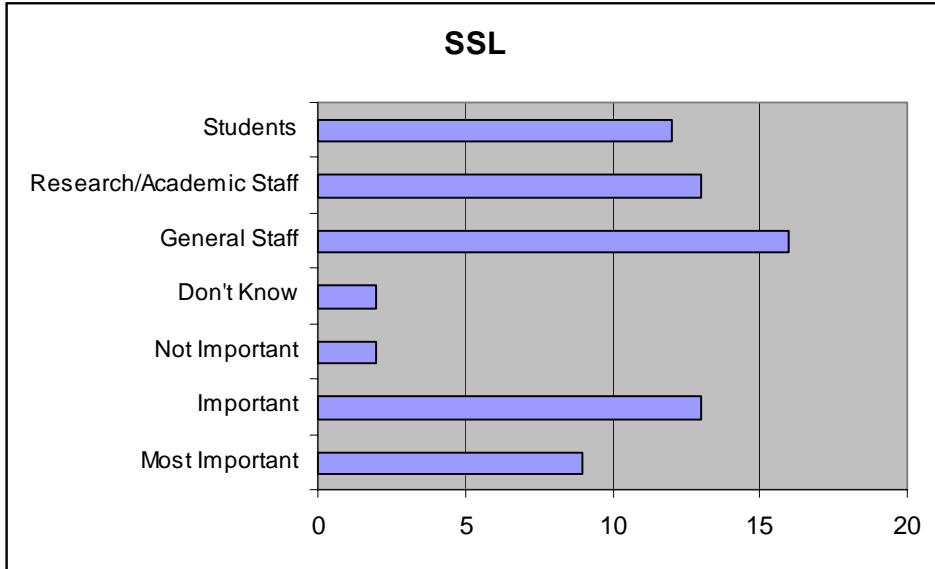


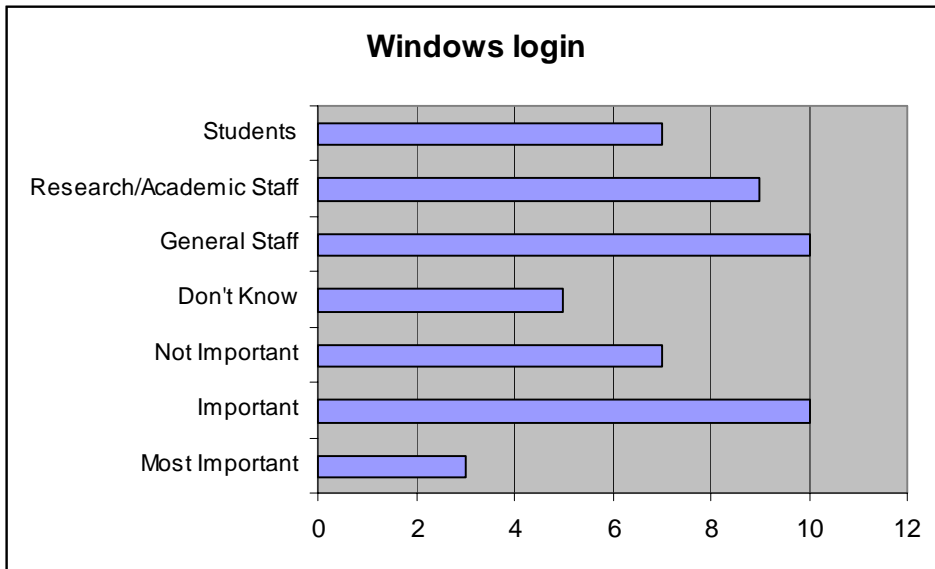
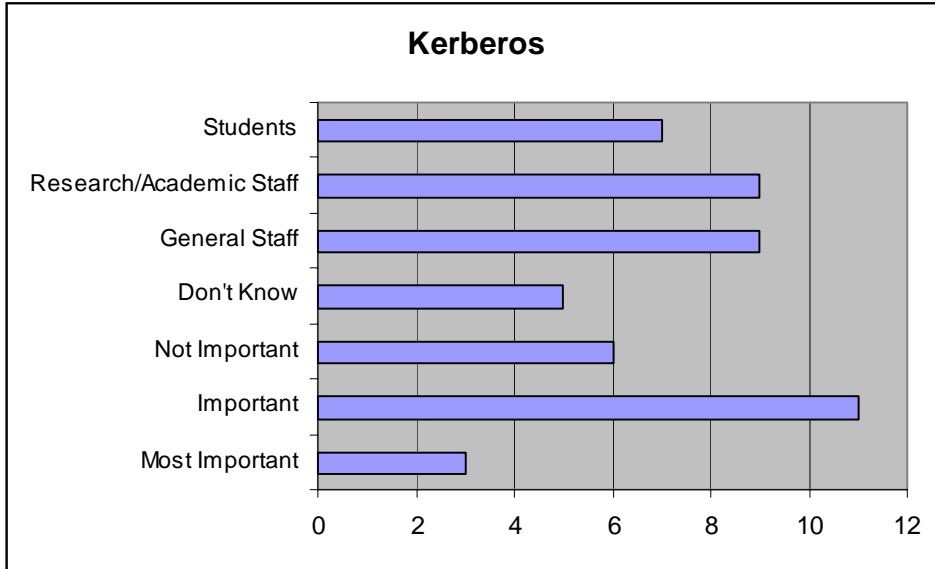


