

Identity Management



UNIVERSITY OF MINNESOTA

Outline of Presentation

- ***Passwords***
- ***Other Options***
- ***Background on the U of M Pilot Project***
- ***Other things to consider if implementing a 2 factor authentication tool with PKI***



Passwords

The most common method of authentication

*Are there ways we can
make passwords better?*



Steps that can be taken to directly affect password quality and password attacks

- ***Require passwords to include alpha and numeric characters***
- ***Require passwords to be a minimum length***
- ***Require passwords to be periodically changed***
- ***Require users to keep passwords in secure location if they need to write them down (e.g., their wallet)***
- ***Require users not to use the same password for all of the systems they have access to***



Steps that can be taken to directly affect password quality and password attacks

- ***Send out an e-mail to remind people to change their password if it has not been changed in over “x” period.***
- ***Send out an e-mail reminder prior to passwords expiring***
- ***Slow down the invalid password attempts to protect against brute force attacks.***
- ***Batch test password strengths (e.g., use word tests like John the Ripper) and then send e-mail to users of weak passwords to recommend they change to a stronger password.***



Steps that can be taken to directly affect password quality and password attacks

- ***Create an option on the password change screen to test password strength.***
- ***Use a password generation program to assist help line staff changing other staff's passwords***
- ***Display login history back to user.***
- ***Monitor intrusion logs***
- ***Establish a series of one-time passwords for use in cyber cafes/workstations not managed by the user***



Steps that can be taken to indirectly affect password attacks

- ***Require users to use secure e-mail clients.***
- ***Keep current on workstation patches and anti-virus updates.***
- ***Have a Security Awareness program, including putting responsibility for providing password on the end user and specific directions to not share the password with anyone.***
- ***Create a workstation pre-scan before allowing access to network applications.***



Steps that can be taken to indirectly affect password attacks

- ***Require scanning based on Network Registration (RegNet) for residence halls,***
- ***Require VPN (data encryption) for wireless access.***
- ***Install software to check workstations for spyware***



Risks

Compromises of authentication processes can result in compromised :

- Production data/ transactions or***
- Computer applications or***
- Servers and/or networks hosting computer applications***

***Passwords can be improved
but is that good enough?***

Are there other options?



Authentication Options

- ***User ID and Password***
- ***Hardware Token (SecurID)***
- ***Software Token***
- ***One Time Certificates***
- ***Digital Certificate***
- ***Smart Card + Digital Certificate***
- ***USB Token + Digital Certificate***



Some Key Evaluation Criteria

- *Confidence that authentication process will be effective*
- *Strategic Fit*
- *Cost*
- *Scalability*
- *Reliability*



RSA Rating of Options

	UserID / Password	RSA SecurID Hardware Tokens	RSA SecurID Software Tokens	RSA Mobile	Digital Certificates	Smart Cards + Certificates	Biometrics
Source: RSA Security product management							
Strategic Fit - Corporate Systems							
Relative Security	●	◎	◎	◎	◎	◎	◎
Interoperability/Back-End Integration	◎	◎	◎	◎	◎	◎	○
Robustness / Scale	●	◎	◎	◎	◎	◎	●
Future Flexibility	○	◎	◎	◎	◎	◎	●
Strategic Fit - Users							
Convenience/Ease of Use	●	◎	◎	◎	◎	◎	◎
Portability	●	●	◎	◎	●	◎	◎
Multi-Purpose	○	○	●	●	◎	◎	◎
Total Cost of Ownership (TCO)							
Acquisition Cost	↓	■	↓	↓	↓	■	■
Deployment Cost	↓	↓	↓	↓	↓	■	■
Operating Cost	↑	↓	↓	↓	↓	■	■

