

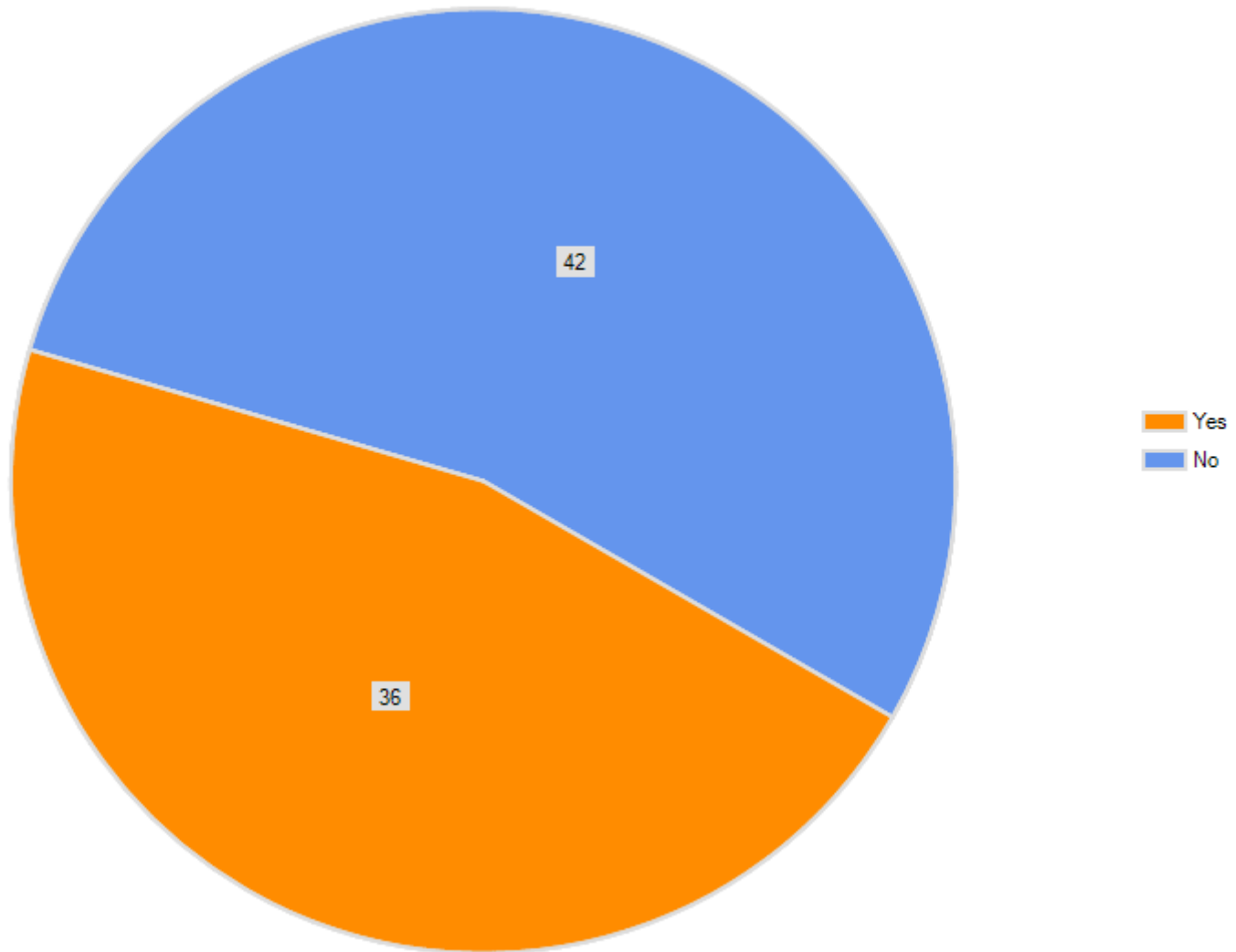
# InCommon Survey on Campus Use of 2-Factor Authentication

Final Results  
November 16, 2011

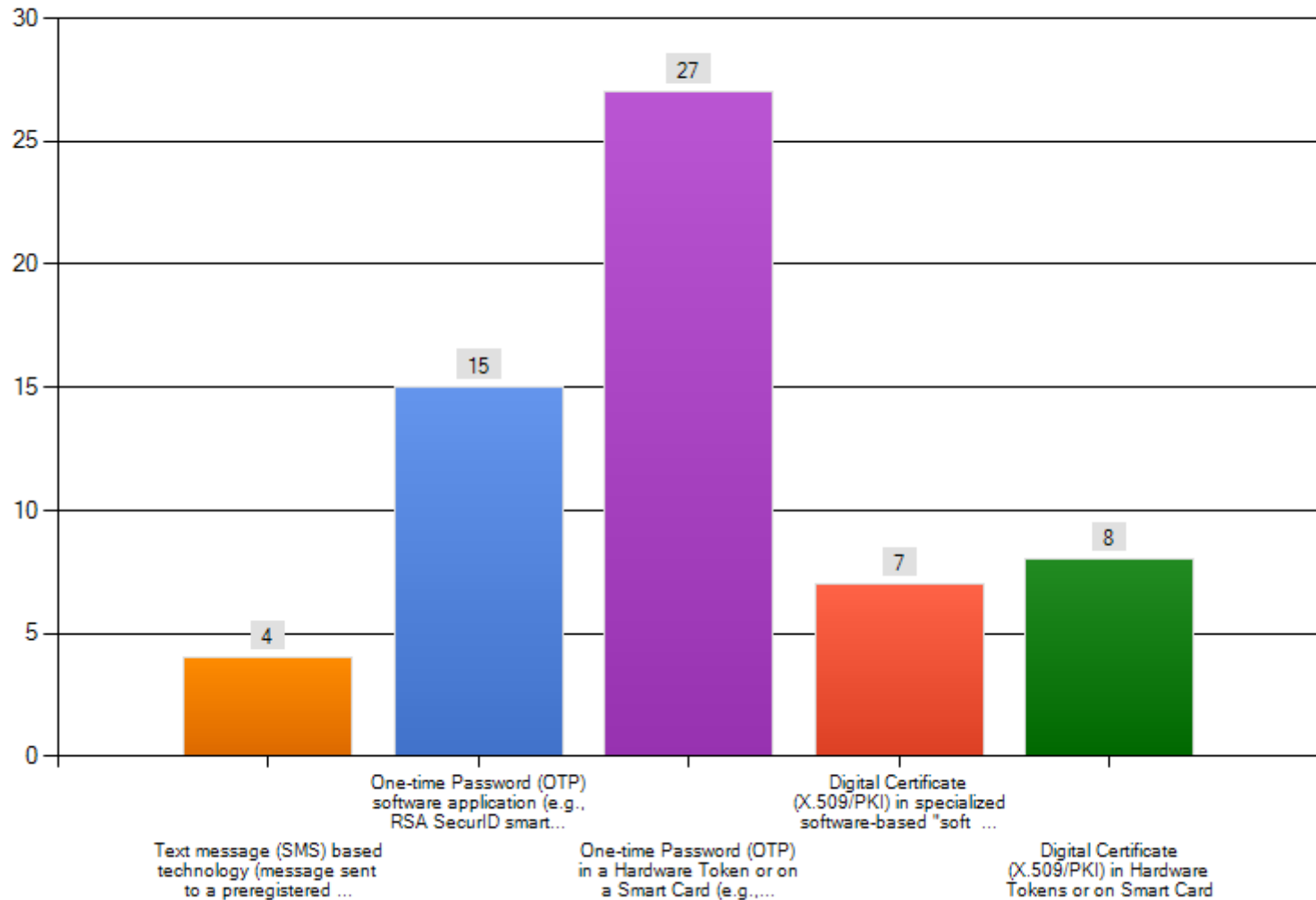
# Survey Demographics

Name	Count	Average	Median	Min	Max
Employees	82	9,261	6,000	500	40,000
Students	82	27,274	25,000	1,800	107,160
2-factor AuthN campus users	36	887	125	4	9,000
Annual \$ for 2- factor AuthN	28	22,418	5,500	0	200,000

