InCommon Multifactor Authentication

Joe St Sauver, Ph.D.
(joe@internet2.edu or joe@uoregon.edu)
InCommon Certificate Program Manager and
Internet2 Nationwide Security Programs Manager

Techs In Paradise

Tuesday, 15 January 2013

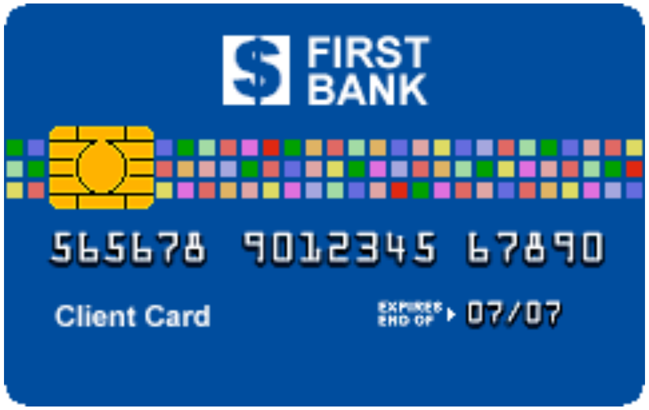
10:20-10:40

http://pages.uoregon.edu/joe/jt-multifactor/

I. Introduction

What Is Multifactor Authentication?

- Normally you authenticate with one factor, something you know, such as a password or PIN. Multifactor authentication adds a second factor, either something you have or something you are.
- *Example*: you use multifactor authentication every time you get money out of an automatic teller machine: you use both your ATM card (something you have), and something you known (your PIN).



- *Another example:* Multifactor authentication that leverages something you are (e.g., biometrics), is less common, but if you're a member of the Global Online Entry System Trusted Traveller Program you may remember that Customs collected a copy of your fingerprints (a biometric identifier) as part of enrolling in that program.

[Image credit: http://en.wikipedia.org/wiki/File:ClientCardSample.png]

Multifactor In *Our* World

- We're not spitting out twenty dollar bills like an ATM or working hard to quickly let legitimate citizens and visitors in while keeping inadmissible people out (like the examples from slide three).
- Our use case is rather more mundane, if no less important: we want to secure logins to our networks and systems, particularly when:
  -- logins are to things like <u>VPN</u>s, which intentionally punch holes right on through normal perimeter security defenses
  -- logins are to <u>accounts with special privileges</u> (root/system/administrator, or "enable" on a router, etc.), or
  -- logins are to <u>systems of special sensitivity</u>, such as to admin systems with PII, health information, academic records, financial information, etc.; core routers; security systems; etc.)
  -- users have demonstrated a real predisposition towards being <u>phished</u> (resulting in spam and institutional blacklisting, etc.), yet we must continue to allow them access, nonetheless...

Four Quick Questions for Today's Attendees

1) Do **YOU** currently use multifactor authentication to help secure logins to one or more of **your own** accounts or systems? If so, please raise your hand.
2) If you've got your hand up, do you think multifactor HELPS to protect that account or system? If so, please leave your hand up. If you don't think it helps to protect your account or system, please put your hand down.
3) If you've still got your hand up, is your current multifactor authentication system EASY and CONVENIENT or painful to use? If multifactor authentication you're using is easy and convenient, please leave your hand up. If it's painful, hand down.
4) One last question: if you have **easy to use** and **cost effective** multifactor authentication for **ALL** your users for **ALL** your systems and applications, please leave your hand up.

What We Expected We Might See

1) We expected to see that a significant portion of today's attendees would already be using multifactor authentication on one or more of their own accounts (hey, this is a security and privacy conscious audience with lots network engineers, sys admins, etc.)
2) We also believed that many of those in the audience using multifactor authentication would "get" that multifactor authentication actually does help secure those accounts. (You can see an earlier discussion of security problems with plain old passwords at http://pages.uoregon.edu/joe/passwords/)
3) However, unfortunately, we suspected that many of you would report that using multifactor is painful rather than painless
4) Finally, we expected that very, very few of you (if any) would report that you use multifactor for all services and all users. (If you are doing so, we're in awe of your accomplishment!)