Key

Strategic Fit

●- Excellent

◎- Very Good

◎- Good

●- Adequate

○- Fair

Total Cost of Ownership

↑- Very High

↑- High

■- Medium

↓- Low

↓- Very Low



RSA Rating of Options

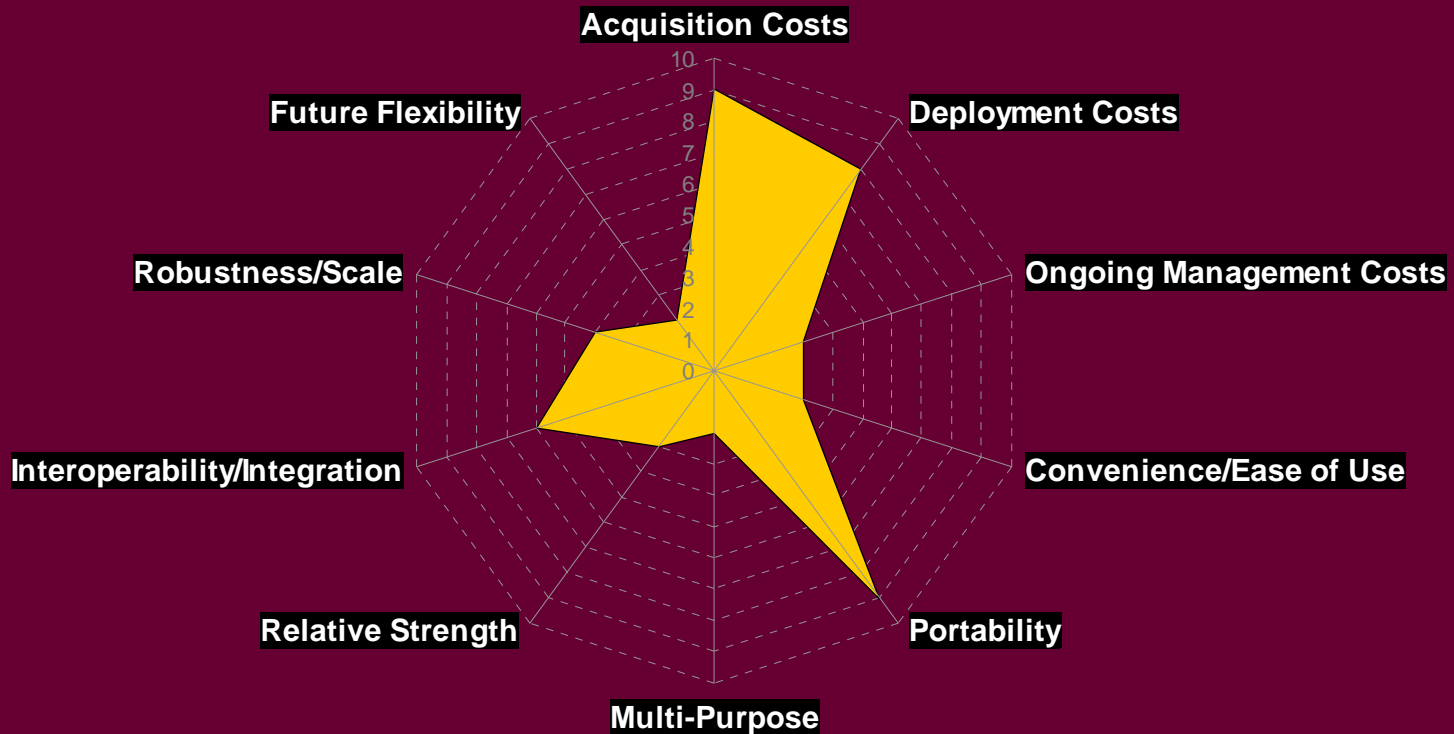
			Unweighted base rankings--rollover to learn more (high scores are better)																																																				
Category	Evaluation Criteria	Weight	UserID / Password	RSA SecurID Hardware Tokens	RSA SecurID Software Tokens	RSA Mobile	Digital Certificates	Smart Cards + Certificates	USB Tokens + Certificates																																														
Total Cost of Ownership	Acquisition Costs	10.0%	9	6	7	8	8	6	7																																														
	Deployment Costs	10.0%	8	7	6	8	8	6	7																																														
	Ongoing Management Costs	10.0%	3	8	7	7	7	6	6																																														
Strategic Fit (Users)	Convenience/Ease of Use	10.0%	3	8	7	7	7	7	7																																														
	Portability	10.0%	9	9	8	6	4	6	7																																														
	Multi-Purpose	10.0%	2	3	4	4	6	8	7																																														
Strategic Fit (System)	Relative Strength	10.0%	3	8	8	8	5	8	8																																														
	Interoperability/Integration	10.0%	6	7	6	5	5	5	5																																														
	Robustness/Scale	10.0%	4	7	7	7	8	8	8																																														
	Future Flexibility	10.0%	2	5	5	5	8	8	8																																														
Weighted Scores:		100.0%	4.90	6.80	6.50	6.50	6.60	6.80	7.00																																														