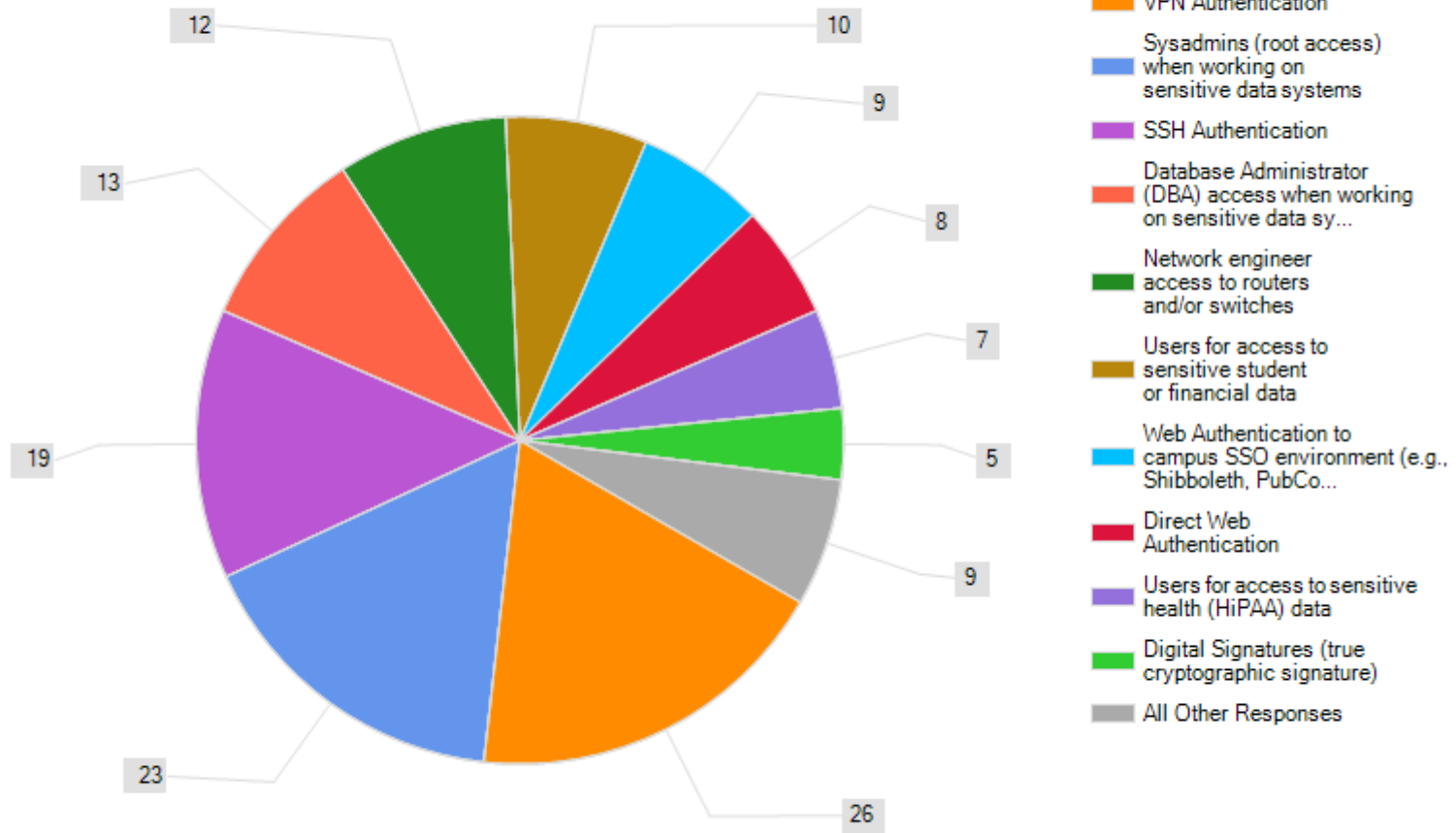
**Do you presently employ 2-factor authentication on your campus?**



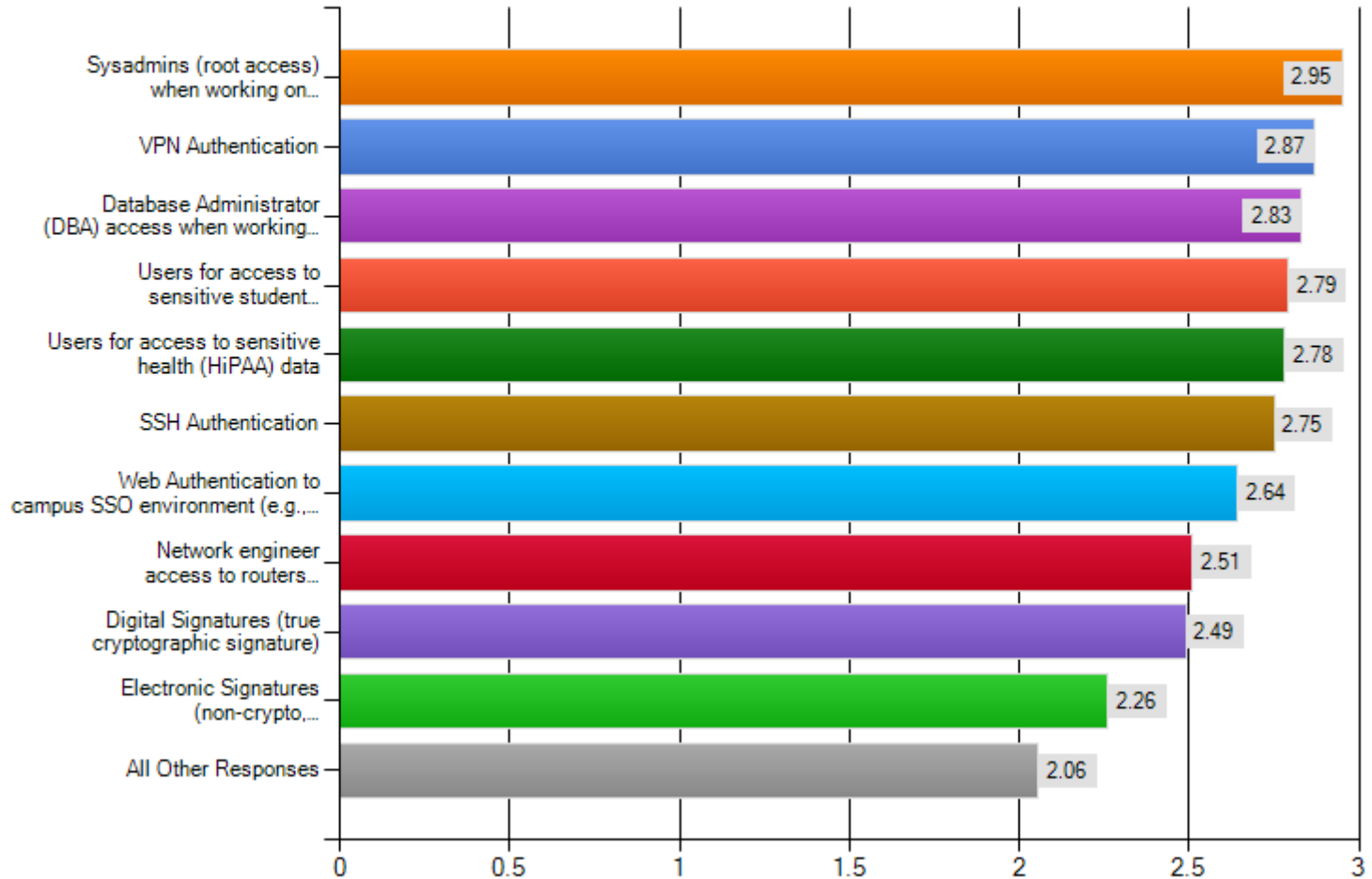
**If you presently employ 2-factor authentication on your campus, please tell us what type of technology you employ (please select all that apply)**



