

The InCommon/Net+ Multifactor Authentication Program

Joe St Sauver, Ph.D. (joe@internet2.edu or joe@uoregon.edu)

InCommon Certificate Program Manager and
Internet2 Nationwide Security Programs Manager

Internet2 Annual Member Meeting
Salon A, 3-4PM, Monday, May 22nd, 2013

<http://pages.uoregon.edu/joe/internet2-2013MM/>

Note: These slides are provided in a detailed format for those who may be hearing impaired, for participants whose primary language may be something other than English, and to meet the needs of those who may be viewing these slides after the meeting is over.

I. Introduction

This Is Not the Only Multifactor Session at the I2MM

- Before we get down to business with this session, I wanted to make sure that everyone's aware that this is not the only multifactor session at this meeting (in fact, multifactor is something of an informal "mini theme" for this meeting). If you're interested in multifactor, you may also want to consider (or would have wanted to consider) attending:
 - The PKI BoF (it was at noon today)
 - Multifactor Authentication (MFA) and Assurance BoF:
Advantages of moving beyond passwords to MFA approaches
(Noon Tuesday, Rosslyn I/II)
 - Toward a Scalable Approach to Privacy and Security
(3PM Wednesday, Salon K (netcast session))

Our Issue: Multifactor Authentication (Non) Use

- **Most people don't use multifactor authentication – at least not "everywhere."**
- In many cases, even if you **wanted** to use multifactor authentication "everywhere," you **couldn't** – while a growing number of sites do offer it, many sites still don't (and yes, that includes many university sites/systems).
- To a disconcerting extent, we still rely on passwords to limit access to information, systems, and networks – even when those information/systems/networks are sensitive in nature.
- That's just crazy. Plain old passwords simply aren't good enough, particularly when it comes to securing sensitive resources.
- **Since InCommon offers several multifactor authentication solutions to the higher education community, we'd like to tell you about them -- and understand why more InCommon participants aren't already deploying multifactor authentication.**⁴

Deploying Multifactor At Scale

- We are particularly interested in seeing multifactor deployed **at scale**, e.g., ubiquitously -- for everyone, everywhere.
- This is one reason why we were so pleased that InCommon/Net+ has been able to enter into two "at scale" multifactor vendor relationships:
 - Duo Security's phone-based multifactor authentication solution, including both ala carte and site license programs, and
 - The InCommon Certificate Service, featuring SSL and client certificates (aka personal certs, or PKI) -- again, as a site licensed offering -- supported by deeply discounted SafeNet USB-format PKI hard tokens and smartcards for those that need/want them.
- But we're still not seeing the ubiquitous deployment we'd expected.

One Time When We All DO Use Multifactor Auth

- Even though I believe that there isn't even a single person at this meeting who uses multifactor authentication for everything everywhere, **I would bet that EVERYONE at this conference uses multifactor authentication for AT LEAST one service**, namely their ATM card. To get out money you need to insert your card (something you have) and supply something you know (your PIN).
- Why do we accept multifactor auth for that purpose? Well, **the banks make us**, at least if we want to use their ATMs.
- Unfortunately, that sort of "we're just going to make you do it" model doesn't tend to work well in higher ed.
- Of course, some parts of higher ed already **do** use multifactor...

Isolated Higher Ed Deployment Cases

- If any of you are a system administrator ("have root" access) or are a router admin ("have enable" access), you probably use multifactor authentication for that work.
- If a financial aid officer snuck in to this session, we know that he or she would also use multifactor authentication, because the federal Department of Education requires him or her to do so as part of their work around securing access to federal financial aid-related information.
- Another example: if you're a university pharmacist licensed by the DEA to purchase scheduled narcotics for administration to patients with severe pain in your hospital or clinic, you'll also be using multifactor authentication when you place orders for controlled drugs with your pharmacy wholesalers.
- Are there other higher ed MFA examples that come to mind?

II. Phone-Based Multifactor

This Is The Year of Phone-Based Multifactor

- There's no doubt in my mind that this is the year of multifactor authentication, at least in the commercial space (and hopefully in higher education, too!)
- Consider the following commercial phone-based multifactor rollouts...