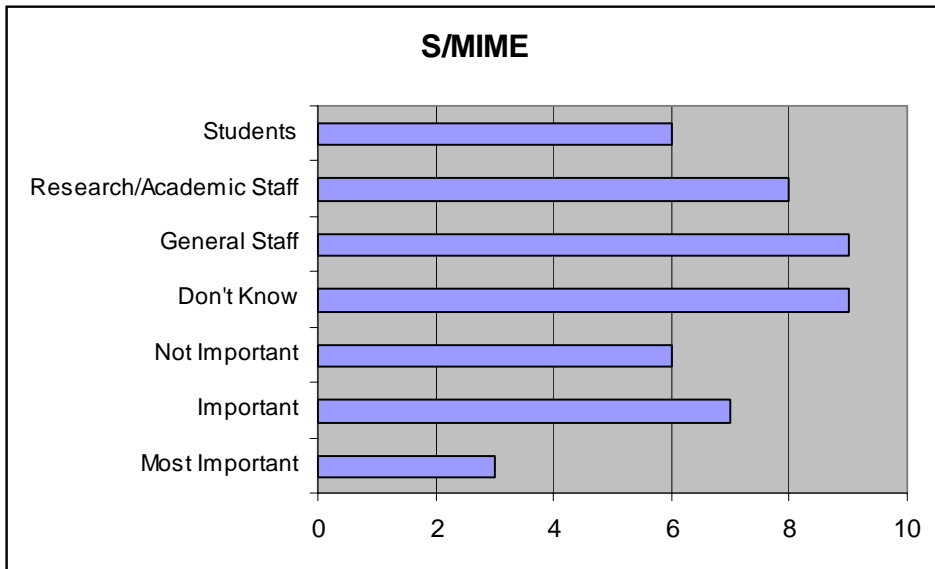
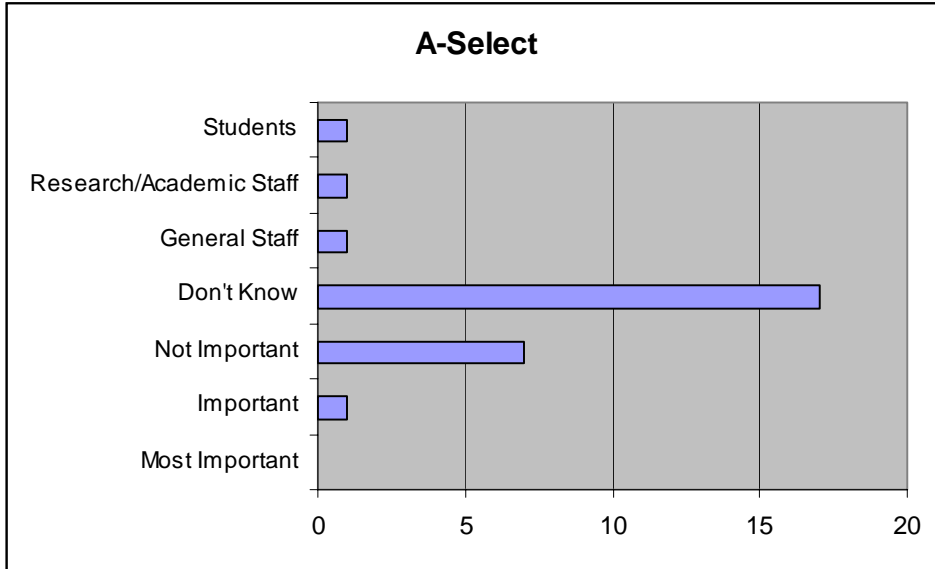