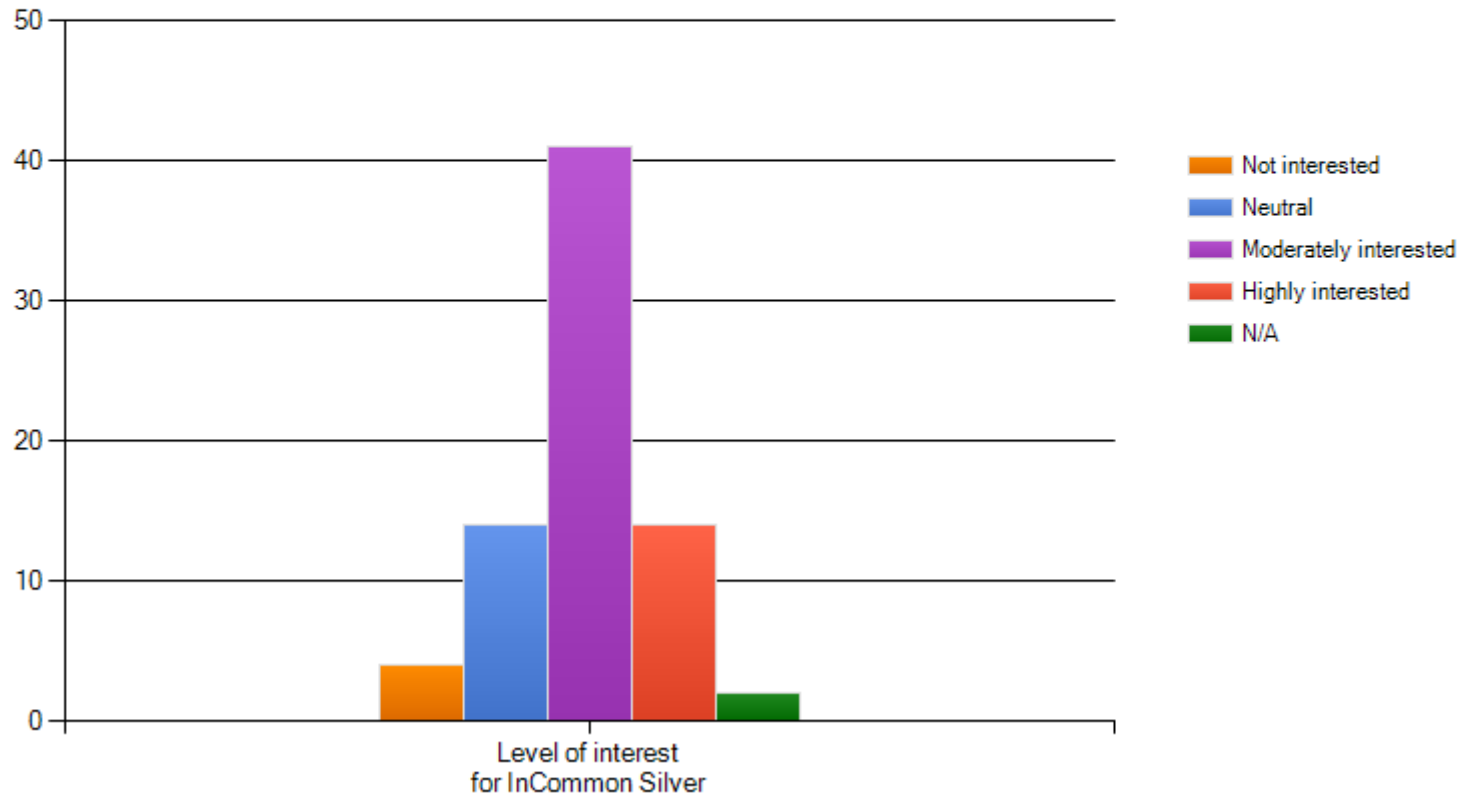
**If you presently employ 2-factor authentication on campus, please identify which applications, services, or user populations leverage the technology. Please check all that apply even if not all instances of a particular environment require 2-factor authentication.**