2-step verification

Help keep the bad guys out of your account by using both your password *and* your phone.

Get Started



2-step verification adds an extra layer of security to your Google Account

In addition to your username and password, you'll enter a code that Google will send you via text, voice call, or our mobile app.

How it works

1

Enter your password

Whenever you sign in to Google you'll enter your username and password as usual.

2

Enter a code from your phone

Then, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.



Keep it simple

During sign in, you can tell us not to ask for a code again on that *particular computer*. You'll still be covered, because we'll ask for codes when you or anyone else tries to sign in to your account from *other computers*.

How do I set up two-step verification?

Set up two-step verification at [My Apple ID](https://appleid.apple.com) (appleid.apple.com):

1. Select "Manage your Apple ID" and sign in.
2. Select "Password and Security."
3. Under Two-Step Verification, select Get Started and follow the onscreen instructions.

How does it work?

When you set up two-step verification, you register one or more trusted devices. A trusted device is a device you control that can receive 4-digit verification codes using either Find My iPhone notifications or SMS to verify your identity.

Then, any time you sign in to manage your Apple ID at [My Apple ID](https://appleid.apple.com) or make an iTunes, App Store, or iBookstore purchase from a new device, you will need to enter both your password and a 4-digit verification code as shown below.



You enter your Apple ID and password as usual.



We send a verification code to one of your devices.



You enter the code to verify your identity and complete sign in.

After you sign in, you can manage your account or make purchases as usual. Without both your password and the verification code, access to your account will be denied.

You will also get a 14-digit Recovery Key for you to print and keep in a safe place. You will use your Recovery Key to regain access to your account if you ever lose access to your devices or forget your password.



Introducing Login Approvals

by Andrew Song for Facebook Engineering (Notes) on Thursday, May 12, 2011 at 9:58am

Facebook has always been committed to both protecting our users' account and information, as well as giving them more control over their Facebook experience. From our User Operations team, who work to re-secure compromised accounts, to the Engineering team that designs and implements new security features like login notifications, one-time passwords, and remote session management, everyone at Facebook is working to ensure users have a safe, enjoyable experience.

Even interns like myself are tasked with big projects to help improve account security. Instead of working on mundane tasks and simple problems, interns are given high-impact assignments that reach out to hundreds of millions users every time they use Facebook.

Today, we're announcing our newest opt-in security feature that I've worked to build over the past few months: Login Approvals.



The Official Microsoft Blog

News & Perspectives

TechNet Blogs > The Official Microsoft Blog > Microsoft Account Gets More Secure

Microsoft Account Gets More Secure

17 Apr 2013 9:00 AM

Over the next couple days we will roll out a major upgrade to Microsoft account, including optional two-step verification to help keep your account more secure.

Microsoft has increasingly focused on delivering connected devices and services that are currently used by more than 700 million people around the world. A Microsoft account is the key that unlocks your experience across these products—from your Windows PC to your Windows Phone, from Xbox to Outlook.com, from SkyDrive and Skype to Office and much more.

Given this critical role for Microsoft account, we remain vigilant in working hard to protect your account, which is why we're adding an option so you can enable two-step verification to further protect yourself. You should see this option show up in your account in the next few days. You can enable this capability at <https://account.live.com/proofs/Manage>.

One account connects your digital world

A Microsoft account makes your experiences on devices and services more personal and relevant. When you sign in to any device or service with your Microsoft account, your personal settings, contacts and other information meet you there. It keeps you connected to the

PAYPAL

https://www.paypal.com/us/webapps/mpp/security/hardware-software-protection ☆ ▾ ↻ Google

Secure Passwords ➔

Security Key

Logging in with your PayPal user name and password is secure-but if you're looking for an additional layer of protection, the Security Key might be for you.

The Security Key generates a random security code that you enter along with your PayPal username and password. It's easy to use, and it even works with your eBay account.