<table border="1"> <thead> <tr> <th>SUMMARY</th> <th>Weight</th> <th>UserID / Password</th> <th>RSA SecurID Hardware Tokens</th> <th>RSA SecurID Software Tokens</th> <th>RSA Mobile</th> <th>Digital Certificates</th> <th>Smart Cards + Certificates</th> <th>USB Tokens + Certificates</th> </tr> </thead> <tbody> <tr> <td>Total Cost of Ownership</td> <td>30.0%</td> <td>2.0</td> <td>2.1</td> <td>2</td> <td>2.3</td> <td>2.3</td> <td>1.8</td> <td>2</td> </tr> <tr> <td>Strategic Fit (Users)</td> <td>30.0%</td> <td>1.4</td> <td>2</td> <td>1.9</td> <td>1.7</td> <td>1.7</td> <td>2.1</td> <td>2.1</td> </tr> <tr> <td>Strategic Fit (System)</td> <td>40.0%</td> <td>1.5</td> <td>2.7</td> <td>2.6</td> <td>2.5</td> <td>2.6</td> <td>2.9</td> <td>2.9</td> </tr> <tr> <td colspan="2">Weighted Scores:</td> <td>100.0%</td> <td>4.9</td> <td>6.8</td> <td>6.5</td> <td>6.5</td> <td>6.6</td> <td>6.8</td> <td>7.0</td> </tr> </tbody> </table>										SUMMARY	Weight	UserID / Password	RSA SecurID Hardware Tokens	RSA SecurID Software Tokens	RSA Mobile	Digital Certificates	Smart Cards + Certificates	USB Tokens + Certificates	Total Cost of Ownership	30.0%	2.0	2.1	2	2.3	2.3	1.8	2	Strategic Fit (Users)	30.0%	1.4	2	1.9	1.7	1.7	2.1	2.1	Strategic Fit (System)	40.0%	1.5	2.7	2.6	2.5	2.6	2.9	2.9	Weighted Scores:		100.0%	4.9	6.8	6.5	6.5	6.6	6.8	7.0
SUMMARY	Weight	UserID / Password	RSA SecurID Hardware Tokens	RSA SecurID Software Tokens	RSA Mobile	Digital Certificates	Smart Cards + Certificates	USB Tokens + Certificates																																															
Total Cost of Ownership	30.0%	2.0	2.1	2	2.3	2.3	1.8	2																																															
Strategic Fit (Users)	30.0%	1.4	2	1.9	1.7	1.7	2.1	2.1																																															
Strategic Fit (System)	40.0%	1.5	2.7	2.6	2.5	2.6	2.9	2.9																																															
Weighted Scores:		100.0%	4.9	6.8	6.5	6.5	6.6	6.8	7.0																																														