So Why Isn't Everyone Doing Multifactor Auth?

- We think the most common reasons are:

  -- Traditionally, multifactor has been seen as being **too expensive** for broad deployment
  -- Multifactor has also been seen as **burdensome or inconvenient**, and thus something to avoid if at all possible
  -- Users think that their access "isn't anything special" and doesn't need "special protection," or they don't think that they're at any special risk of being targeted for attack
  -- Multifactor was viewed as too complex to scalably deploy

- We hope that you'll change how you feel about broad deployment of multifactor authentication once you hear about the multifactor authentication programs that InCommon is now offering

InCommon's Multifactor Authentication Offerings

- InCommon currently offers two main approaches to multifactor authentication:
  -- One solution, from **Duo Security**, leverages user smart phones (see http://www.incommon.org/duo). Duo Security is a Net+ service (see www.internet2.edu/netplus/cloud-services.html)
  -- The other solution, a traditional client certificate ("PKI") solution leveraging client certificates from **Comodo** (offered through the very popular InCommon Certificate Program) along with USB format hard tokens or smart cards from **SafeNet** (see http://www.incommon.org/safenet and http://www.incommon.org/certificates)
- InCommon also has an affiliate program (see http://www.incommon.org/affiliates/). Vasco, a provider of multifactor solutions, is currently a participant in that program, and we anticipate that we'll see more multifactor affiliates in the future.

II. InCommon's Multifactor Authentication Offerings:

Duo Security

Duo Security: Multifactor for Everyone

- The Duo Security multifactor program is designed to leverage a modern reality of campus life: everyone's got a smart phone (or at least some sort of cell phone). Given that, we can probably use those phones as a second factor.
- In a nutshell, after Duo's been enabled for an account:
  -- a user will enter their username and password as they normally would (this is the "first factor" of the two factor login process)
  -- a request will then get sent to the user's phone asking the user to confirm that they'd like to login (this is the "second factor"). On a smart phone, a user will simply push Approve or Deny.
- If a user has basic cell phone that can't run apps, or only wants to authenticate from a land line, they can be called and asked to press a button to confirm their desire to login that way, instead.
- If a user doesn't have *any* sort of phone, a site using Duo can also issue users a traditional $20 hardware cryptographic fob, instead.