We can send your security code to your mobile phone by SMS message or you can order a credit-card size Security Key to carry with you.

- There's no fee to use your mobile phone as your Security Key but standard text messages rates apply when you receive a secure code by SMS. Check with your mobile provider for details.
- The portable, credit-card size Security Key has a one-time fee of \$29.95.

[Get one today](#) or visit the [FAQs page](#) for more information.


www.urf.com Log Out | Help | Security Center Search

PayPal

Security key setup

Order a new security key, register your mobile phone, or activate a security key you already have. [Learn more about Security Key](#)


Order
PayPal security key



Order

[Get the PayPal Security Key](#) for an extra layer of protection: every time you log in to PayPal.

Order
SMS Security Key



Order

[Use your mobile phone](#) to receive an SMS message with a secure code every time you log in to PayPal.

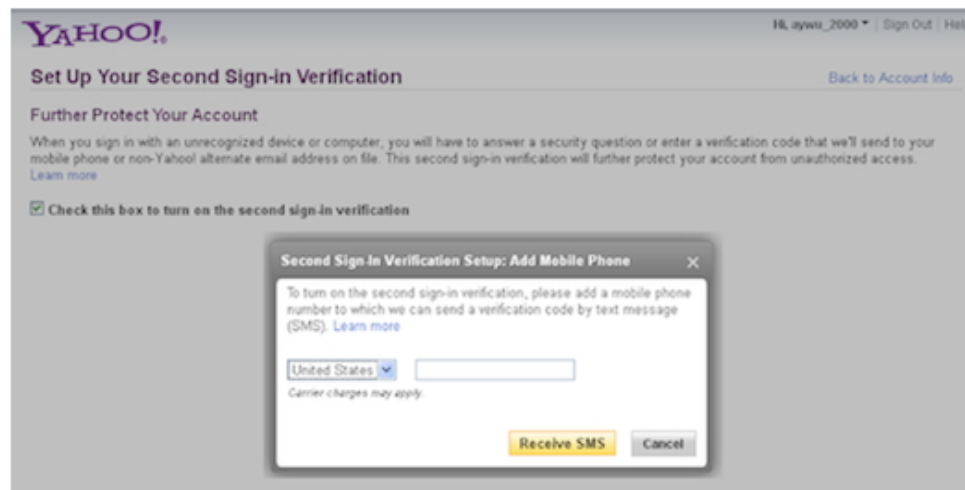
Y A H O O

Yahoo! Introduces Stronger User Authentication – Second Sign-in Verification

Posted December 13th, 2011 at 10:00 am by [HuongT](#) Categories: [General](#)

Online account compromise occurs regularly and will probably continue in the foreseeable future. Often hackers employ [botnets](#) to hijack accounts from millions of unsuspecting consumers. In turn, these hijacked accounts are sold and used to initiate email scams, with messages seemingly sent from the legitimate account owners to their contacts. Scams can range from the less harmful "check this cool stuff" advertising spam to the more damaging "send money to help your friend" email. Worse still, the scam emails may contain malicious links that lead to the installation of malware on computers, which then makes the computers part of the ever-growing botnet networks.

To thwart account compromise, Yahoo! is introducing a stronger user authentication feature that aims to prevent account hijackers with a stolen password from accessing a person's account. If you have a Yahoo! account, you can now further protect it by activating this new [second sign-in verification](#) feature from [Yahoo! Account Info](#). As part of the process, you will be required to add a mobile phone number to your account and verify it via SMS.



Once the feature is turned on, any suspicious account sign-in attempt will be challenged by a second sign-in verification beyond the initial password validation. To confirm the legitimacy of the sign-in attempt, you or the hijacker will have to answer your account security question or enter a verification code that will be sent to your mobile phone. Presumably, only you, as the legitimate user, can sign in. Account

A Noteworthy Point of Commonality: Mobile Phones

- If you look at the multifactor services that Google, Apple, and all the other commercial services are deploying, there's one factor that really jumps out: they're ALL deploying mobile phone-based solutions, just as InCommon is with its multifactor offering from Duo Security.
- Using a mobile phone-based solution has multiple advantages, including being cost effective, but also introducing a second independent channel, making it harder for malware to subvert your authentication process.