Authentication Scorecard

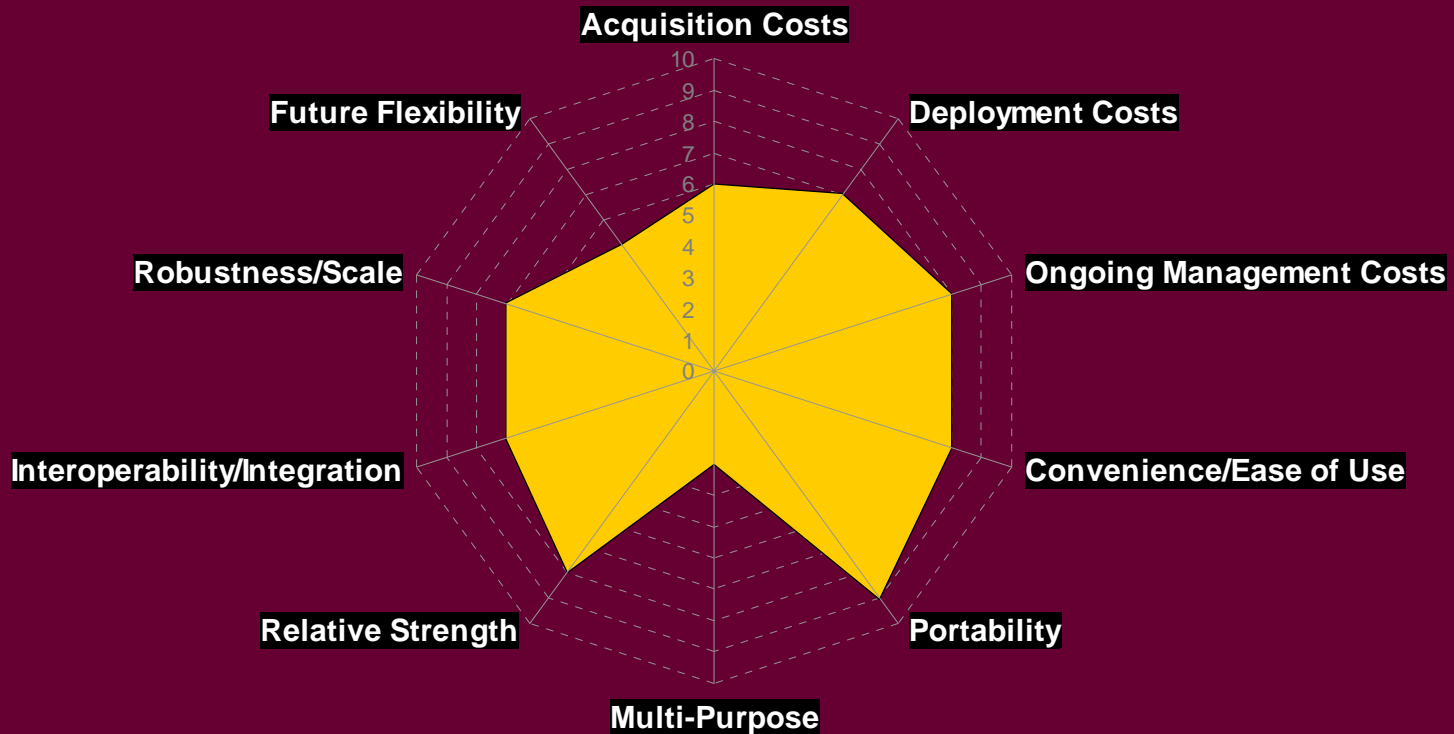
UserID / Password

Source: RSA Security product management



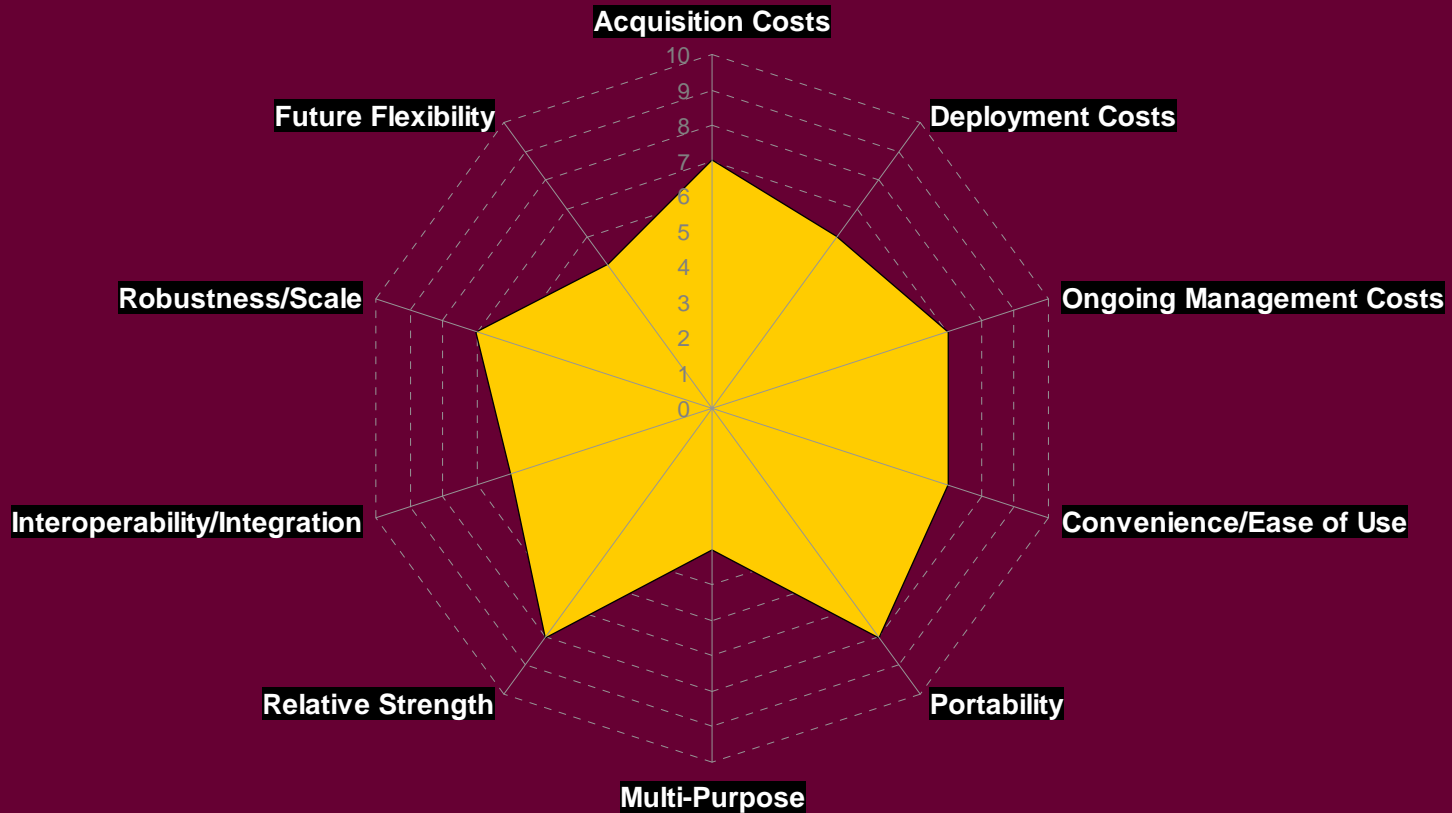
Authentication Scorecard Hardware Tokens