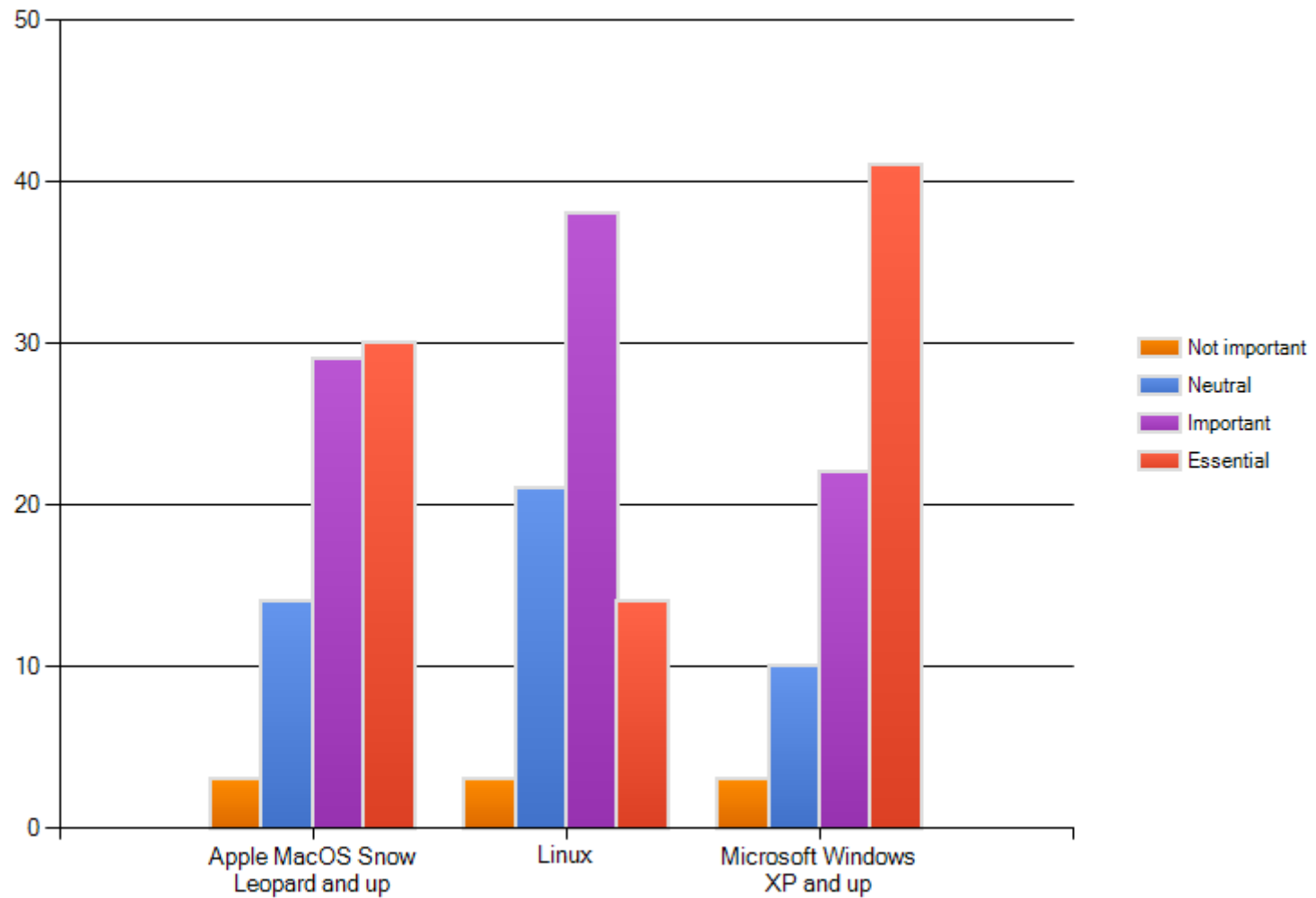
**Campus Use: Under a scenario where InCommon makes a certificate-based token solution available that includes integration with the Comodo CA, provisioning of tokens and token management (password resets, etc), please rate the likelihood that your campus would deploy the technology. Please rate the likelihood for each of the common campus 2-factor authentication applications listed below.**



**InCommon Service Use: How interested might your campus be in leveraging a complete solution for using InCommon Certificates and hardware tokens to meet the requirements of InCommon Silver? The solution would include integration with the Comodo CA, token provisioning and management, and the components, policy, and procedures needed to implement InCommon Silver. Additional information on InCommon Silver is available at <http://www.incommon.org/assurance/> This could be for a permanent solution or as an interim plan while the other components of the campus IdM system are addressed to meet InCommon Silver.**

