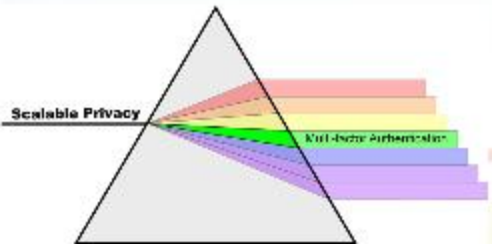
Are Passwords Passé?

Deployment Strategies for Multifactor Authentication

IAM Online – December 10, 2014

Mike Grady, Scalable Privacy Project
David Walker, Scalable Privacy Project



Thank you to InCommon Affiliates for helping to make IAM Online possible

aegisIDENTITY
the identity software company
www.aegisidentity.com | @aegisidentity

cirrus identity

FISCHER INTERNATIONAL

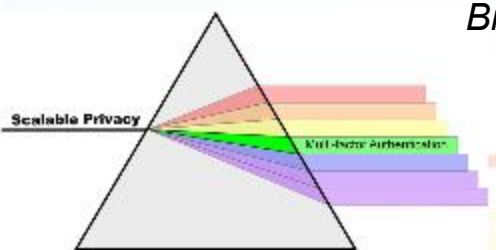
IDM integration

MOO
Spherical Cow Group

Microsoft

UNICON®

Brought to you by Internet2's InCommon in cooperation with the Higher Education Information Security Council

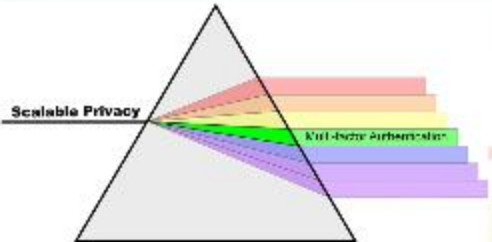


INTERNET 2

Presenters

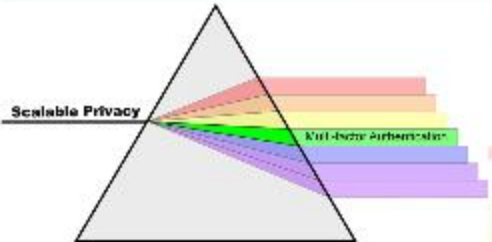
Mike Grady, Scalable Privacy Project
Senior IAM Consultant, Unicon

David Walker, Scalable Privacy Project
Independent Consultant



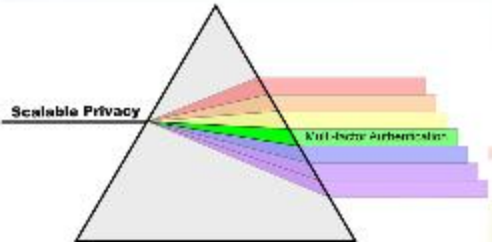
Overview

- What is Multi-Factor Authentication?
- Why Is Multi-Factor Authentication Important for Higher Education?
- Planning for Multi-Factor Authentication
- Deploying Multi-Factor Authentication
- Operating Multi-Factor Authentication
- MFA Cohortium
- Questions?



InCommon®

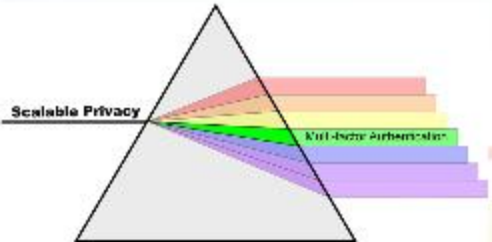
Getting to Know Ourselves



INTERNET 2

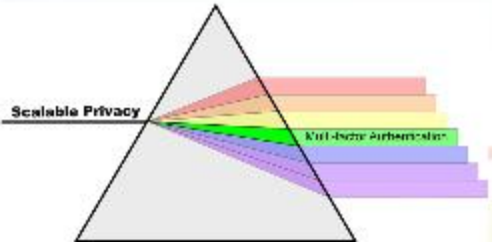
How Long Will You Rely on Passwords for Sensitive Resources?