Source: RSA Security product management



Authentication Scorecard Software Tokens

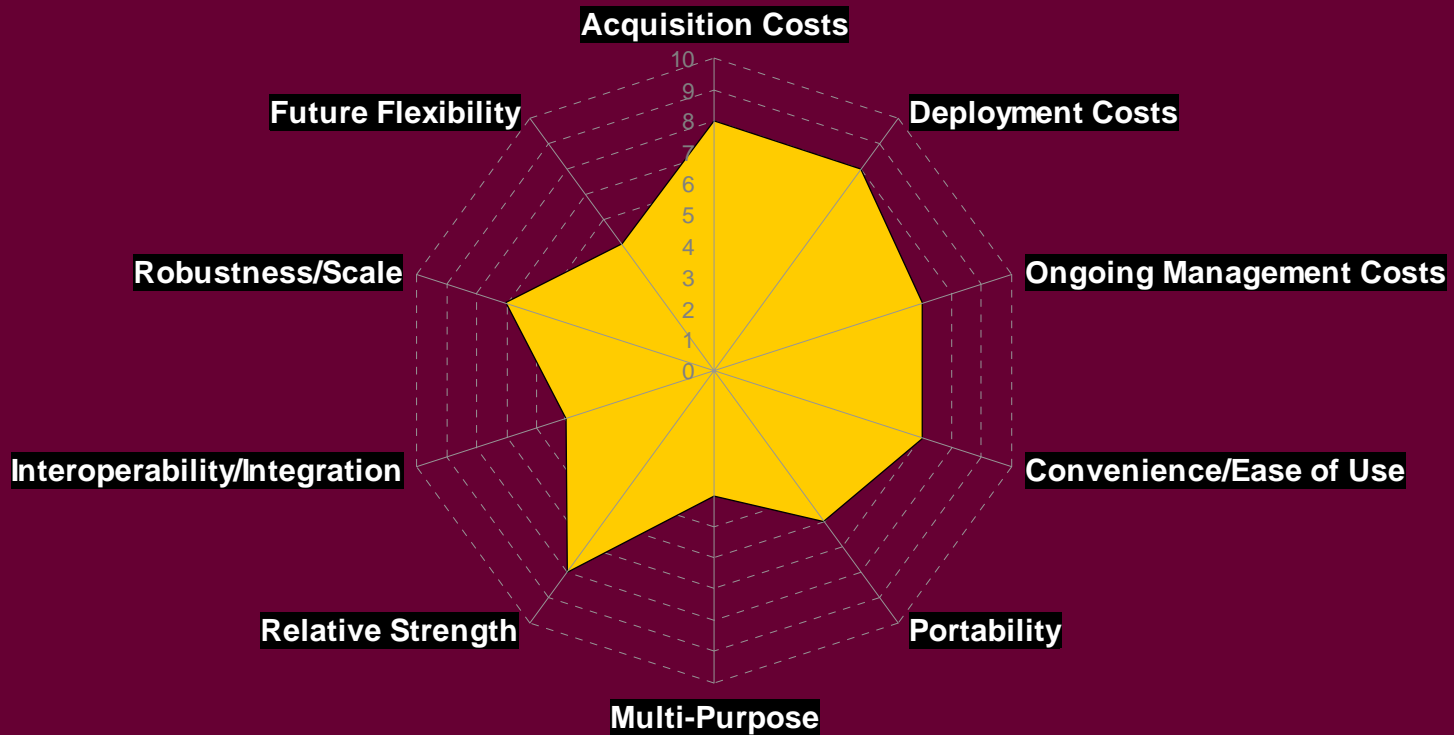
Source: RSA Security product management



Authentication Scorecard

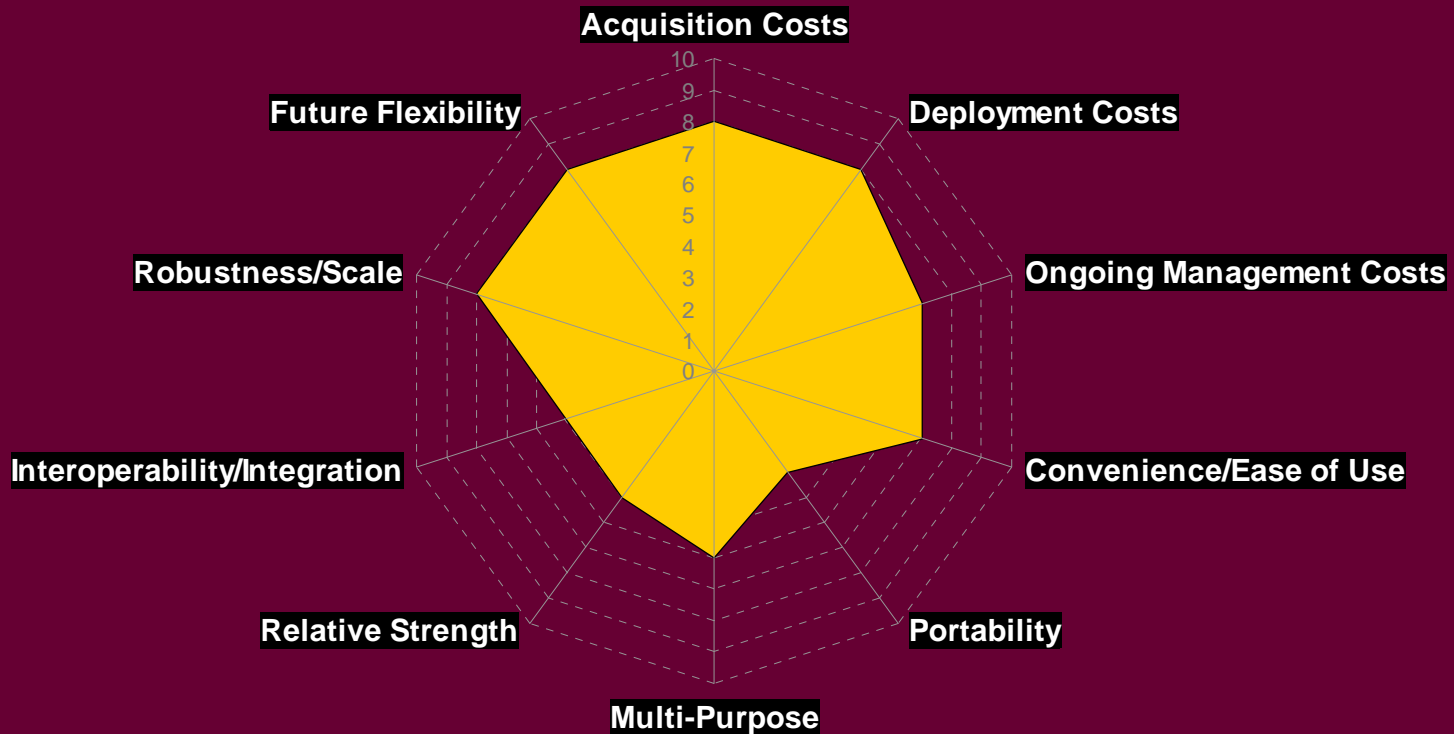
RSA Mobile (One Time Passwords)