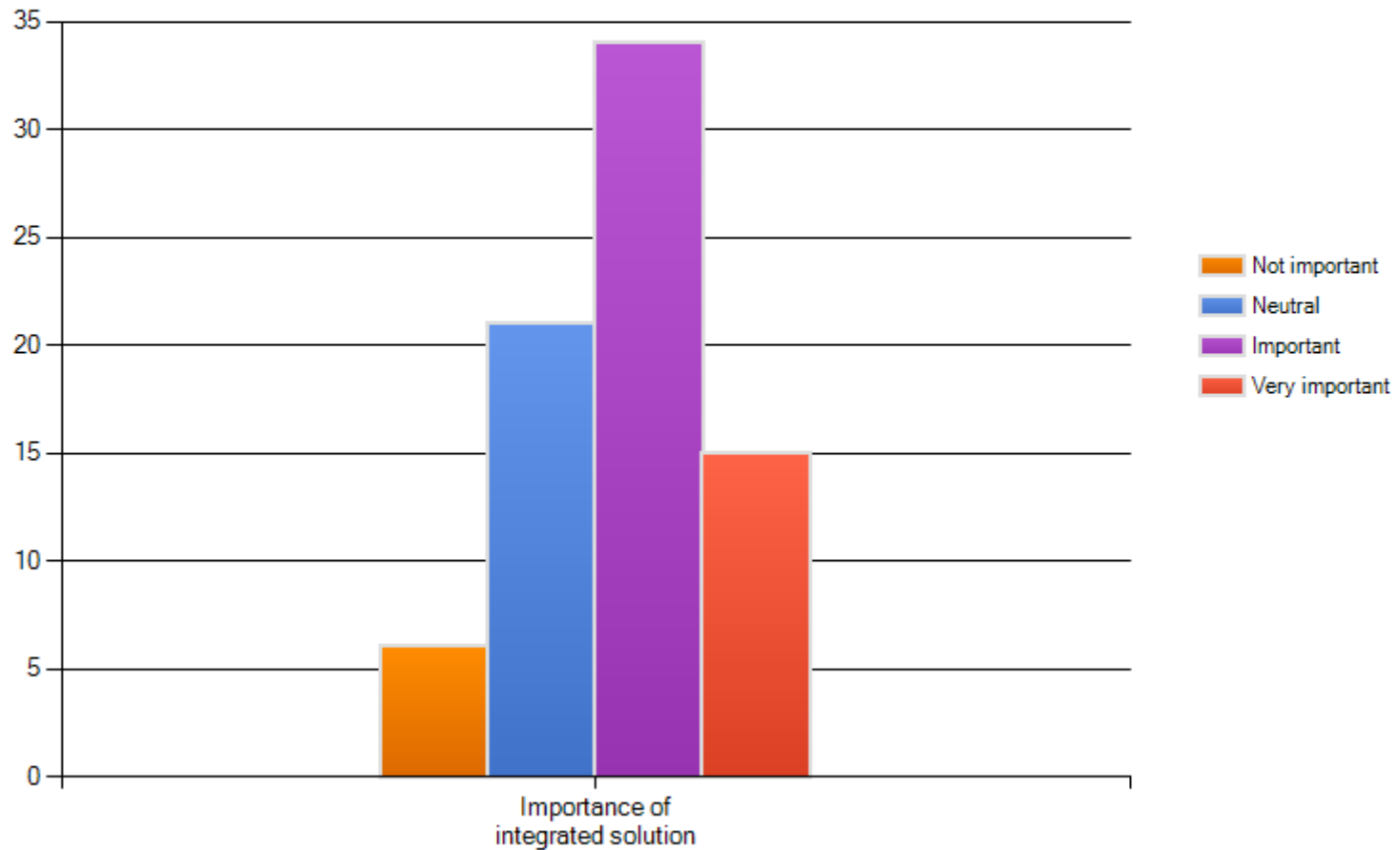


### Campus Use: How important is PKI hardware token support for the following Operating Systems?

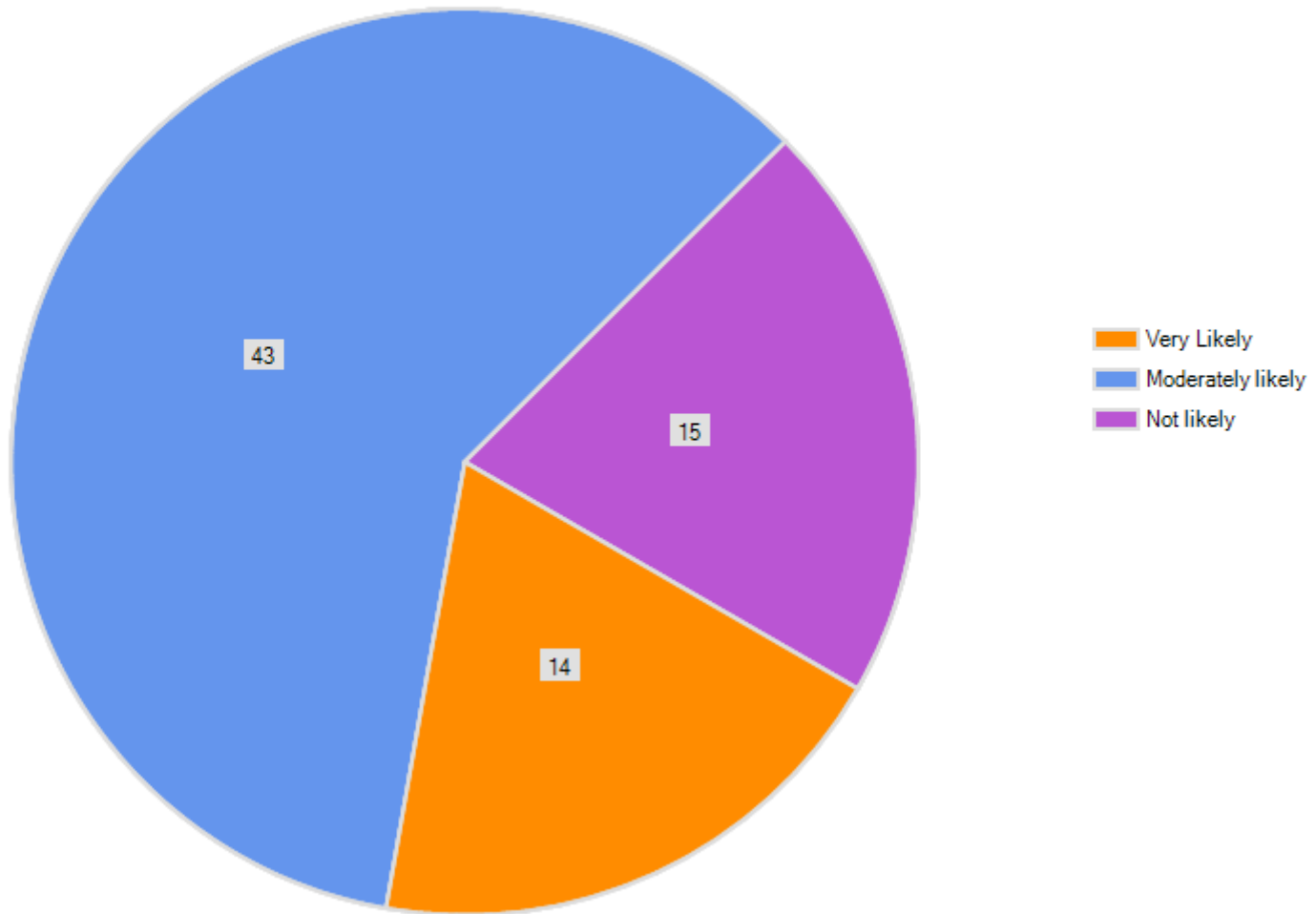




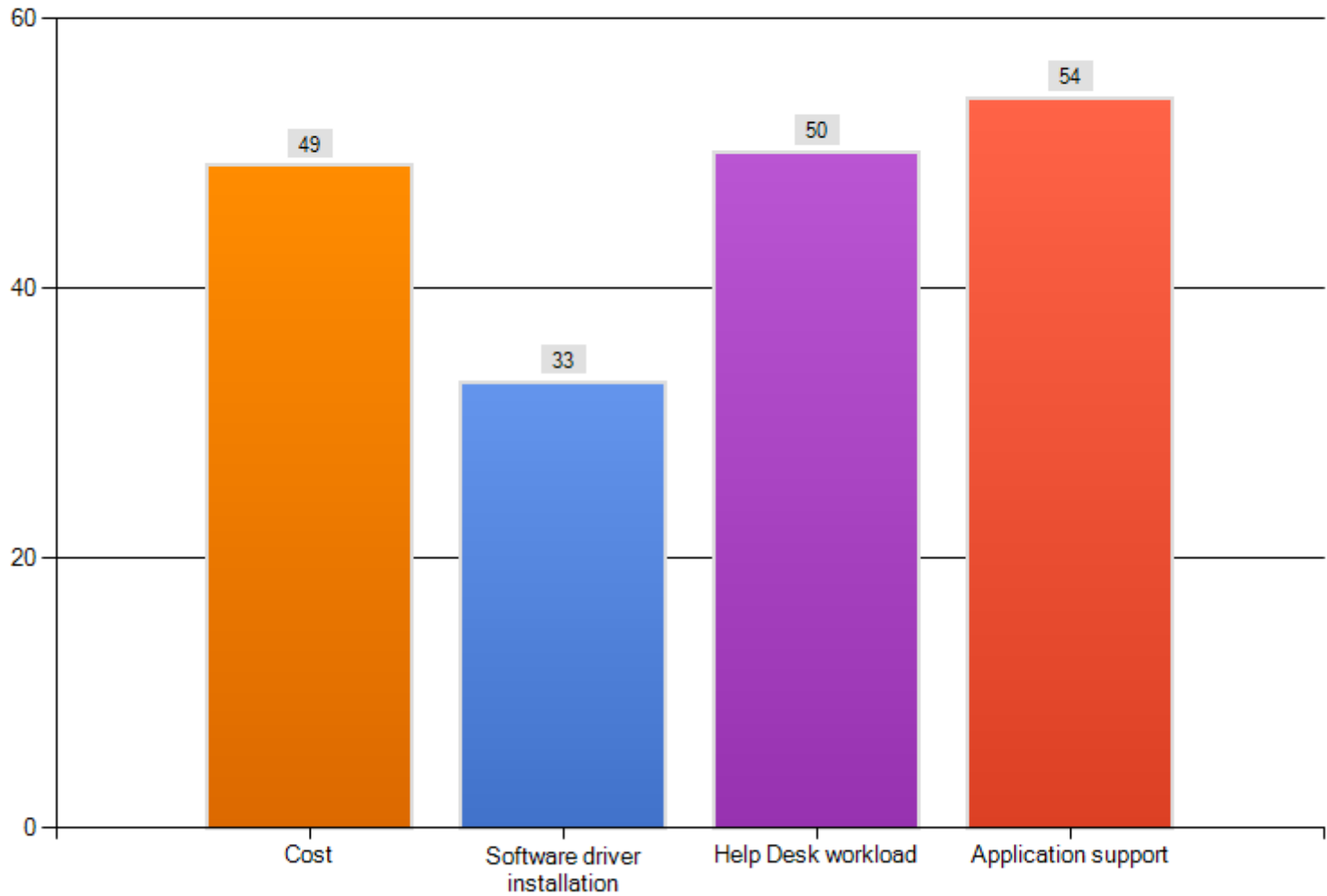
**Campus Use: Hardware tokens from different vendors typically require different management packages for provisioning, password reset, and other related functions. How important is it for adoption on your campus that any certificate-based hardware token be part of a compatible series of products, managed by a single management package, that cover the needs of a range of Levels of Assurance from soft or hard One Time Password (OTP) solutions through FIPS certified PKI hardware tokens?**