Are You Using Multifactor Authentication With These Or Other Popular Consumer ISP Services?

- If so, we'd love to hear about your experiences with them, if you're willing to share your point of view. (Our general assumption is that these services typically have some of the most carefully engineered multifactor deployments in existence, so we'd like to glean any lessons we can from them)
- If you're not using multifactor authentication with those services, or on your campus, we'd like to understand why not.

There Can Be Many Reasons Why a Site Doesn't Deploy Multifactor Authentication

- Some of those reasons may relate to people/processes/funding; other issues may relate to technology, or something else entirely. The critical reason (or mix of reasons) may vary widely from site to site, and may evolve over time.
- We know (or at least we've know we've repeatedly heard) that sometimes folks think that the decision to deploy (or to not deploy) multifactor authentication is one that rests with just one person, perhaps the institution's chief information security officer (CISO). We believe that's an oversimplified decision making model.
- We believe that many people actually help make decisions about multifactor (or may drag their heels and resist multifactor authentication deployment)...

Some of the People Who May Gate the Decision To Deploy (Or To NOT Deploy) Multifactor Auth

- **CIO (and above):** Is information security an institutional priority? Is there interest in (and funding for) a multifactor initiative?
- **Security Team:** What MFA technology does the security team trust? Are there other security projects that are a higher priority?
- **Identity Management:** Does the multifactor technology integrate with the ID management team's strategies and pending projects?
- **Systems Staff:** Is the multifactor technology easy to integrate and use with the systems that the systems staff administer?
- **User Support Staff:** Will users "melt the help desk phones," struggling to use the new multifactor authentication technology? Who will produce local documentation and do local training on it?
- **Users:** Will average users (as well as highly influential opinion leaders) accept, or at least tolerate, a new MFA deployment?

Suggestion...

- If you want to deploy multifactor authentication on your campus, but things haven't been going well to-date, could it be that you don't have all the right folks talking?
- Would it help to be able to trade notes and share war stories with others from the community? If so, please consider joining the Multifactor Cohortium, see <https://spaces.internet2.edu/display/scalepriv/Multi-factor+Authentication+in+Higher+Education+--+MFA+Cohortium+and+Pilots> (If that long URL gets munged, you can also try <http://tinyurl.com/cohortium> to get to the same site)
- That project is part of the work enabled by the NSTIC Scalable Privacy grant obtained by Ken Klingenstein of Internet2.
- Campus communication issues aside, there are plenty of other issues that may also at least temporarily stall deployment of multifactor authentication...

If Sites Aren't Using Multifactor, Is It Because They...

- Don't really think they're at risk?
- Find it too inconvenient for something used all the time?
- Worry they'll lock themselves out of their own accounts?
- Think that multifactor is too expensive?
- Worry that deploying multifactor will make their authentication infrastructure more fragile/less robust somehow?
- Think that multifactor is too hard to deploy in a scalable way?
- Believe that multifactor product doesn't integrate well with the systems that need to be secured, right out of the box?
- Have privacy concerns?
- Poor availability/performance in some locations (e.g., for phone-based solutions?)
- Let's consider some of those possibilities...

1. "My Account Isn't Really At Risk"

- Hypothetically, some users might say:

"I really don't feel as if I'm at risk of having my account hacked. Other people – people like movie stars or prominent politicians – they might be at risk, but who really cares about me or wants my Gmail account? I just don't think account hijacking is a very big risk for me."

- What do folks think? Is that statement about right? Do you think it's as true for your **university account** as it is for your Gmail account? More so? Less so?
- What about accounts for your senior people (Chancellor/ President/Provost, etc) – are they almost like movie stars or prominent politicians, in terms of being targets for attacks?

What About Phishing?