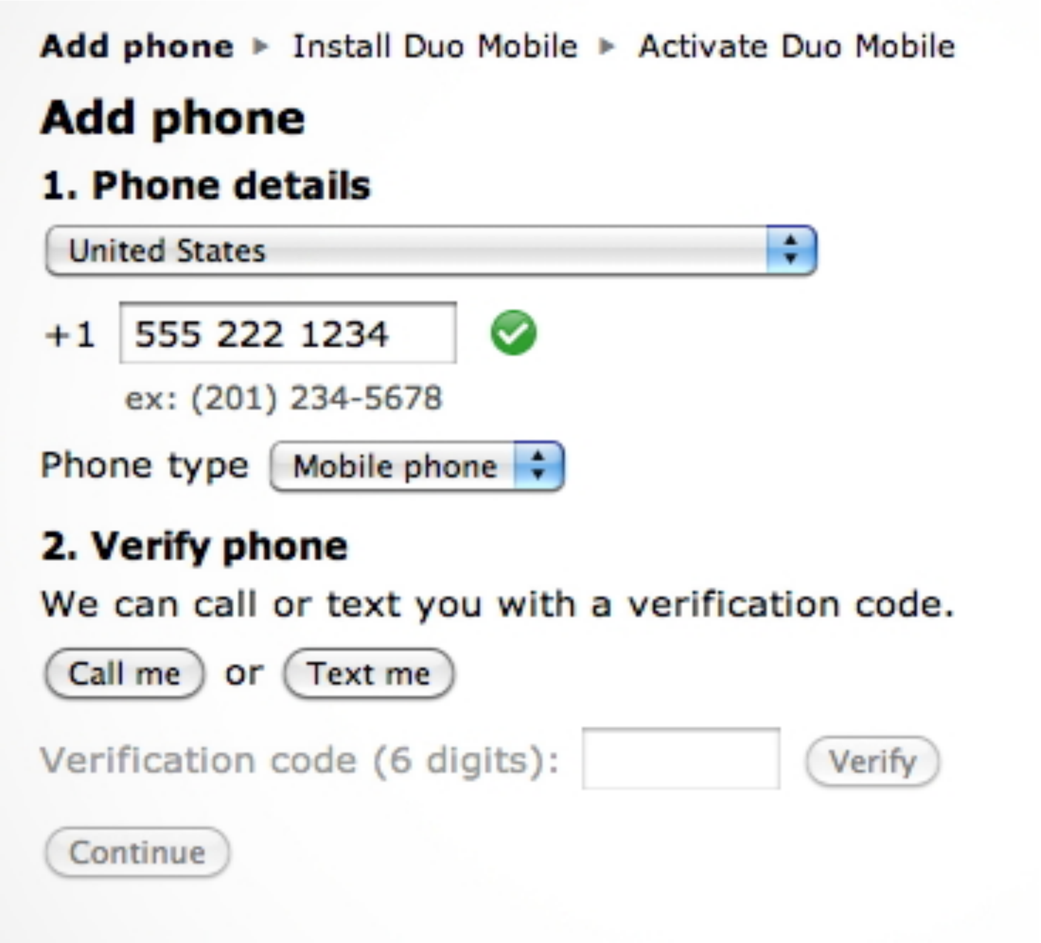
Trying Duo; Getting Users Enrolled

- If you want to try Duo, you can try it for free for up to ten users, see https://www.duosecurity.com/pricing to sign up.
- Extensive documentation about Duo is available online at https://www.duosecurity.com/docs

- People sometimes wonder *how do users get enrolled to use Duo?* While local Duo administrators can chose to "bulk enroll" users (see https://www.duosecurity.com/docs/administration), in most cases users will *self-enroll*. Self-enrollment happens after normal login the first time the user goes to login after their account has been set to use Duo, leveraging "trust on first use" principles.

  Let's run through the user self-enrollment process -- it has three basic steps: linking the user's phone to their account, installing the Duo Mobile App, and finally, activating Duo Mobile.

User Self-Enrollment Step 1 (Link Your Phone), Done The First Time A User Logs In After Duo Has Been Installed On A System They Use



