

# Flexible Vetting: Using a point System to Verify Identity

Jesse Rankin & Bert Bee-Lindgren

Georgia Tech

InCommon Assurance Call – May 6, 2015

# Agenda

- History
- Theory
- Practice
- Future

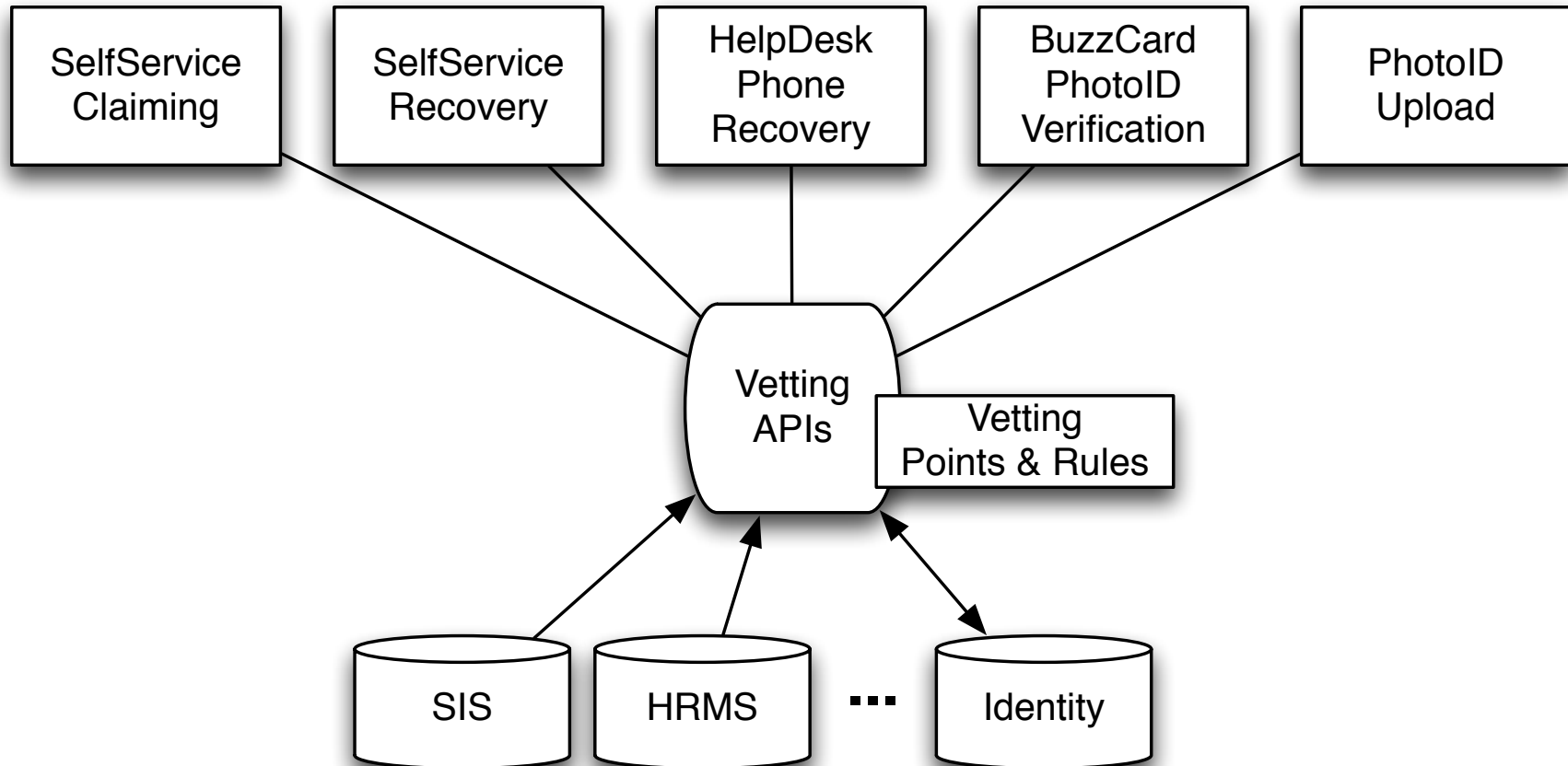
- Self-service password recovery, v1
  - Same Security for everyone
    - “A Google incident cannot lead to a FERPA report”
      - GT Registrar
    - Security Question, Shared secret, Repeat
    - ➔ Low success, helpdesk rates still high
- Pressures to improve
  - Affiliation growth, far beyond students & employees
    - Parents, applicants, guests, alumni, former employees, retirees, online students, etc
  - Competition
    - Beyond kneejerk “My bank is easier than this”
    - Continuing-education alternatives
    - Separate alumni accounts