Source: RSA Security product management



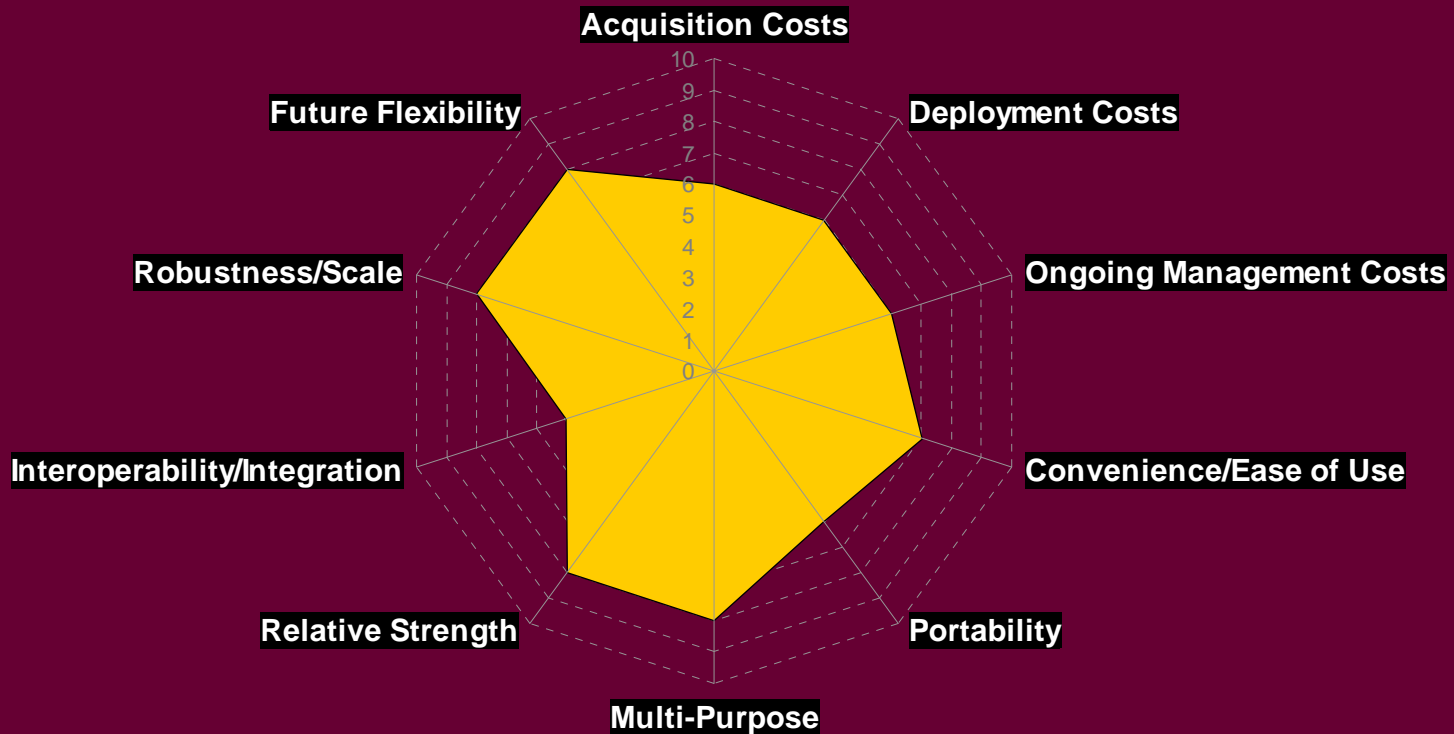
Authentication Scorecard Digital Certificates