Add phone ▸ Install Duo Mobile ▸ Activate Duo Mobile

Add phone

1. Phone details

United States

+1 555 222 1234 ✓

ex: (201) 234-5678

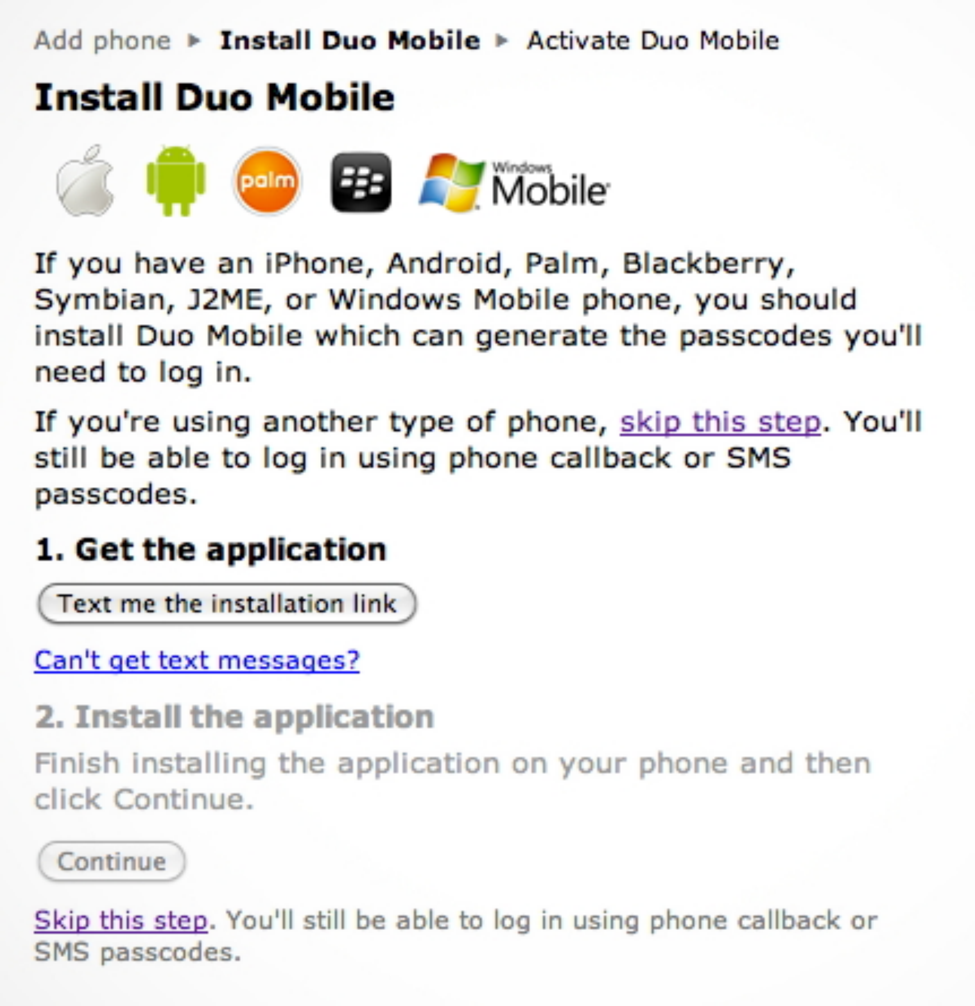
Phone type: Mobile phone

2. Verify phone

We can call or text you with a verification code.

Verification code (6 digits):

User Self-Enrollment Step 2 (Install Duo Mobile App on the User's Smart Phone)



Add phone ▸ **Install Duo Mobile** ▸ Activate Duo Mobile

Install Duo Mobile

If you have an iPhone, Android, Palm, Blackberry, Symbian, J2ME, or Windows Mobile phone, you should install Duo Mobile which can generate the passcodes you'll need to log in.

If you're using another type of phone, skip this step. You'll still be able to log in using phone callback or SMS passcodes.