- If you really believe that your users aren't at risk, that must mean that you don't routinely see phishing attacks targeting them.
- Unfortunately, I think that most schools **do** see phishing attempts, and most schools, including those with aggressive training and awareness programs, still see at least some of their users victimized by it (the nicer and more compliant your users are, the bigger a problem phishing can be).
- I'd urge anyone who thinks that the bad guys aren't interested in university accounts, including your school's accounts, to think again. The bad guys love getting fast systems that are connected to big network pipes.

And What About Compliance?

- Even if you don't believe that there are substantive security risks (such as phishing) that are sufficient to motivate you to deploy multifactor auth, compliance requirements may effectively take the decision out of your hands.
- For instance, PCI DSS section 8.3 explicitly requires the use of multifactor authentication for remote access.
- In other cases, such as those working with protected health care-related information subject to HIPAA, the need for multifactor authentication is generally understood and accepted by those in the industry, based on the goals and objectives of the act. That may be important if your school has a hospital, clinic, or other medical facility on campus.

2. "Doing Multifactor Is Too Inconvenient"

- Another commonly heard reason for not doing multifactor authentication goes something like this:

"I don't want to have to go around copying some goofy code all the time. I just want to click on an icon, be logged in, and get at my stuff. Multifactor is just too inconvenient for me."

- I can certainly believe that some folks have had this experience. If you need to enter (and reenter!) six digit codes all the time, it can quickly become burdensome – but what about a model like Google's, where you only enter a confirmation code **once** from each new system you use? Would even that still be too hard?
- Or what if you didn't have to transcribe a number across at all?

Easy-Peasy: Push A Button To Allow or Deny Access

- Duo Security, one of the multifactor authentication services offered through InCommon, is a phone based multifactor solution. But, as Duo is usually used, it doesn't require the user to transcribe a number from their mobile device in order to login.
- In Duo's case, if you're on a smart phone, such as an Apple iPhone or an Android device, you can simply download and run a special app that will popup at login time.
- When that app runs, it gives some details about the connection that's in progress and then essentially asks, "Do you want to permit this login?" Users can push a green "Yes" button, or a red "No" button. It is hard to imagine any interactive multifactor approach that could be simpler.
- For information, see <http://www.incommon.org/duo/> or watch the demo at <http://www.youtube.com/watch?v=23MCmlaSmTk>

3. "I'm Going to End Up Locking Myself Out!"

- In talking with users, another scenario that some folks worry about is getting accidentally locked out if they forget their phone (or other hardware multifactor device) at home.
- In the best of cases, you can quickly pop back home to retrieve the forgotten device, or a system administrator may be able to temporarily override your normal "multifactor device required" setting. However, if you forget a key device while traveling (particularly on long trips), that can be a bit more problematic.
- But does this worry really have to be a "show stopper?" What if you can carry a sheet of backup access codes in your purse or wallet, just in case? Or what if you could register your cell phone number AND your desk phone number, using either of them to let you login? Or maybe you could register a backup contact person's phone number, for an emergency "phone-a-friend" assist?

Avoiding Lockouts With Duo

- There are many ways that you can avoid lockout conditions when using Duo, including:
 - registering multiple devices (your cell phone, AND your desk phone, your home phone, the phone number of a trusted loved one or friend, etc.)
 - carrying a sheet with a list of backup SMS codes in your purse or wallet
 - knowing how to contact the local Duo administrator for your site (they can give you a temporary bypass code if you need one, assuming they're able to verify your identity to their satisfaction)

4. "It Costs Too Much To Do Multifactor Auth"

- All of the major multifactor consumer services mentioned in the first section of this talk are free. If you're not using multifactor with **those** services, the real issue **can't** be cost, right?
- One possibility, I suppose, is that some folks may not have a cell phone (do those sort of people still exist?), or if they do have a cell phone, they only have a personal one, not a university-issued and funded one. In that case, I suppose that some users might resent their employer attempting to "take advantage" of their personal cell phone, or some users might understandably be reluctant to pay out-of-pocket fees for any per-message SMS charges, etc.
- And it is true that some traditional hard cryptographic token solutions can be rather pricey

What Would It Cost to Deploy DuoSecurity?