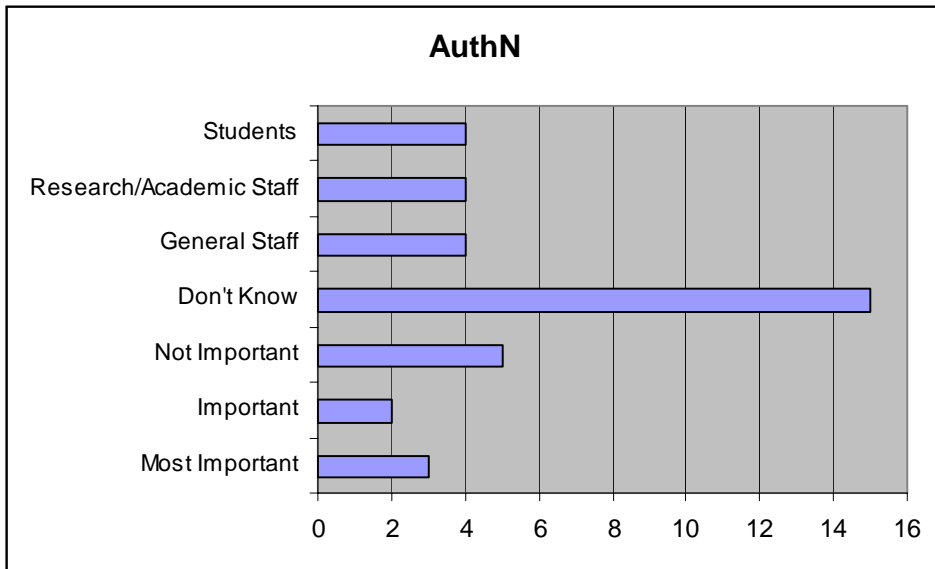
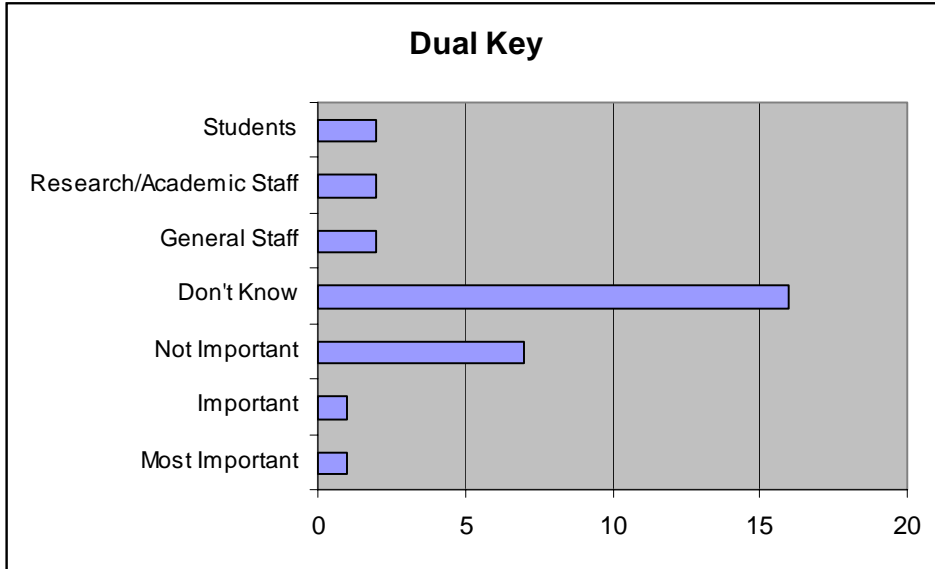