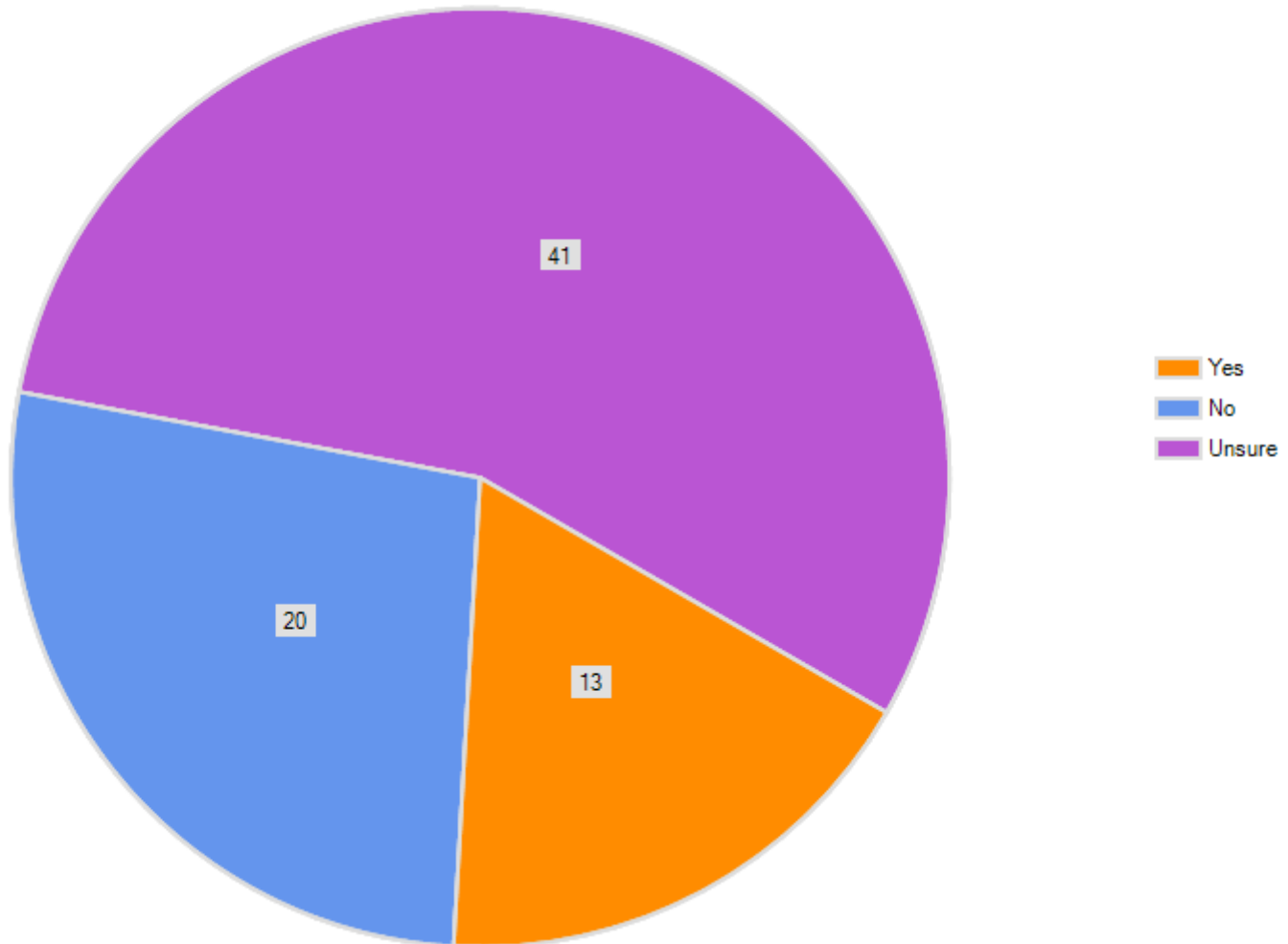
**Campus Use: If integration with the InCommon (Comodo) CA and/or hosted token management services are not important to your school, would your campus make use of a service that simply offered discounts on hard authentication tokens (assuming that such a contract could be negotiated)?**



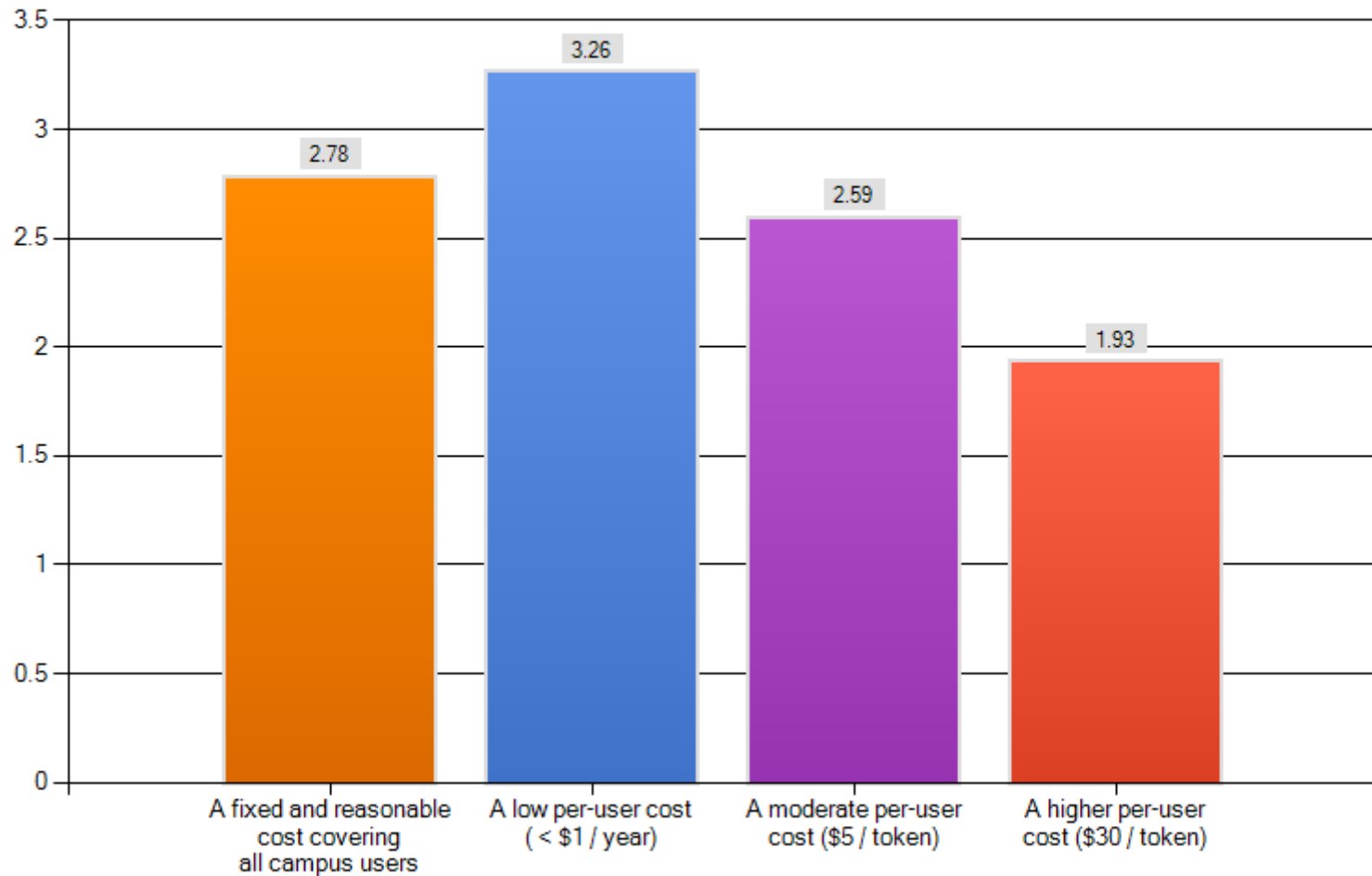
**What do you believe are the major issues, if any, that make the widespread adoption of 2-factor PKI-based token authentication difficult?**