- If you just want to try Duo, you can do up to 10 users for free.
- InCommon participants can deploy Duo for 500 users or more for just \$5 per user per year with no paperwork or special agreement required. I think that's an incredible bargain.
- If you want to cover all your site's users, a Duo site license will usually make financial sense. For example, if you come from a school that has 20,000 to 34,999 students, and you wanted to cover all your faculty/staff/students (except hospital staff, who need to be licensed separately), and your school is a member of Internet2, you'd pay just \$40,000/year (only \$1-\$2/user/year). A small Internet2 school (<2,500 students) would pay only \$4K/year.
- Note: some Duo methods, such as automated voice phone calls or SMS messages, will require sites to also purchase inexpensive telephony credits. See <http://www.incommon.org/duo/fees.html>

Why Would Anyone Pay to Deploy Duo When They Could Get Google Authenticator For Free?

- You may know that you can get Google Authenticator for free from <http://code.google.com/p/google-authenticator/>
- Given that, some may ask, "Joe! Why would we buy Duo when we can just run the free Google Authenticator application, instead?"
- First of all, note that while the Google Authenticator software is free, you still need hardware to host the backend infrastructure that Google Authenticator needs. That hardware will not be 'free' – you'll need the hardware itself, and you'll need someone skilled and trustworthy to administer it. In many scenarios, these costs may dwarf the cost of simply deploying Duo.
- And then there's the somewhat disquieting note on the Google Authenticator project site mentioning that you can download the 2.21 version of the code, but not more recent versions due to proprietary bits and pieces it includes (a real bummer IMHO).

5. "A Multifactor Service Hosted In The Cloud Might Leave Us Unable to Login If We Got DDoS'ed..."

- If the ability to login to critical local services relies on the continued ability to contact a remote multifactor service provider, a local DDoS might make it impossible for users to login locally
- What happens in that case depends on how you have your cloud-based multifactor service configured.
 - One possibility is that you will have the service set to "fail closed," in which case you would be unable to login until the DDoS is abated, or the admin temporarily disables the requirement for multifactor use.
 - You could also set the service to "fail open" if the remote multifactor service can't be contacted, accepting the loss of multifactor protection when/if the site suffers a DDoS attack (perhaps a bad idea since it incents DDoS attacks)
- Alternatively:
 - You might prefer to locally host your backend multifactor infrastructure, or
 - You might want to provision dedicated network capacity reserved just for accessing the multifactor provider if a network emergency were to arise

6. "Deploying Multifactor Authentication on Service-By-Service Basis Just Doesn't Scale..."

- In some cases, system administrators need to tweak each and every service on a service-by-service basis to enable multifactor authentication. If you have a lot of services, this can be tedious.
- On the other hand, imagine a scenario that decouples identity providers and service providers, as federated login does.
- In that case, you can imagine enabling multifactor authentication **once**, at your IdP, and then being able to leverage that multifactor support on each and every service that trusts that IDP without having to do a tedious service-by-service rollout on each of the SPs themselves.
- Fortunately, Duo has a login handler that integrates Duo with Shibboleth, see <https://www.duosecurity.com/docs/shibboleth> if you'd like to try doing this.

"It's a Pain To Have To Issue Hard Tokens To All My Users"

- If you need to physically visit with each user to issue them a hardware cryptographic token, this is indeed a pain, basically kin to users needing to arrange to get a key for their office or residence hall room. That can be (and obviously is) routinely done, but usually everyone dreads the process since it often is time consuming and tedious, particularly during start of term times.
- Fortunately, Duo leverages a "TOFU" (trust on first use) model, allowing users to register their mobile device the first time they login after Duo is enabled for their account. This eliminates the need for users to visit an accounts clerk or help desk at the time they're getting started with multifactor. This may be particularly important if you're working with distance education students who may rarely be on campus...

7. "The Multifactor Solution We Looked at Didn't Integrate Well With Our Systems..."