1. Get the application

Text me the installation link

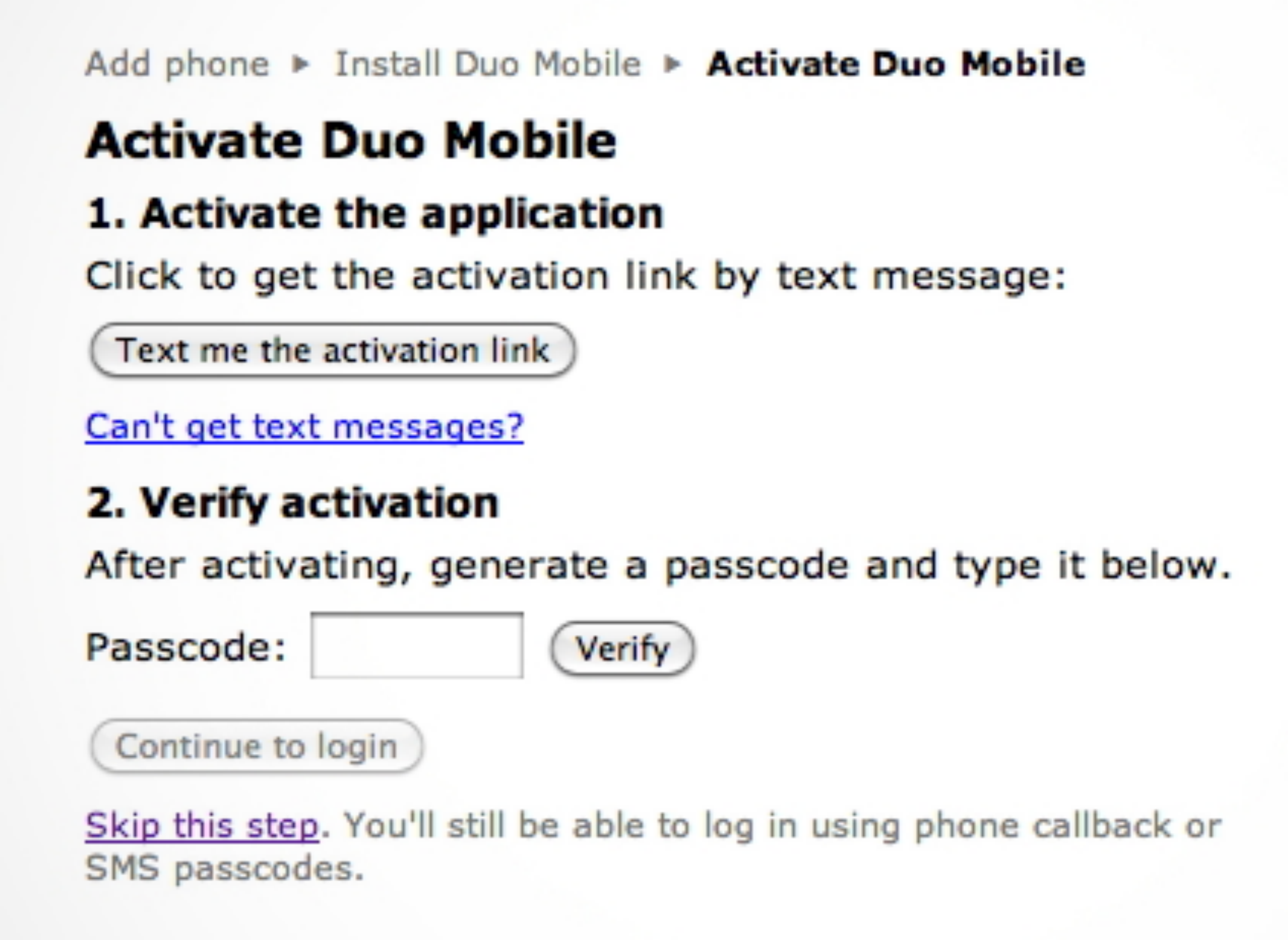
Can't get text messages?

2. Install the application

Finish installing the application on your phone and then click Continue.

Skip this step. You'll still be able to log in using phone callback or SMS passcodes.

User Self-Enrollment Step 3 (Activate Duo Mobile)



Add phone ▸ Install Duo Mobile ▸ **Activate Duo Mobile**

Activate Duo Mobile

1. Activate the application

Click to get the activation link by text message:

Text me the activation link

Can't get text messages?