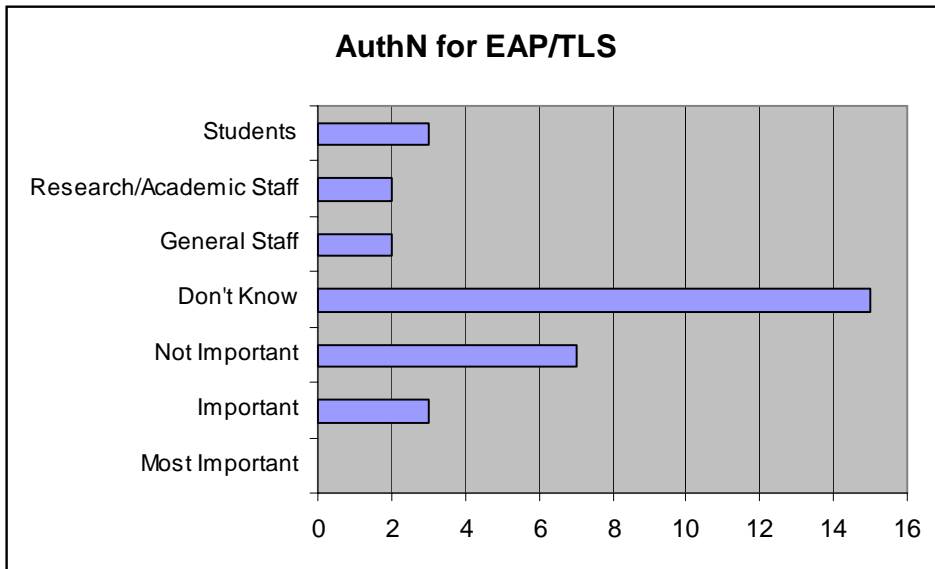
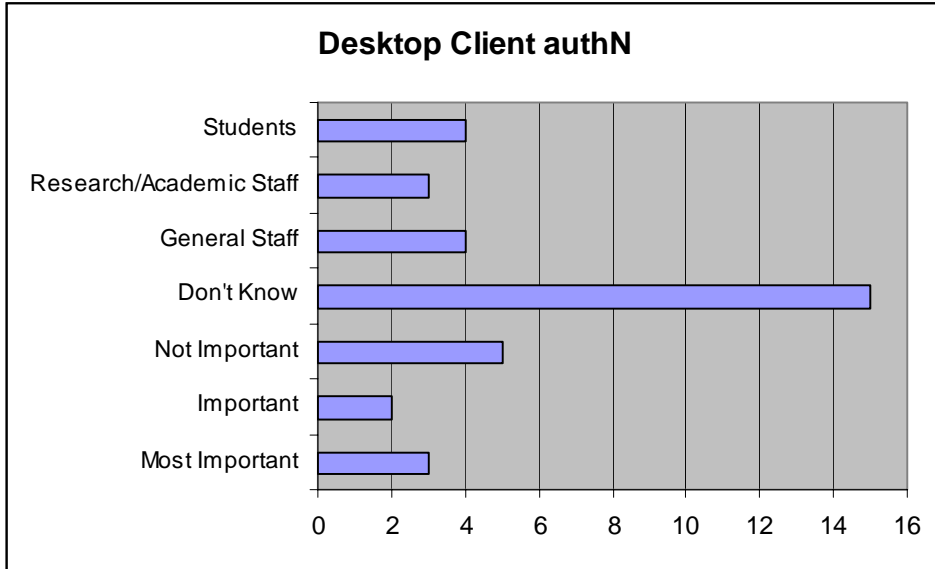


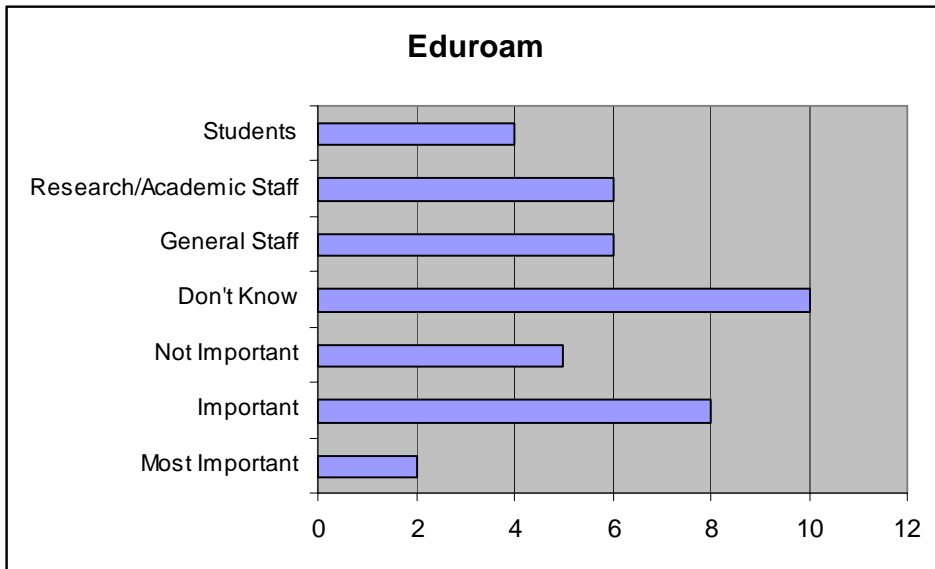
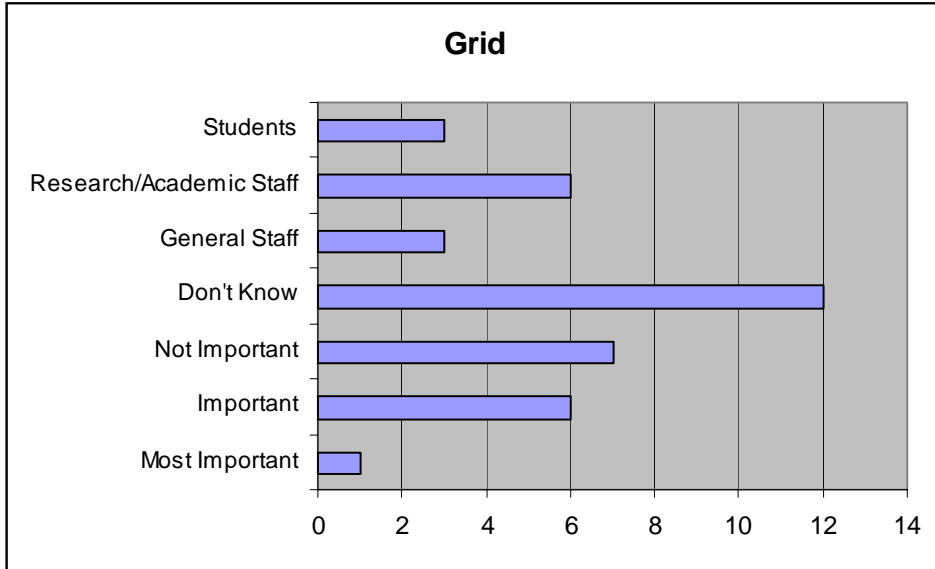