- We don't rely on them now.
- 1 year
- 3 years
- 5 years
- Forever

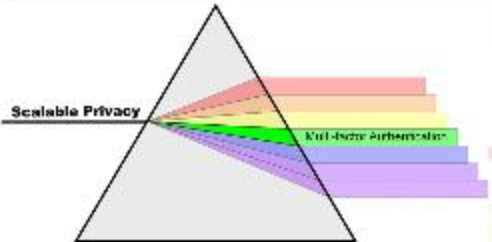


What are your institution's primary roadblocks to deploying MFA?

- Not a management priority
- Lack of funding
- Lack of people
- Lack of expertise
- Not warranted in our environment



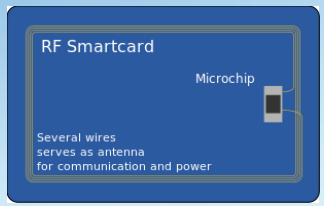
What Is Multi-Factor Authentication?



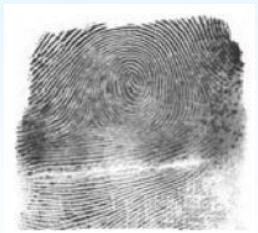
Authentication Factors

password

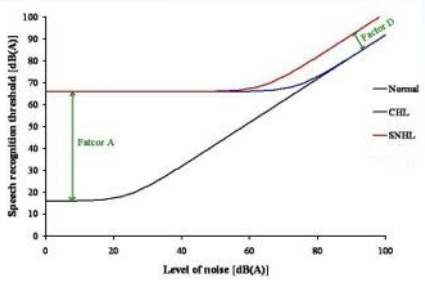
Something you know

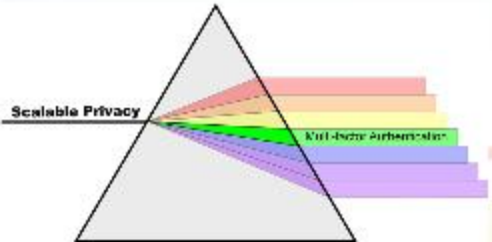


Something you have



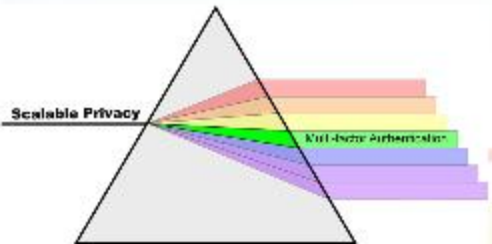
Something you are



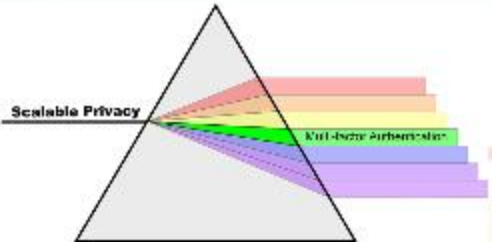


MFA is using more than one factor

- Password is something you know
- Combine with something you have or are, with growing # of choices/vendors:
  - Phone & mobile app based
  - Security tokens (hardware, USB, software)
  - Smart cards
  - Biometrics



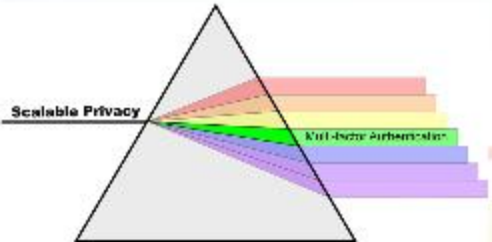
Why Is Multi-Factor Authentication Important for Higher Education?



We've Tried to Shore Up Passwords ...

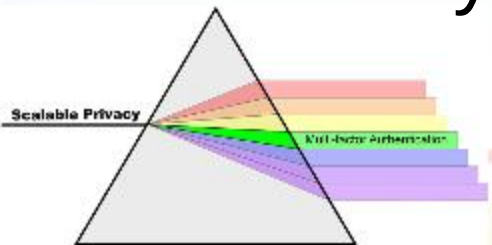
- Password complexity policies
- Frequency of change policies
- User education programs
- Password management tools

Despite all our efforts…..