2. Verify activation

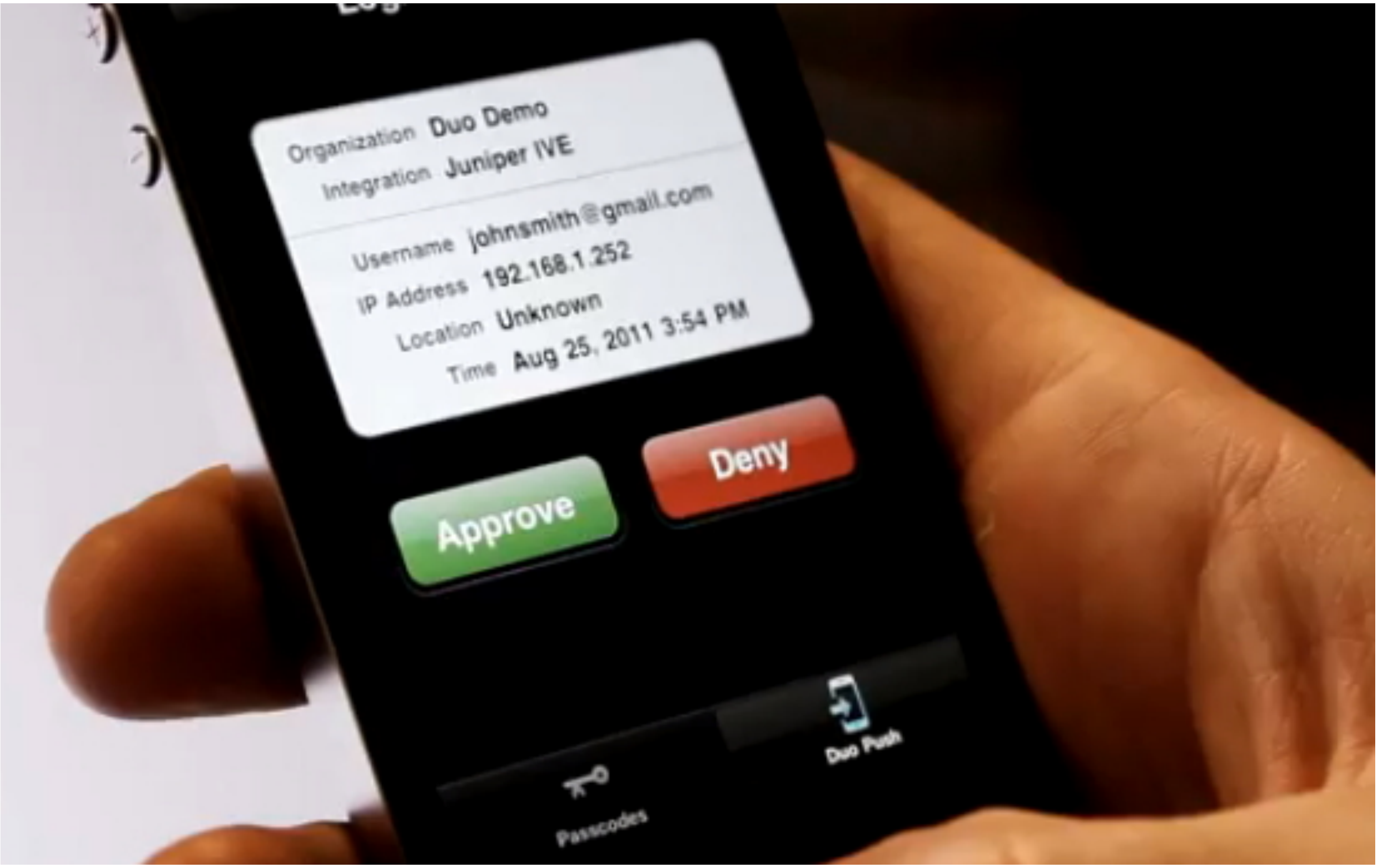
After activating, generate a passcode and type it below.

Passcode: Verify

Continue to login

Skip this step. You'll still be able to log in using phone callback or SMS passcodes.

After One Time Activation, What Most Users Will See At Login Time on Their Smart Phones



Organization Duo Demo
Integration Juniper IVE

Username johnsmith@gmail.com
IP Address 192.168.1.252
Location Unknown
Time Aug 25, 2011 3:54 PM

Duo Phone Calls vs. Duo Internet Connections

- Note that Duo can make connections to your phone both over the Internet and via the traditional phone network.
- Connections to your smart phone made over the Internet are free, and since that's also the easiest way to use Duo (just hit Accept or Deny), this is the way that we believe most users will use Duo.
- Duo connections made to your phone over the traditional phone network (after initial phone setup) use Duo *telephony credits*.
  An SMS (text) contact in the US costs one credit; a voice call in the US uses two credits. Sites can buy 1,000 telephony credits for $10
- If you're traveling abroad, Duo can still call you while you're on the road in most countries, but due to the cost of international long distance, getting called abroad costs more telephony credits than being called within the US. See https://www.duosecurity.com/docs/telephony_credits for details

Duo From the Other Side

- Clearly Duo is pretty straightforward to use from the user side of things, but what about from the other side, e.g., from the point of view of an admin who needs to integrate Duo with his/her service?