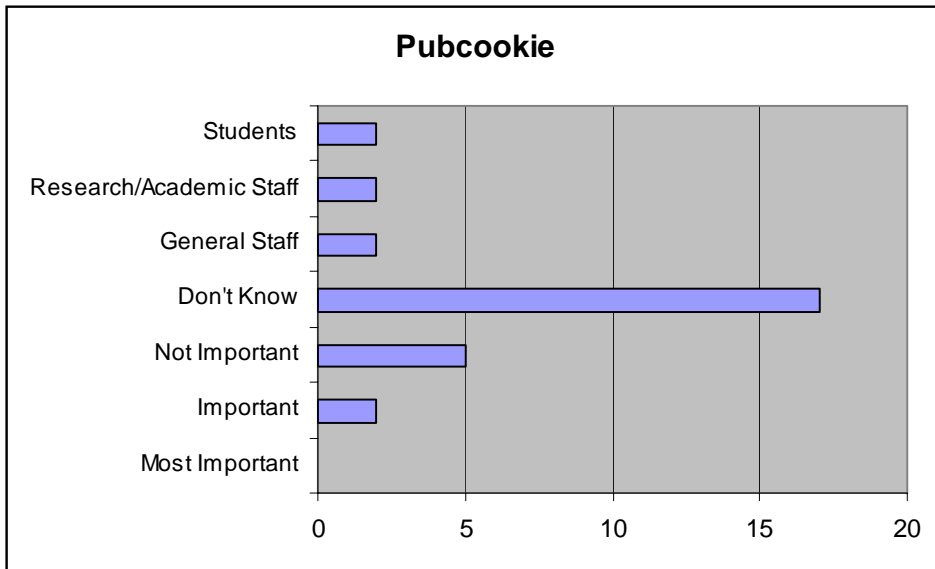
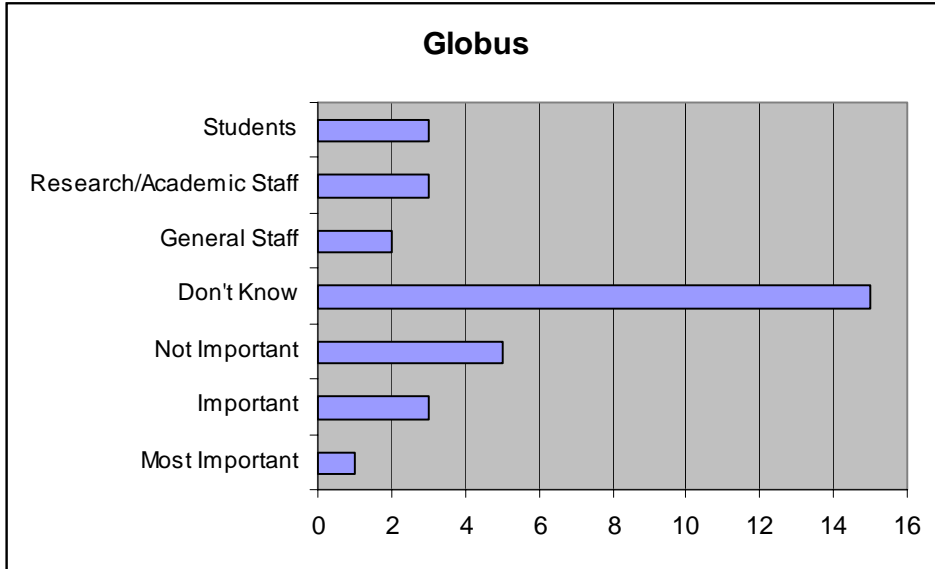