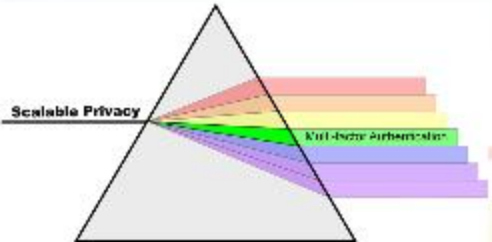
Passwords Are Compromised

- Breaches of increasingly critical and sensitive resources due to
  - Phishing
  - Online guessing
  - Reuse across services
  - Cracking password files
  - Key loggers



Passwords *are* Passé

- We've gone about as far as we can go (maybe too far?)
- We've made passwords more expensive
  - End-user effort and confusion
  - Help desk calls
- Yet they're increasingly less effective

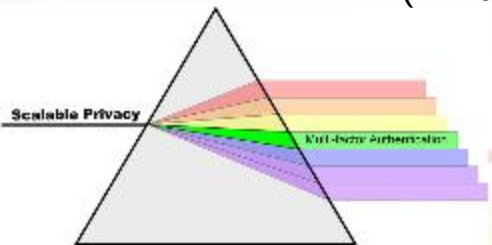


More Reasons to Move beyond Passwords

- Greater online access to high-risk services
  - *e.g.*, self-service payroll
- Compliance and regulations

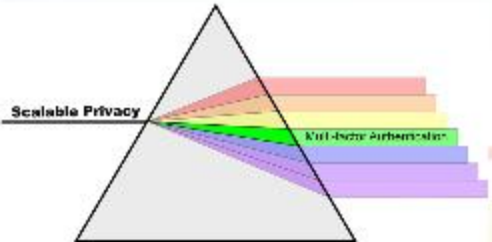
"*...ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate. Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps ...*"

(White House Executive Order of 10/17/2014)



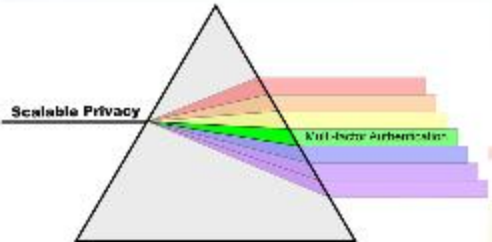
MFA Is Now a Viable Option

- MFA is getting easier to use
- MFA is getting more popular exposure
- Cost of technology and licenses decreasing

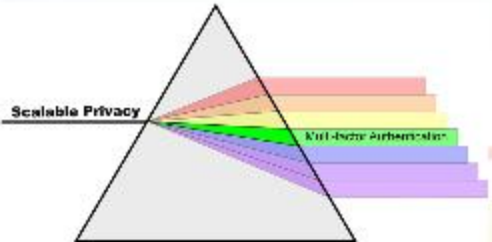


Higher Education Survey Results

- IAM Online webinar Sept. 2013: 75% of 120+ institutions indicated that within 5 years “using more than passwords for sensitive resources”
- MFA Cohortium institutions (45+) survey spring 2014: 80% within one year of “more than password”, with the other 20% within 3 years.
- Informal poll at beginning of Educause 2014 presentation aligned with MFA Cohortium survey results

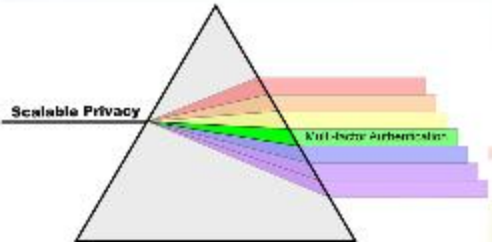


Planning for Multi-Factor Authentication



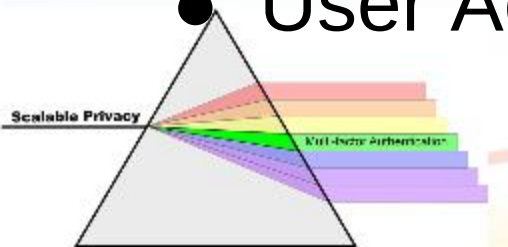
Among what audiences on your campus is the conversation about MFA taking place?