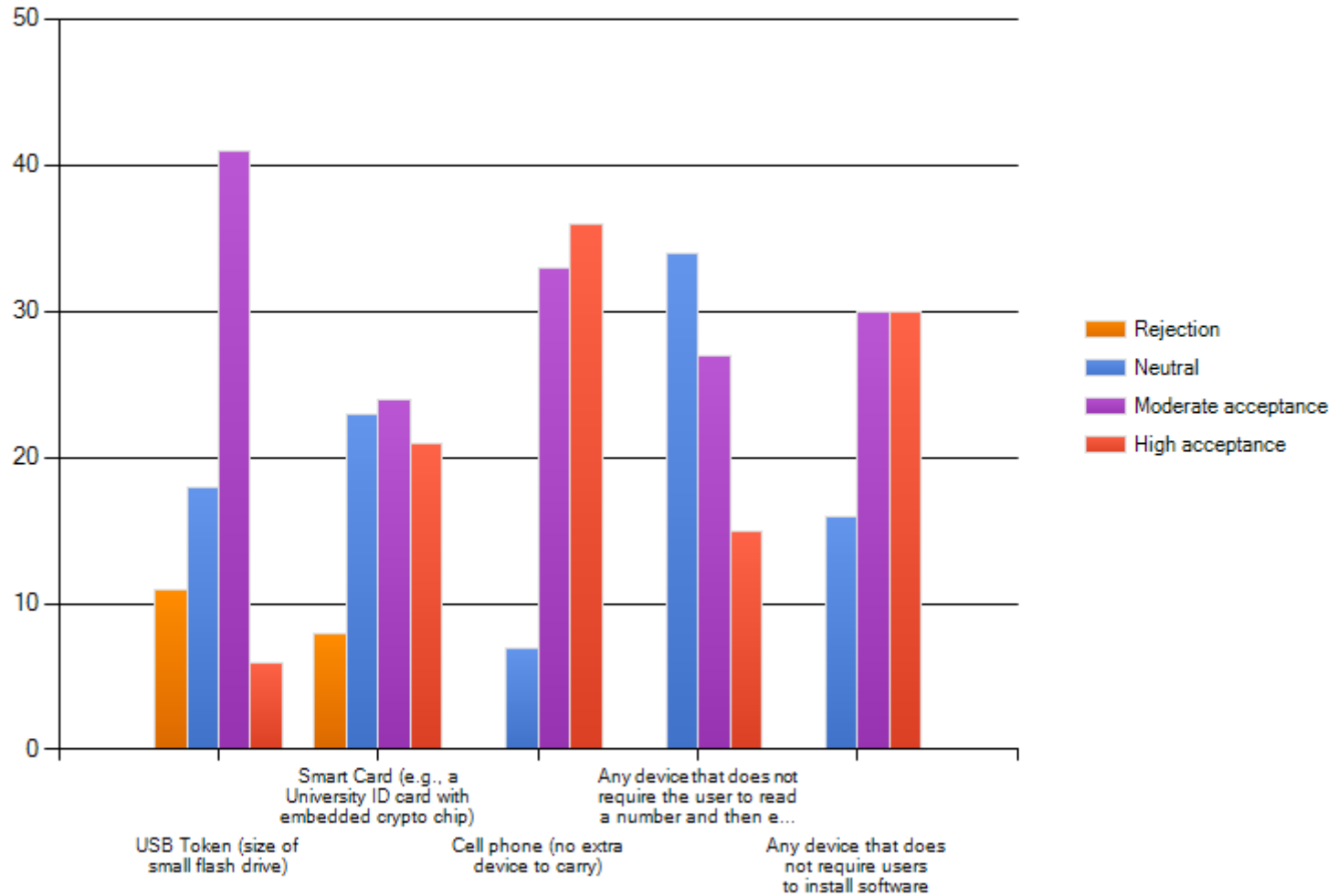
**If InCommon were able to negotiate contracts for hard tokens or other 2-factor authentication services, would your institution require that InCommon used a formal competitive rfp-style procurement in order to be able to use the contract(s)?**