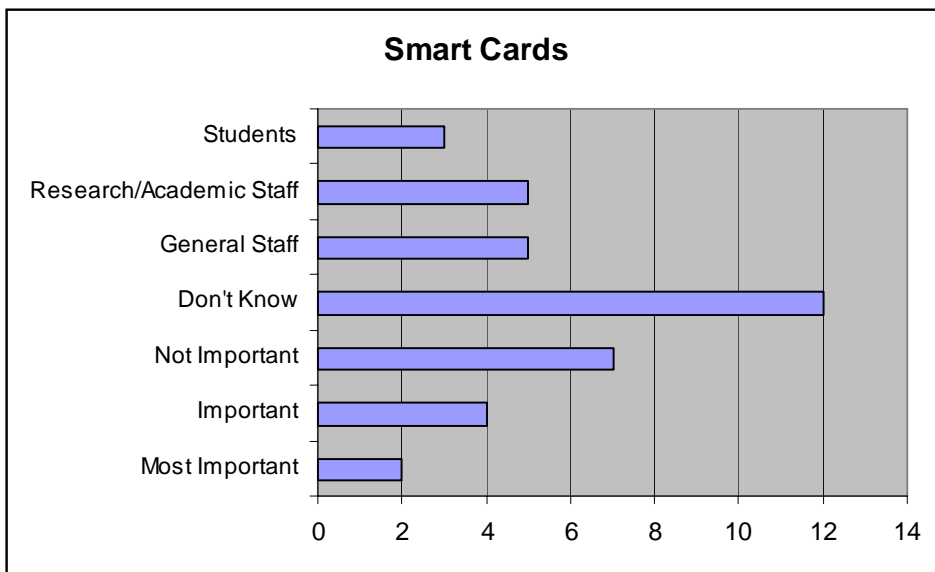
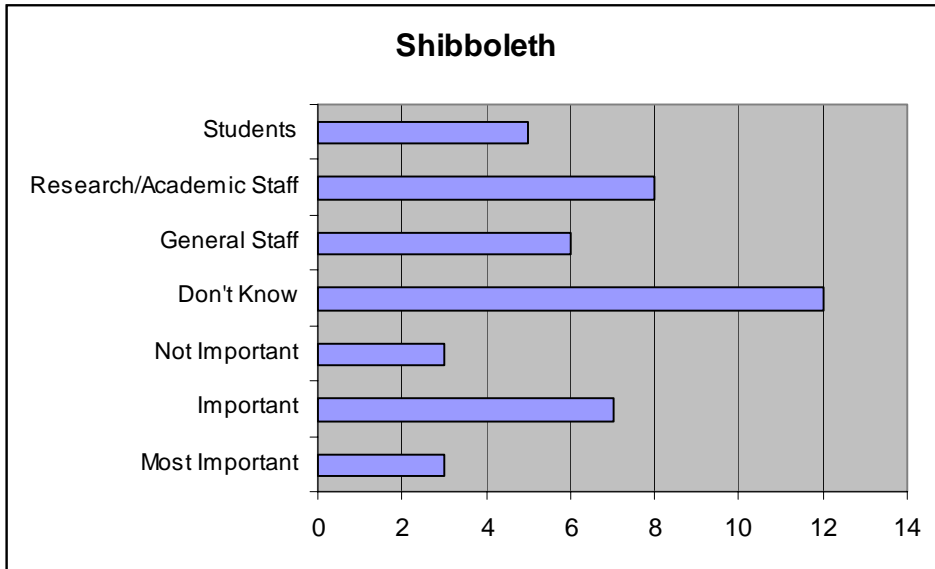