- Duo offers Duo-enabled login handlers for a wide variety of systems/services, including:
  -- popular **VPNs** (https://www.duosecurity.com/vpn)
  -- **ssh** logins to Unix hosts (https://www.duosecurity.com/unix)
  -- **web applications** (https://www.duosecurity.com/web)
  -- **Microsoft Remote Desktop and Outlook Web App** (https://www.duosecurity.com/microsoft)
  -- applications that use **RADIUS** for authentication (https://www.duosecurity.com/docs/radius)
  -- and even applications that use **Shibboleth** for authentication (https://www.duosecurity.com/docs/shibboleth)

Going Beyond Those 10 Free Trial Users

- Assuming you try Duo and like it, what are you options for going beyond the ten free trial users? Obviously, anyone interested in doing so can buy regular licenses from Duo for $36/user/year (see https://www.duosecurity.com/pricing).
- InCommon participants have two additional options now...
  -- Higher ed InCommon participants can buy Duo for **$5/user/year**, 500 user minimum, see https://www.duosecurity.com/incommon (payment is by credit card and no special paperwork is required)
  -- InCommon participants can also purchase a **site license** for Duo covering all non-hospital faculty/staff, or both non-hospital faculty/staff and students. Pricing varies by school size, see http://www.incommon.org/duo/fees.html
- A Duo site license example: an Internet2 member university with 20,000-34,999 students would pay $40,000/year to cover all their non-hospital faculty, staff and students, less than $2/user/year.

Does The New "Ala Carte" Option Somehow "Undercut" the Classic Duo Site License Option?

- No. While we still fundamentally believe that multifactor auth should ideally be used to protect all users, we recognize that some sites may not be willing to dive right in with a full site license until they have more experience with Duo. In those sort of cases, the "ala carte" model allows for something between baby steps (the free 10 user trial model) and going "whole hog" with a Duo site license.
- In the case of the nominal 20,000-34,999 user Internet2 university case, given that a site license covering all faculty/staff and students (except hospital staff) costs $40,000/year, it wouldn't make sense to continue to buy more than 8,000 seats of Duo "ala carte" since for the same price you could buy a site license that would cover all faculty, students and staff members.
- Similarly, by the point you hit 70 users at full price ($36/user/year), it's cheaper to buy a discounted 500 user license (at $5/user/year)

Duo and NSTIC

- Internet2 was very fortunate to recently receive one of five pilot awards from the National Strategy for Trusted Identities in Cyberspace (NSTIC), see http://www.nist.gov/itl/nstic-092012.cfm

- That grant, while primarily focused on scalable privacy in the identity ecosystem, also included funding to encourage use of multifactor authentication at three designated pilot sites.
  The technology that was proposed and accepted for that effort was Duo Security.

- Among other things, Internet2's NSTIC efforts will also include work to create a broader multifactor cohort, so that sites can learn from and help support each other, whether they're using a multifactor solution from Duo or some other vendor.

III. InCommon's Other Multifactor Authentication Offering:

Comodo Client Certificates on SafeNet Hard Tokens or Smartcard

Client Certs and PKI Hard Tokens/Smart Cards

- While we think that most users will find the Duo Security phone-based multifactor option the easiest to deploy and use, some users may have different needs, needs best met by traditional client certs on PKI hard tokens or smart cards. InCommon can help in that situation, too.

- We offer currently offer standard assurance client certificates at no extra cost as part of InCommon's Certificate Service, and we also offer USB-format PKI hard tokens and smart cards from SafeNet at a significant discount from market prices.

See http://www.incommon.org/certificates and
http://www.incommon.org/safenet/

Understanding Client Certificates

- We don't really have time to give you a thorough introduction to client certificates today during today's brief session, but we do have a three hour tutorial from Security Professionals 2012 that you can go through at your leisure, see: "Client Certificates: A Security Professionals 2012 Preconference Seminar," http://pages.uoregon.edu/joe/secprof2012/
- For now, just think of client certificates as binding an identity (such as your email address) to a pair of cryptographic keys, one key that's publicly shareable, and a corresponding one that's secret. If you've got those credentials handy, you can use them for things like serving as a 2nd factor for login, or for digitally signing or encrypting email.
- The question is: how can you keep those credentials readily available for use, yet not have them be at constant risk of being stolen or misused by some hacker/cracker?