- Security/IdM group
- Central IT
- Campus-wide technologists
- CIO
- Campus-wide IT governance
- Executive management



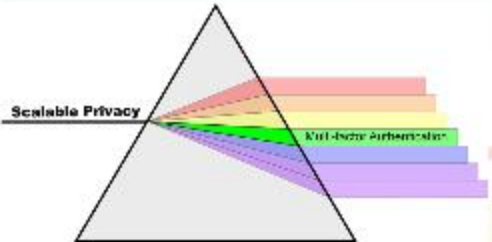
Making the Business Case

- Risk Assessment
  - Where are the greatest needs?
  - What is the risk of project failure?
- Resources
  - Who has the money?
- Future Proofing
  - What is the best path for future applications and future technologies?
- User Acceptance



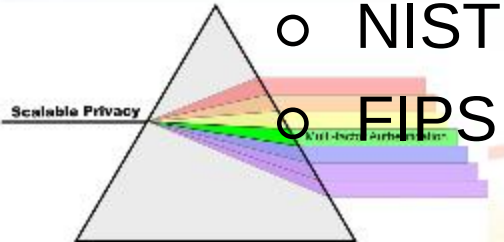
Initial Deployment Options

- Limited to specific services
- Integration with VPN
- Integrated in SSO service
  - User Opt-In (versus required)



Selecting Technology - How Much Security Is Enough?

- Recover confidence lost in passwords
  - “Two Step” authentication, *etc*.
- Address higher security needs
  - OTP
  - “Push” mobile apps
  - PKI
- Assurance and compliance
  - InCommon Assurance Program
  - NIST 800-63
  - FIPS 140-2

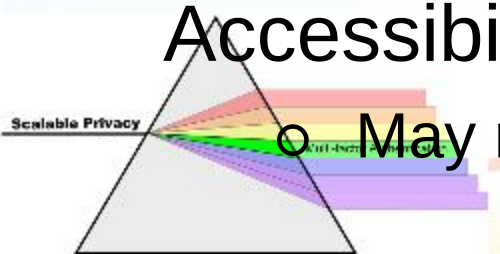


Selecting Technology - Form Factor

- Cell Phone
- Smart Phone or tablet
- Soft tokens
- Hardware tokens
  - USB dongle
  - NFC
  - Display, keypad, button to prove current control

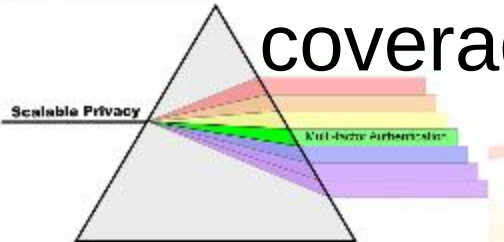
Accessibility

- May need to support multiple form factors



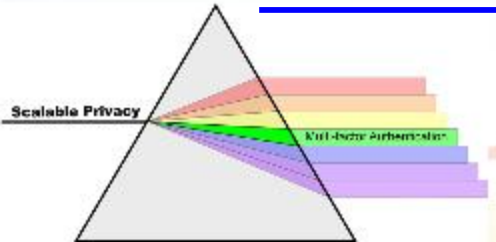
Selecting Technology - Other Factors

- Ease of deploying devices
  - objections to use of personal devices
- Management and self-service capabilities
- On-premise or cloud (or hybrid)
- Ease of technology refresh or changing technology choice
- Telephony issues: SMS costs, cell coverage, international



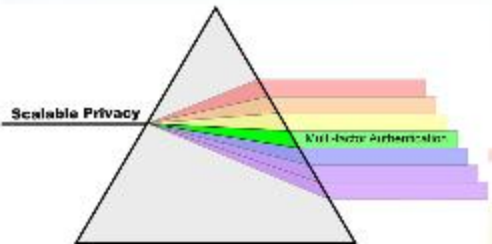
Selecting Technology - More Factors

- Vendor viability
  - Product suite and roadmap
  - User community
- Cost
  - Technology acquisition & refresh
  - Help desk
  - Support personnel, service contracts, communications & marketing, telephony (*e.g.*, SMS)
- NET+ offerings