Source: RSA Security product management



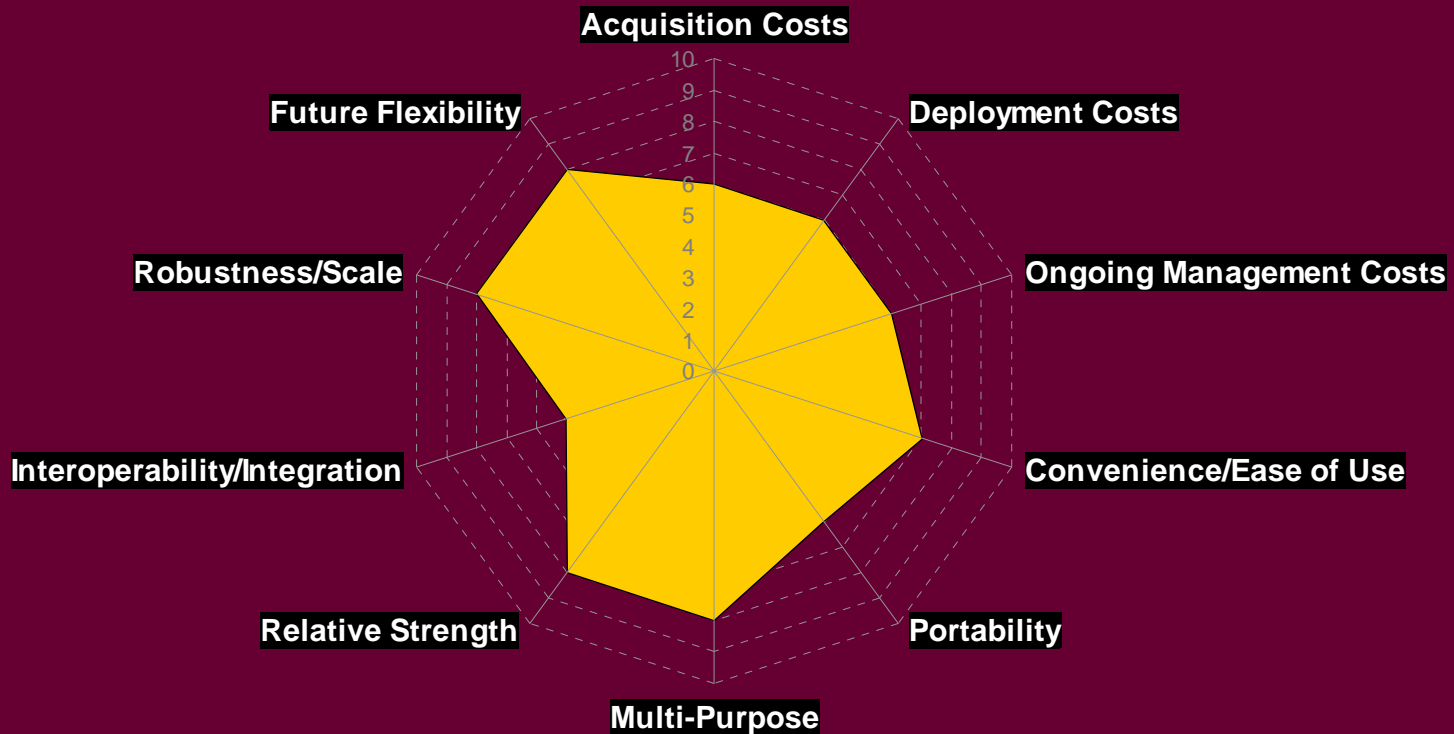
Authentication Scorecard Smart Cards

Source: RSA Security product management



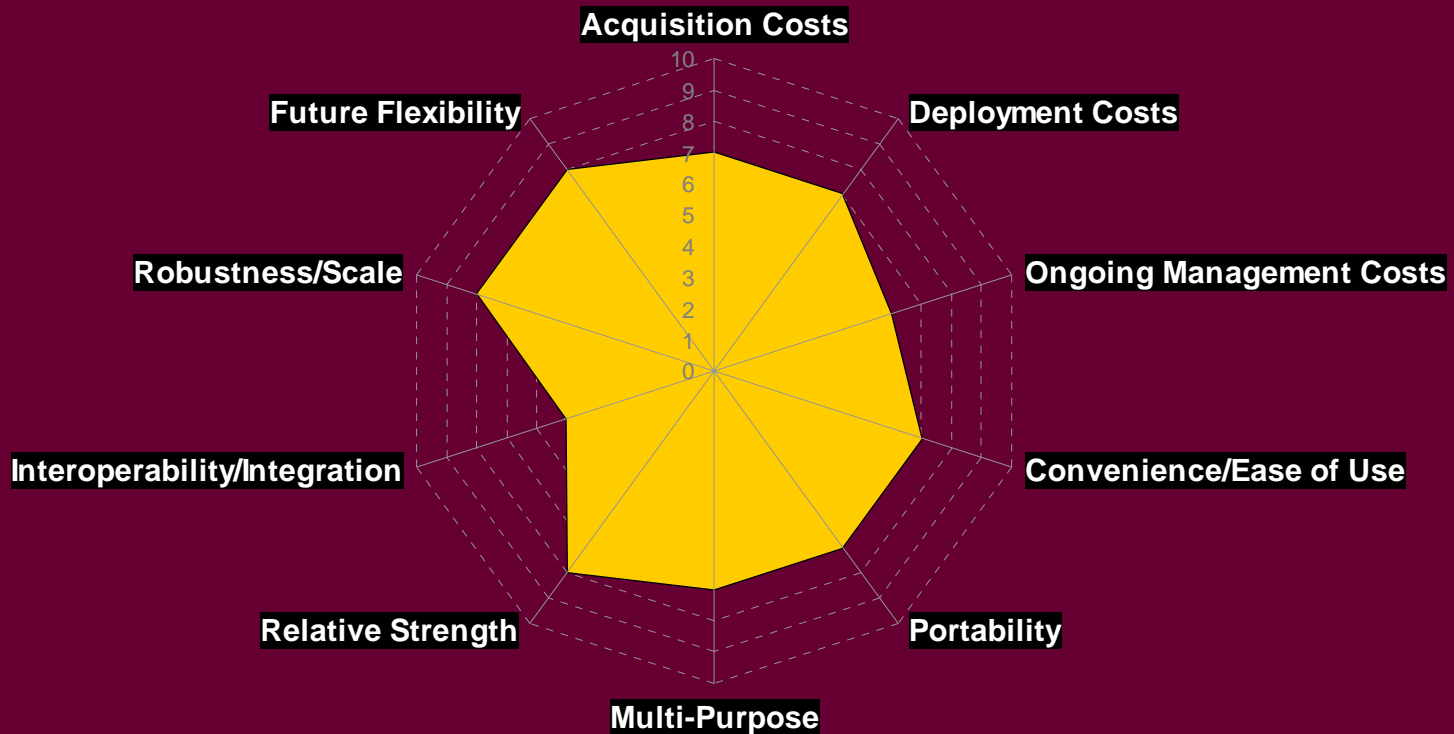
Authentication Scorecard Smart Cards + Certificates

Source: RSA Security product management



Authentication Scorecard USB Tokens + Certificates

Source: RSA Security product management



About the U of M Pilot Project

- ***Beginning a proof of concept project***
- ***Testing 2-factor authentication using a USB token and PKI***
- ***Pilot will use PKI certificates created, registered and managed by the U of M***
- ***Pilot will leverage the U of M's existing directory***
- ***Pilot will test concepts for authentication of users of WEB based applications***