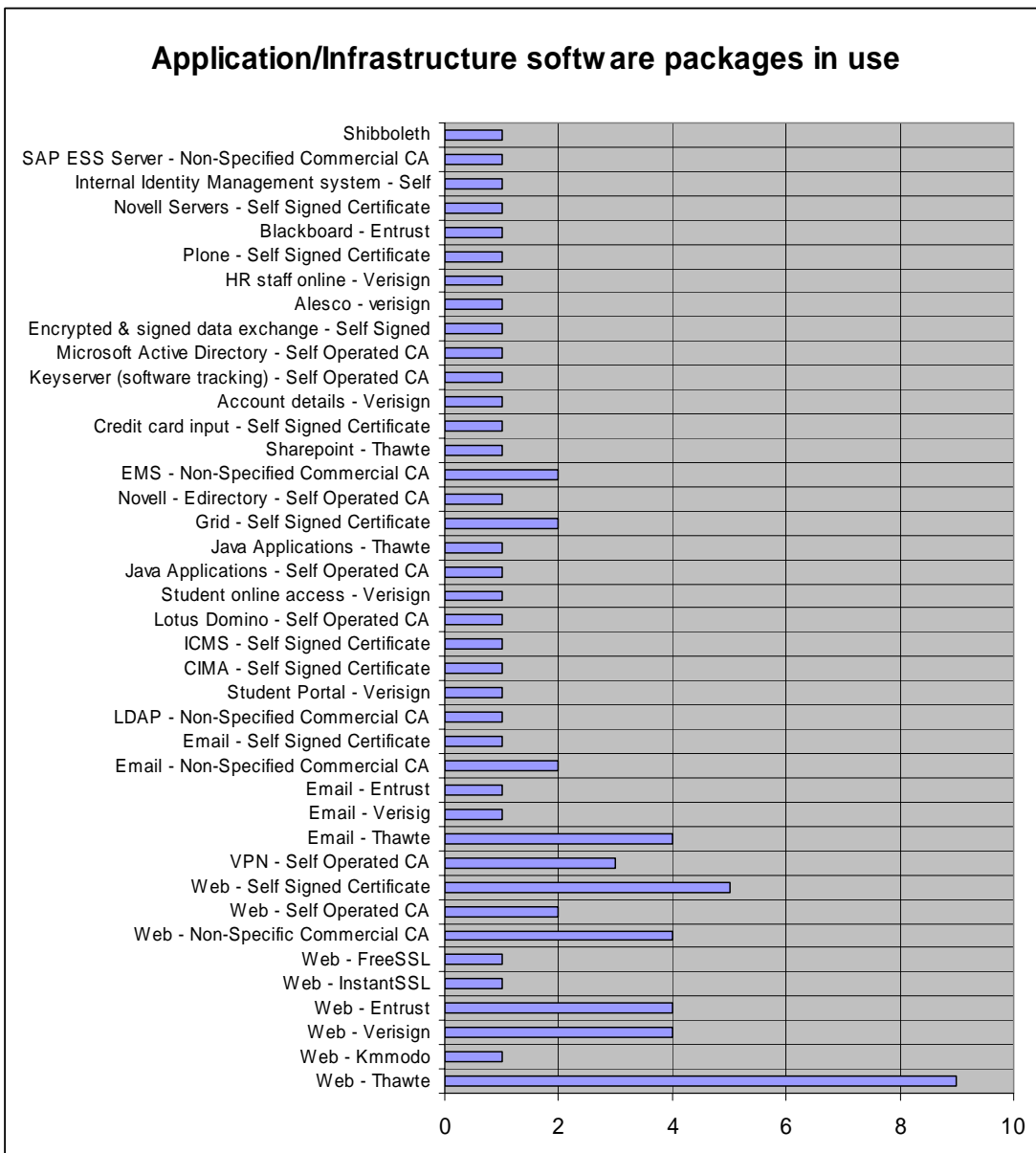






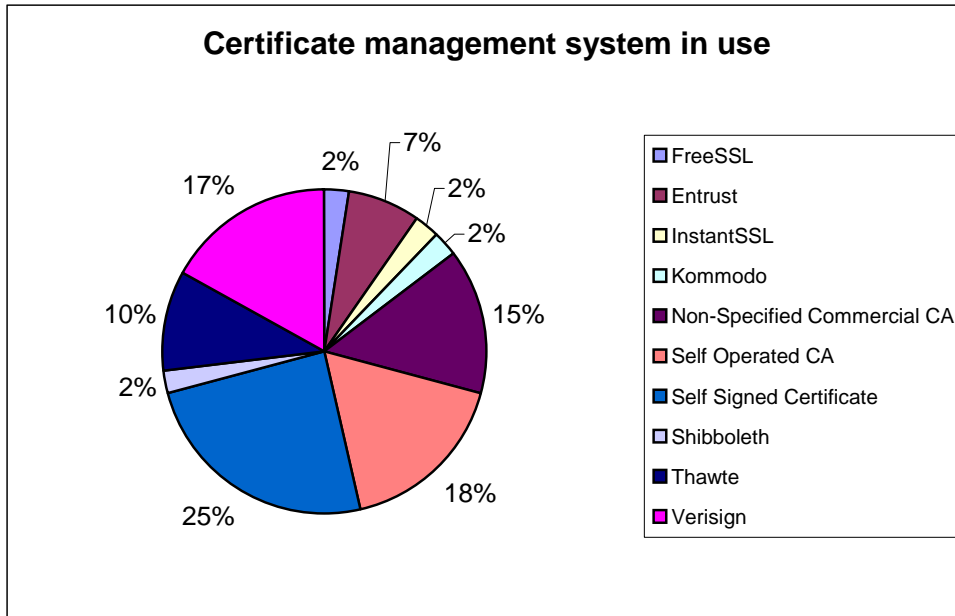
**Application/Infrastructure software packages currently in use**