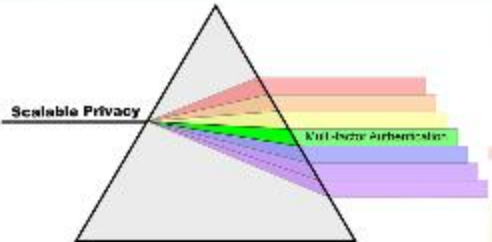
Selecting Technology - SSO Options

- User opt-in
- Multi-factor for specific users
- Multi-factor for specific services
- Some options
  - Shibboleth: Multi-Context Broker
  - CAS: CAS-MFA (MFA extensions for CAS)
  - Incorporate into Active Directory
    - Office 2013/ADAL



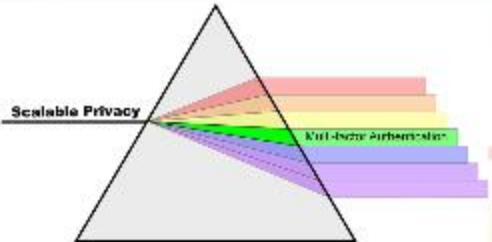
Establishing Policy

- Risk assessment
- Authentication requirements for services and people
- Token management
- Identity proofing

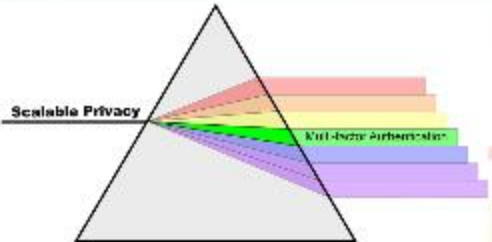


Other Planning Issues

- Alternative authentication strategies when tokens are not available
  - Printed list of OTPs
  - Friends as “biometric”
- Building campus consensus
  - Transparent decision process
  - Start with opt-in
- Marketing and communications

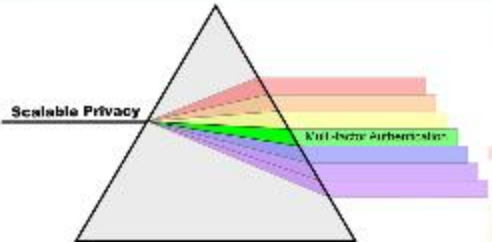


Deploying Multi-Factor Authentication



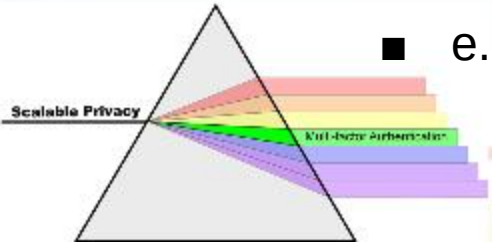
State of Your Campus's MFA Deployment

- My campus has established an action plan for MFA
- My campus's action plan has been funded



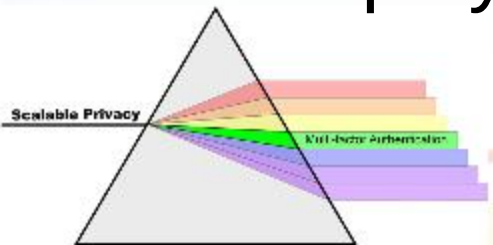
An Emerging Deployment Pattern ….

- Pick a technology
  - Rely on User devices (mobile, phone)
  - Rely on cloud-based vendor
- Conduct a prototype/pilot
- Integrate into SSO
- Likely will need (eventually)
  - Hardware token option
  - Supplement the vendor-supplied enrollment/mgmt interface
    - e.g. print OTP list, register friend, ...



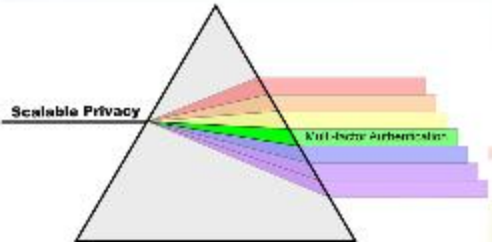
….. An Emerging Deployment Pattern

- Start with core IT staff, then expand
- Begin to train support staff
- Deploy for early adopters (opt-in)
- Focus on developing marketing & communications
- Start work with service managers for mandatory use
- Deploy for all users