Overall Goals

- *Provide better authentication controls for some of our most critical applications and computer processes*
- *Provide a tool that is easy to use and scalable*
- *Provide a tool that can be integrated into existing infrastructure*

(Goal should not necessarily be “one size fits all” user authentication)



Expected Benefits For U of M

- ***Provide higher assurance that only authorized users are accessing key systems at the U of M***
- ***Help us address compliance requirements of HIPAA, FERPA, GLB, and VISA CISP***
- ***Help reduce attacks like the ones against super computer installations (i.e., like the attack Stanford described)***
- ***Make user sign on to multiple U of M applications easier (i.e., help us move a little closer to the feel of single sign-on)***



Pilot Project Plans

- ***Implement 2-factor authentication using PKI for a pilot group of University users.***
- ***Monitor external PKI developments (e.g., HEPKI group, USHER) which impact viability of PKI solutions.***
- ***Evaluate the results of the pilot and make recommendations for future expansion or alternatives.***



Decisions Needed for Pilot Project

- ***What functionality is in scope***
- ***What functionality is out of scope***
- ***Expectations for authentication of person's identity before certificate is registered***
- ***Processes needed for initial roll-out vs. ongoing use***
- ***Processes needed for re-issue of certificates***



Decisions Needed for Pilot Project

- ***Hardware that will be used***
- ***Desktop hardware and software (OS and Browsers) with which the solution must work with***
- ***Applications that will be used to test concept***
- ***Roll-back strategy***
- ***Specific testing objectives***
- ***Testing strategy***
- ***Length of pilot***
- ***Staff who will be involved in the pilot***



Possible Future Uses of Certificates

- ***Authenticating to email systems***
- ***Object code signing/Digitally signing documents***
- ***Use for encrypting and decrypting data***
- ***Authenticating to server operating systems (e.g., Unix or Linux)***
- ***Facilitating single sign on capabilities***



Other Things To Think About When Implementing PKI

- ***Certificate Lifecycle***
- ***User Authentication Process Before Issuing Certificate***
- ***Types of Certificates***
- ***Certificate Construction***
- ***Security and Management of CA certificates***
- ***Strategies for Roll Back if CA or RA is compromised***
- ***Audit Trail Requirements***



Certificate Life Cycle

- ***Initial Roll-out***
- ***On-going Use***
- ***Revocation Inactivation***
- ***Re-Issue***

***(Inactivate certificate vs.
revocation of certificate)***



User Authentication Process Before Issuing Certificate

- ***Use previous authorization (e.g., password)***
- ***Use shared secrets (e.g., SSN)***
- ***Authorization from another user***
- ***Presentation of derivative identify information (e.g., University ID)***
- ***Presentation of trusted base identify information (e.g., drivers license or passport)***



Types of Certificates

- *Authentication key*
- *Key for signing email (S/Mime signing)*
- *Encryption key*



Certificate Construction

- *Bind ID data*
- *Identifiable ID information (e.g., email address)*



Security and Management of CA Certificates

- ***Where to get root certificate***
- ***How many levels of CA certificates are needed***
- ***How many branches of CA certificates are needed***
- ***Should certificates have a short or long expiration time frame***
- ***Where is root certificate kept***
- ***Should CA be on-line or off-line***



Strategies for Roll Back If CA or RA is compromised

- ***Use of single or multiple branches of certificates***
- ***Use of directory (published or unpublished certificates)***



Audit Trails

- *On CA*
- *On RA*
- *On certificate challenge process*
- *On evaluation of certificate*
- *On comparison of cookie to services table*
- *On use of cookie with WEB application*
- *On revocation process or inactivation process*





The Aladdin eToken NG - OTP hybrid token is a 2-in-1 device, incorporating state-of-the-art smart card technology for usage with PKI/digital certificates AND a one-time-password(OTP). The PKI functions are primarily used for digital signing, encryption and securing access to personal/corporate/network resources. The OTP functions are used to secure access to network resources.

eToken NG - OTP is a highly flexible and versatile device, enabling a variety of authentication and security related solutions including PKI authentication, Static passwords and One-Time password. By supporting multiple strong authentication methods, the same device becomes capable of dealing with a wide range of networks, applications and customer needs.

The following remote access scenario illustrates the benefit of integrating multiple authentication methods into a single security device. With eToken NG - OTP, an organization can strongly authenticate user access to the network using Microsoft's Smart Card logon mechanisms based upon a private key stored on the Smart Card (the USB-based technology). A user may use the same token to securely access the network from a public network (e.g. Internet cafe), via any VPN connection and authenticate with the OTP capability. Throughout the described scenario, the user also enjoys the full variety of Aladdin eToken solutions (e.g. SSO, WSO, and more), in order to enhance his password management needs and his productivity.

One-Time Password enabled USB token (LCD display, battery and generation button)

Smart card support for RSA 1024 bit, Triple DES, SHA1, OTP-160bit

Standard PKI Support for CAPI, PKCS11 and RADIUS OTP

Fully compatible with eToken PRO technology

Highly secure implementation using smart card chip for both PKI and OTP operations

Robust plug-and-play USB connectivity

Modular OTP algorithm support

Two-factor authentication: requires password and the token

Non-repudiation using advanced on-board PKI digital signing technology