- It's easy to forget that there needs to be some way to tell servers that they should be doing multifactor auth. That is, sysadmins need to be able to easily enable multifactor auth via PAM or whatever authentication system their server, router, VPN, or other device uses.
- Some multifactor solutions have login handlers for "everything" right out of the box, but some others may only support a small subset of those devices. If you pick the wrong multifactor solution, you could potentially spend a lot of time doing custom integration.
- At least in the case of Duo, happily enough, it integrates out of the box with pretty much everything our community uses: popular web servers, Unix/Linux servers, Microsoft servers, VPNs, Python, Ruby, PHP, Java, .NET, etc. See "Solutions → Platforms" on the Duo web site, <https://www.duosecurity.com/>

8. "What About Privacy? (My Phone #, Etc.)"

- Privacy-oriented individuals may be concerned about the fact that their phone number gets disclosed to the multifactor provider as part of registering for phone-based multifactor authentication.
- We believe that this concern can be mitigated by an appropriate control, such as a strong multifactor provider privacy policy (see Duo's privacy policy at <https://www.duosecurity.com/privacy>)
- Choice of evils argument: we'd also urge you to contrast two radically different potential privacy breach scenarios:
 - An account that is not using multifactor is compromised, and all account contents (including confidential email, personal photographs, unpublished writings or discoveries, etc.) get exfiltrated; this would be difficult to overcome, and unfortunately this is not at all an uncommon scenario.
 - A phone-based multifactor company somehow leaks or improperly employs registered customer phone #s; this has never happened to the best of our knowledge, but if it did, you could always just change your phone #.

9. "My Cell Doesn't Get Any Bars Where I Work!"

- We know that cell coverage can be imperfect, particularly if you work in a reinforced concrete structure, in a basement lab, or in some rural areas. In other cases you may not be able to bring a cell phone into an area full of sensitive equipment or into highly secure areas. Despite those challenges, you still need to login.
- Duo has a solution for those scenarios, too.
- Even if your phone isn't able to connect to the cellular network or to a local WiFi network, you can still run a soft token app on your phone to generate a traditional six-digit code for login purposes.
- If cell phones are disallowed where you work, Duo can also use a traditional hard crypto token, instead.
- If even that won't work for you, you can fall back to a sheet of pre-generated one time codes that you can carry on your person.

10. "What About Multifactor Auth To Secure Access Via A Smart Phone or Other Mobile Device?"

- We've been talking about using a phone-based solution to secure access via laptops, desktops, etc. That seems logically sound since the two platforms (e.g., the laptop and the phone) are physically separate systems. But these days, some users may not even be carrying a laptop – they may just do all their work via their smart phone or tablet.
- When that happens, it raises the question, "What if I need to secure network access that's taking place via a user's smart phone or other mobile device?" Do users now need two smart phones, one to vouch for the other? (This doesn't seem reasonable to me)
- Or are we comfortable having both factors (e.g., the user's password, persistently stored in applications on the user's device, and the user's device itself), serving as the "multifactor" solution?
- What do folks think?

That's Not An Exhaustive List of Considerations

- While we've talked about a number of considerations that may arise in thinking about multifactor authentication, please don't consider the preceding list to be exhaustive.
- For example, what about non-interactive logins to things like POP/IMAP (e.g., to retrieve a user's mail)? Will those logins need to be secured with multifactor, too? If not, why not?
- If you work with multiple sites, and they all use the same phone-based multifactor system, can all those instances coexist on the same phone? (In the Duo case they can)
- When we deploy a multifactor authentication solution, do we just want it to secure the normal login process, or do we want it to do something more, too, like enabling digital signatures, or serving as the basis for a general campus-wide ID card, too? If so, a phone-based solution may not meet all your needs.

III. Client Certs

Phone-Based Solutions Aren't The Only Solution

- While phone-based solutions appear to be glowing white hot this year, there *are* also other multifactor options.
- For example, you might consider deploying client certificates, instead of doing a phone based solution. Client certs are available as part of the InCommon Certificate Program, bundled at no additional charge along with the more common SSL server certs. See <http://www.incommon.org/certificates/> for details about the Certificate Program
- We don't have time to do a deep dive into client certs as part of today's session, but you can see an earlier tutorial that I did on them for the Security Professionals Meeting last year:
<http://pages.uoregon.edu/joe/secprof2012/sec-prof-2012-client-certs.pdf>

Where Are We Going To Store Our Client Certs?