Institutions were asked to list the application/infrastructure software packages currently in operation that use PKI certificates and mention if the certificates were issued by commercial, self operated CAs or self-signed. The following chart illustrates these applications and types of certificates used.

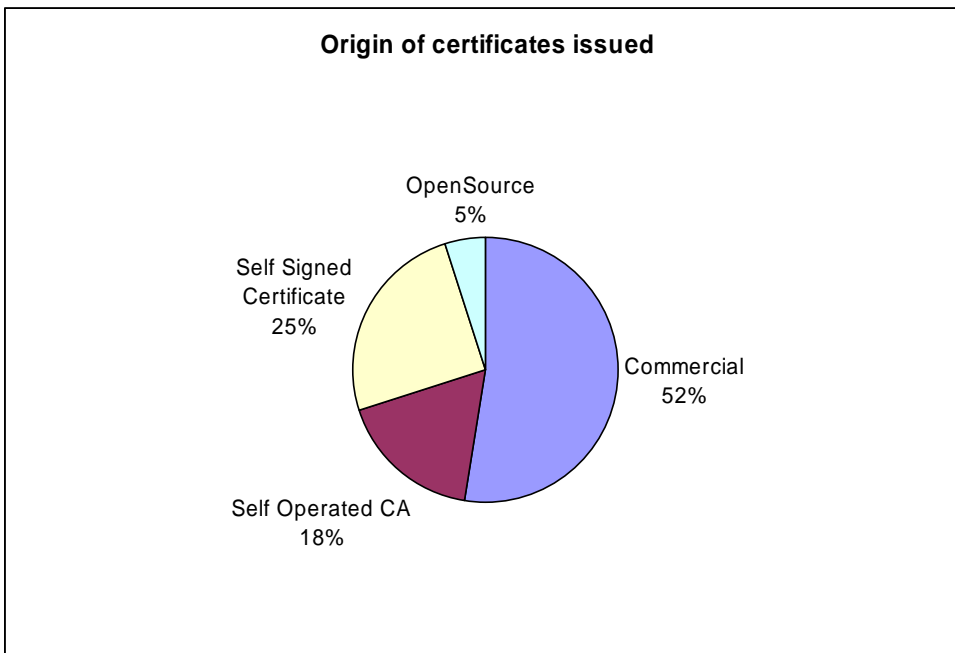


Please note that 'Web' includes servers, services, access, SSL, applications, Webmail, Ezproxy, and HTTPS. Email includes IMAP, POP, Exchange. Java Applications include signed Java code. EMS includes staff and student. Grid includes AccessGrid toolkit and GridSphere.

The chart below illustrates the ratio of commercial and non-commercial products being used by the sector.



Over 50% of the products used were commercial, with only 5% of OpenSource. It is unclear from the responses if the Self Signed Certificates and the Self Operated CAs use commercial or Open Source products.



## **Additional Comments**

This Survey asked for other comments or suggestions. The comments supplied here were rather diverse, but generally echoed the responses supplied earlier in the survey.

Some of these comments are summarised below.

It was indicated that:

- The need for a national position and solutions for PKI is critical for the future deployment of shared e-research infrastructure.
- There is a call for a more financially viable option to implement PKI, using bodies such as AusCERT. They also indicated the need for the Root certificate to be built into browsers such as IE and Firefox and MS applications.
- The costs for utilizing commercial CAs is prohibitive.
- The variety of key formats can be challenging at times.

## **Conclusion**

This Survey successfully accomplished its goal: to better understand the applications currently used by the higher education and research sectors.

The results of this survey provide valuable details that the eSecurity Framework sponsors, stakeholders and project team can use in developing an infrastructure that attends the ever increasing need for secure collaboration within the sector and infrastructure operation of individual universities.