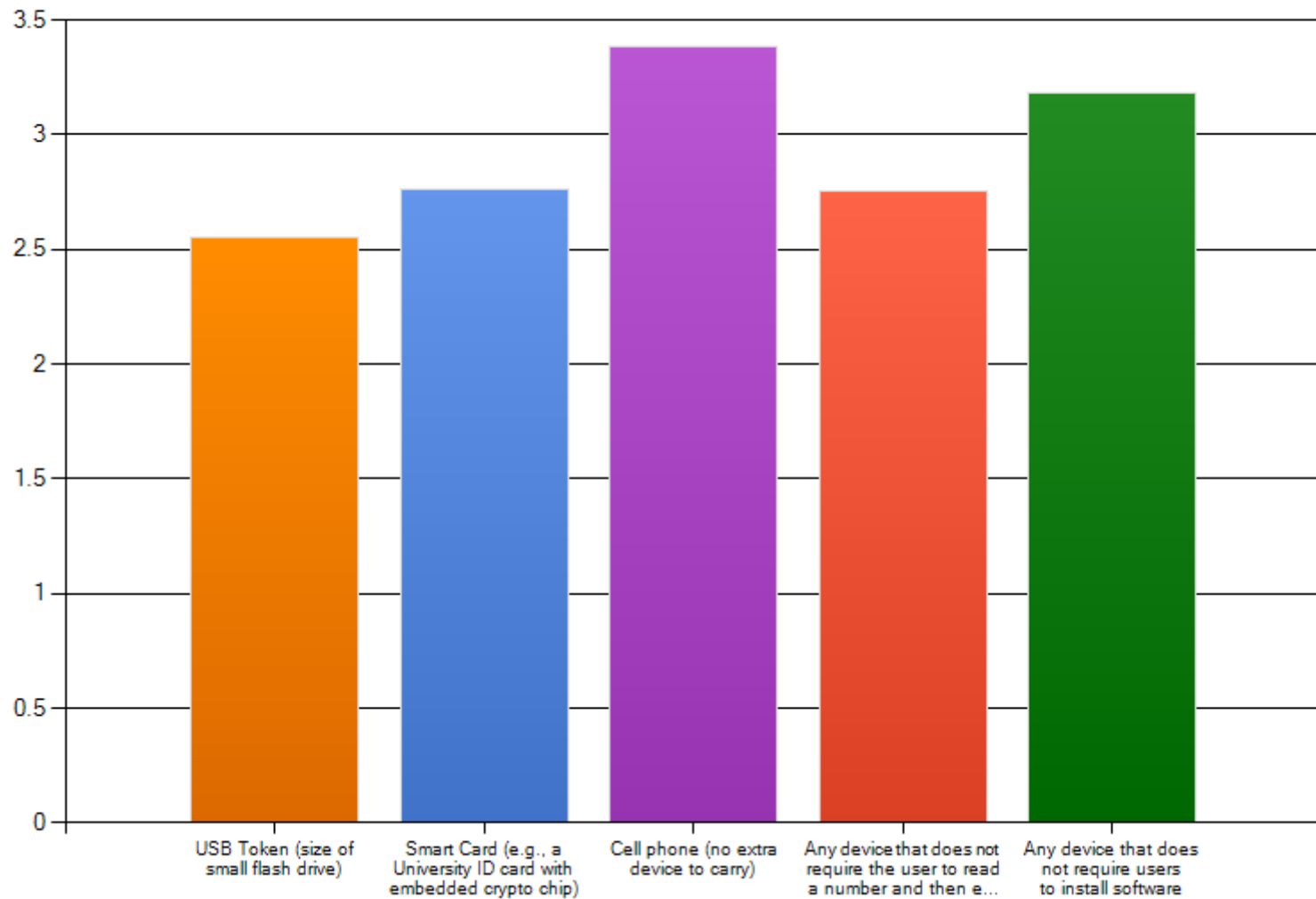
The cost of 2-factor authentication is often a barrier to widespread use on campus. Please speculate on the probability of the widespread use of 2-factor authentication on your campus under the following cost scenarios. By widespread, we mean that a significant portion of your employee and/or student population would use the service.



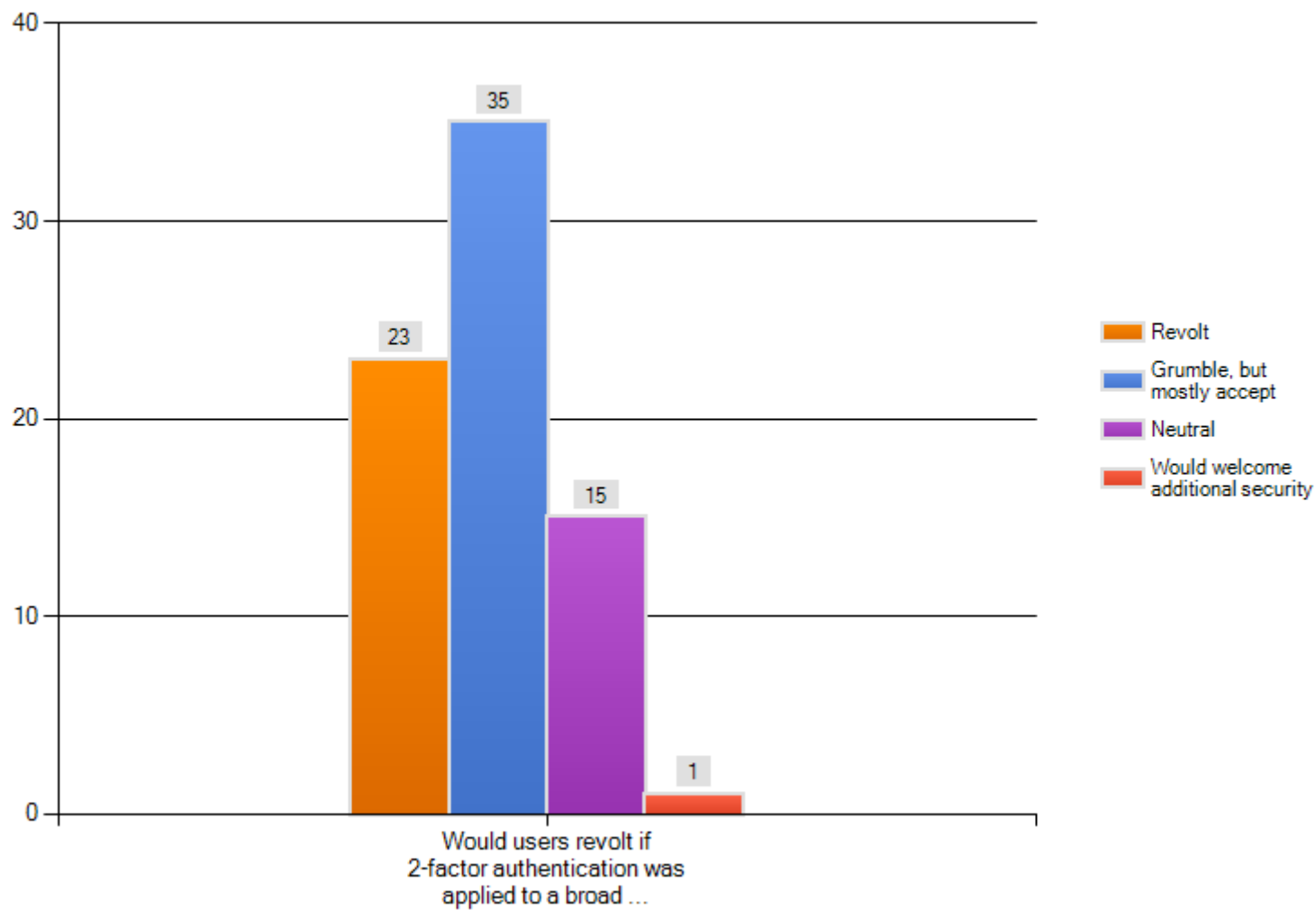
**In terms of user acceptance of a 2-factor authentication solution, please speculate on the potential level of user satisfaction for various types of devices.**



**In terms of user acceptance of a 2-factor authentication solution, please speculate on the potential level of user satisfaction for various types of devices.**



### To what degree is user inconvenience a major impediment to the broad deployment of 2-factor authentication?





Thinking in terms of the part of your user community who are likely to use 2-factor authentication, what percentage of them already carry smartphones (phones that are able to download common applications such as iPhone/iOS devices, Android, Blackberry, Windows Phone 7, etc)?