- One consideration that immediately arises when it comes to client certificates is the question of where they're going to be stored.
- You can store them directly on each end user's devices, but if you want to do that, you need some way to get their certificates installed in the trust repositories on each of them. While this can be done manually, it is a process that's tedious and arcane, and not something that your help desk would want to walk someone through over the phone.
- Historically, sites that have deployed client certs on-device at scale, have done so via locally written custom installer scripts. Unfortunately, most sites do not have the local expertise to craft and maintain such a script locally. You can buy a commercial certificate dropping tool such as XpressConnect from CloudPath (see <http://www.cloudpath.net/>), but some sites might want an alternative option.

InCert(tm)

- In partnership with Indiana University and with the assistance of the University of Virginia, InCommon arranged for production of a custom (and customizable) open-source certificate installer, called InCert(tm), that includes the ability to do basic device onboarding tasks as well as dropping certs.
- That project is currently in pilot phase. An FAQ is available at <http://www.internet2.edu/incert/faq.html> and you can see a description of current InCert(tm) functionality at <http://www.internet2.edu/incert/functionality.html>
- If you'd be interested in being considered for participation in the pilot, please see <http://www.internet2.edu/incert/> or write to incert-info@internet2.edu

SafeNet Hard Tokens and Smart Cards

- Other sites may prefer to store their client certs on USB-format hard tokens or smart cards. While USB-format hard tokens look just like a regular thumb drive, and smart cards look very similar to a normal mag stripe card, in each case the device actually includes special federally-certified cryptographic processing capabilities and secure storage, making them a very secure option for storing client certs.
- Sites interested in learning more about SafeNet PKI hard tokens and smart cards available from InCommon should see <http://www.incommon.org/safenet/>
- We've recently added the ability to do SafeNet token customization if your site requires a particular configuration that isn't adequately address by a stock SKU (additional fees apply).

For more information, please contact admin@incommon.org

Multifactor and SP 800-63 LOAs

- The Assurance program (<http://www.incommon.org/assurance/>) currently offers Bronze and Silver Assurance profiles, equivalent to NIST 800-63 LOA 1 and LOA 2. Neither of those profiles requires multifactor, although some may use multifactor authentication to easily meet and exceed the requirements of those specifications.
- If the InCommon community has a need for higher levels of assurance, such as an LOA 3-ish "Gold" profile, multifactor will be needed (there's a lot more to those higher levels of assurance beyond just use of multifactor, but multifactor is definitely a requirement). If the community needs an LOA 4-ish "Platinum" profile, client certificates on hard tokens or smart cards are effectively the ONLY multifactor technology that will meet NIST 800-63 LOA 4 requirements.
- **Question:** Does the community want/need LOA 3 or 4? If so, for what sort of application/use case?

IV. Other Multifactor Options

Should InCommon Offer Other Multifactor Options?

- Currently we have a phone-based multifactor offering, and a client certificate-based multifactor offering.
- Should InCommon have other multifactor options, too? For example:
 - Is there community interest in InCommon offering a biometric multifactor offering, such as a fingerprint-based solution, or an iris camera-based solution?
 - Or should we be looking at multifactor solutions that integrate well with some of the leading commercial multifactor programs, such as Yubico's one-touch hardware devices, as featured in "Google Declares War on the Password," Wired Magazine, <http://www.wired.com/wiredenterprise/2013/01/google-password/>

We Need Your Input and Feedback

- We'd love to hear from you about what you'd like to see available for your campus.
- What do you need? What have you tried? What worked, and what didn't, and why?
- We recognize that multifactor authentication can sometimes seem dauntingly complex, but truly, it doesn't need to be.
- Thanks for the chance to talk today!
- Are there any questions?