The Solution: PKI Hard Tokens and Smart Cards

- PKI hardware tokens normally come in two formats: smart cards (the size and shape of a credit card), and USB-format PKI hard tokens (which look just like a regular USB-format thumb drive).
- While these cards and tokens may not look like anything special, they actually are – these devices contain special tamper-resistant cryptographic storage and federally-certified cryptographic processing capabilities.
- Cryptographic credentials stored on PKI hard tokens can be configured to be useable but non-exportable, unlike cryptographic credentials stored as conventional files on a hard disk or thumb drive. This makes it difficult for hackers to steal your cryptographic credentials. Using a USB-format hard token or smart card also makes it easy to carry your credentials with you wherever you go.

Duo vs. Client Certs on Hard Tokens

- While the Duo Security option is focused just on two factor auth, using client certificates enables two factor authentication while *also* enabling encryption and digital signatures. For example, if you have a client certificate you can digitally sign or encrypt email using S/MIME, and you can also digitally sign contracts, reports or other documents. (Of course, you could also use an alternative encryption system, like PGP/GPG for encryption and signing, too)
- What about out of pocket costs? Let's compare Duo "ala carte" with client certs. If you're already an InCommon Certificate Service participant, you can get client certificates at no additional cost. SafeNet USB format hard tokens are roughly $20/token when purchased by InCommon participants eligible for the Internet2 discount. This means that the four year cost for a client cert (plus a USB-format hard token on which to store it) is virtually the same as 4 years of Duo Security "ala carte" at $5/user/year

Smart Cards As A Basis for Campus ID Cards

- Another potential advantage of using client certificates on smart cards as your multifactor choice is the fact that smart cards can serve as the basis for a regular campus ID card, containing not just the user's client certificate, but also all the things you'd normally find on a campus ID card, such as the user's name and picture, an identification number, status/role information, a bar code, etc. We talked briefly about this a year ago at Joint Techs Baton Rouge, see "Client Cert Deployment Models and Hardware Tokens/Smart Cards," http://pages.uoregon.edu/joe/client-cert-models/
- Of course, one complexity of deploying client certificates in smart card format is that you need to factor in the cost of deploying smart card readers, not just for campus desktops and laptops, but also potentially for any home users who need to use smart card auth.
- Slick-sided mobile devices (such as smart phones or tablets) can also be a challenge if there's no easy way to add a smart card reader.

Client Certificates, Hard Tokens and Higher LOAs

- Client certs also potentially play a critical role when it comes to attaining higher levels of assurance. NIST SP800-63-1 ("Electronic Authentication Guidelines," dated December 2011) makes it clear that getting to the highest level of assurance, NIST LOA4, would be difficult or impossible without using client certificates on hard tokens/smart cards. The InCommon higher education community doesn't currently seem to have requirements for NIST LOA4-class credentials, but if we do in the future, that would almost certainly imply use of client certificates on hard tokens/smart cards.
- Speaking of assurance, the first higher education institution to achieve InCommon Silver Assurance (equivalent to NIST LOA2) was Virginia Tech. They used SafeNet USB eToken Pro devices (the same sort of USB-format PKI hard tokens offered by InCommon), along with client certificates issued by Virginia Tech's own Certification Authority. (see http://tinyurl.com/vatech-silver)

IV. Some Final Thoughts

We'd Love To Hear Your Feedback

- Do we have the multifactor solutions you want and need? If not, what should we be doing?

- For example, should we be working to partner with a biometric solution vendor?

- Feel free to visit with me directly if you'd like to do so, or send email to joe@internet2.edu if that's easier for you

Whichever Way You Choose To Go...

- Whichever way you choose to go, whether you use:

  -- a phone-based two factor solution like Duo Security,

  -- a classic PKI solution like Comodo client certificates with SafeNet USB-format PKI hard tokens or smart cards, or

  -- something completely different, like biometrics or traditional hard cryptographic tokens

  PLEASE try to do some sort of multifactor authentication for as many of your users as possible. Plain old passwords simply aren't good enough anymore given the increasing threats you and your users face from brute force attacks, traffic sniffing attacks, password stealing malware, and a host of other threats.

The Ten Ton Gorilla In the Room: Compliance

- If nothing else, be sure to recognize that the Payment Card Industry Data Security Standard (PCI DSS) v2.0 (dated October 11th, 2010) requires at section 8.3 that PCI-compliant networks:

> Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)

https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Thanks for the Chance to Talk Today!

Are there any questions?