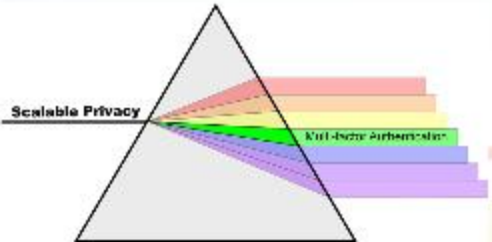
State of MFA Deployment at My Institution

- Core IT staff
- Early adopters (opt-in)
- A few sensitive services
- Available for all users and all services
- Integrated into campus SSO
- Available for federated services

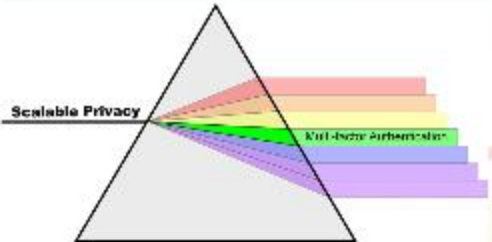


Things You Will Need to Do

- Interface for user self-registration etc.
  - many find that the vendor option needs supplementing
- Delegation of management, registration, and user support responsibilities
- Distribution point(s) for hard tokens
- Help desk / support training
- Marketing and communications!



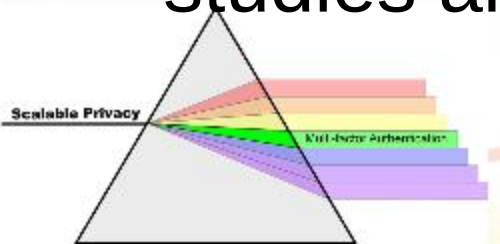
Operating Multi-Factor Authentication



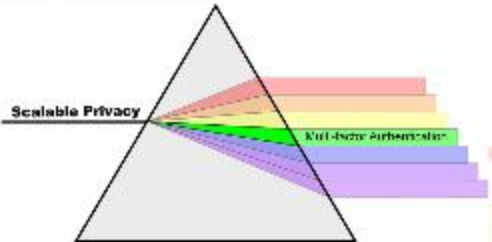
Operational Issues

- Distribution of tokens
- Retiring tokens
- Periodic technology refresh
- Monitoring & metrics
- Help desk

The Cohortium is collecting campus case studies and artifacts from campuses.

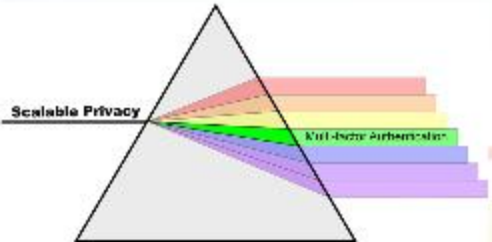


MFA Cohortium



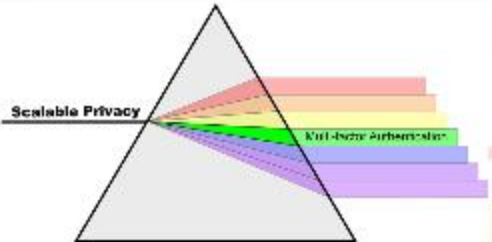
MFA Cohortium Basics

- About 50 institutions now
- Representing roughly 1 million people
- Started late spring 2013
- Meets bi-weekly
- Core work finishing up soon



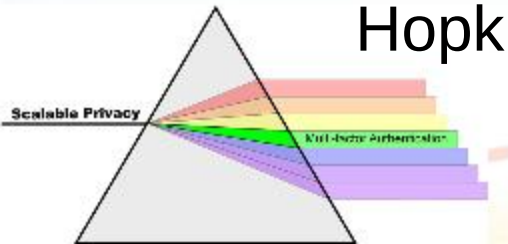
Cohortium Resources

- How Much Security Is Enough?
- Enterprise Deployment Strategies for Multi-Factor Authentication
- Diagrams providing a visual presentation of MFA Business Drivers, Deployment Decision Trees, and Integration (architecture) Patterns
- Multi-Factor Authentication Solution Evaluation Criteria
- Alternative Strategies When Multi-Factor Tokens Are Not Available



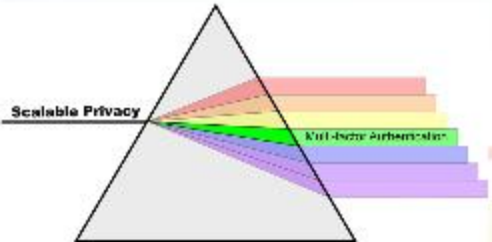
More Cohortium Resources

- The MFA Cohortium Wiki
- Case Studies
- Reference Materials & Artifacts/Examples
- Working on:
  - MFA management console requirements
  - AD/Microsoft ecosystem & MFA primer
- Presentations on campus deployments
  - Duke, Penn, Arizona, Stanford, Chicago, Johns Hopkins



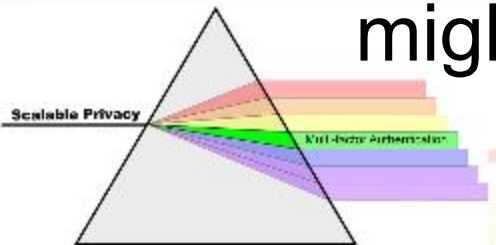
Software

- The Internet2 Scalable Privacy Project has helped to fund software that enables easier deployment of MFA:
  - Shibboleth Multi-Context Broker
  - CAS-MFA
  - InCert



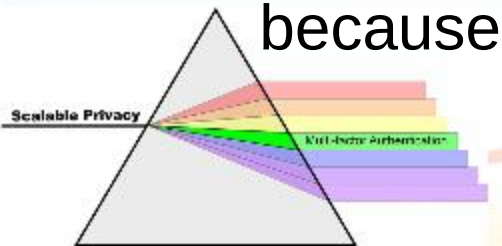
Other Resources

- 2014 HEISC Information Security Guide
  - Two-Factor Authentication section
- "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes"
  - Evaluate based on "broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide."

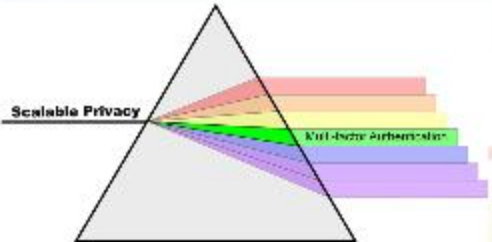


Judging the Impact of the MFA Cohortium (please check all that apply)

- I have previously heard of the MFA Cohortium
- I have visited the Cohortium web site
- I have used Cohortium-provided documents
- I have participated in Cohortium meetings
- I have heard of the Multi-Context Broker (MCB) and/or the CAS MFA enhancements
- My institution is using or is planning to use the MCB or CAS MFA enhancements
- MFA deployment will be (or has been) easier because of the MFA Cohortium



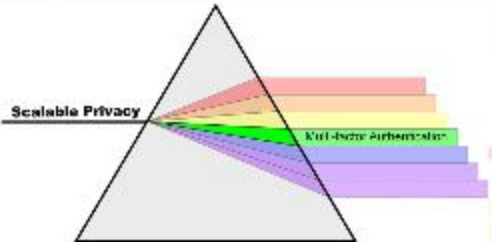
Questions? What else would help you with MFA?



Evaluation

Please complete the evaluation of today's webinar

https://www.surveymonkey.com/s/IAM_Online_December_2014



Thank you to InCommon Affiliates for helping to make IAM Online possible

aegisIDENTITY
the identity software company
www.aegisidentity.com | @aegisidentity

cirrus identity

FISCHER INTERNATIONAL

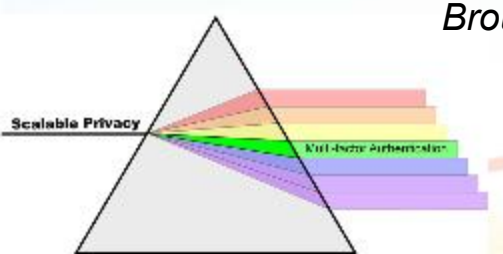
IDM integration

MOO
Spherical Cow Group

Microsoft

UNICON®

Brought to you by Internet2's InCommon in cooperation with the Higher Education Information Security Council



INTERNET 2

46