- Vetting security should be proportional to the account's access
  - Email verification ...or... Several rounds of questions
  - Or, sometimes, in-person process is required
- Affiliations approximate security requirements
- Many password-recovery processes
  - Self Service, IT Helpdesk, Registrar, PE, Delegated Admins
- *Endless* conversations can actually lead somewhere
  - General agreement quickly, the rest took 2.5 years

- Assemble “questions” from many places
  - Enterprise: SIS, HRMS, Data Warehouse
  - Alumni
  - BuzzCard
  - Housing
  - Identity
- Score the questions
  - Security value
  - Difficulty
- Security levels assigned to Affiliations & Apps  
(Vetting disabled for some people)

- Phone (voice/text)
- Email
- Address (MC)
- Plain answer

# Result: Flexible Vetting



## Enter your GT Account and Password

GT Account

Password

Login

Passport offers tools for GT Account password changes, email aliasing and GT Directory options.

[I need to activate my GT Account](#)

[I don't know my GT Account username](#)

[I have forgotten my GT Account password](#)

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

## Claim Your GT Account

### What is your relationship to Georgia Tech?

Please select an option to continue.

#### Students

People attending Georgia Tech as a Credit, Language Institute, or Professional Education Student.

#### Employees

People working at Georgia Tech: Faculty, Staff, Tech Temp, Affiliate, etc.

#### Student-employees

Students who are employed by Georgia Tech.

#### Applicants

People with an undergraduate or graduate application for a future semester.

#### Alumni

People who attended Georgia Tech as a Credit Student.

#### Guests

People with accounts sponsored by Georgia Tech Employees or Students.

#### None of the above

People with a Georgia Tech relationship not mentioned above.



## Claim Your GT Account

Please fill in as much of the form below as you can. The information will be used to look up your record in the GT system.

First Name

\* Last Name

Date of Birth

 /  / 

gtID Number

Number on the front of your BuzzCard or other Georgia Tech paperwork in 90XXXXXXX format. Please do not enter your Social Security Number.

[Lookup](#)

[Cancel](#)

### Results:

<b>Jesse V Rankin</b> Appl Developer Sr Staff in OIT-Enterprise Information Sys	<a href="#">This is me</a>
<b>[REDACTED] Rankin</b>	<a href="#">This is me</a>
<b>[REDACTED] B Rankin</b>	<a href="#">This is me</a>
<b>[REDACTED] Rankin</b>	<a href="#">This is me</a>
<b>[REDACTED] Rankin</b>	<a href="#">This is me</a>
<b>[REDACTED] Rankin</b>	<a href="#">This is me</a>
<b>[REDACTED] Rankin</b>	<a href="#">This is me</a>

## Claim Your GT Account

for **Jesse V Rankin** This isn't me

### Select a GT Account

jesse

Select this account

jrankin31

Select this account

**jrankin** (Primary account)

Select this account

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

# Vetting Demo: Phone & Email

Please select the first method you'd like to use to confirm your identity:

## Call or text your phone

We'll send an SMS text or make an automated call with a PIN number to the phone number listed below.

(\*\*\*) \*\*\*-\*\*-31

[Text This Number](#)

[Call This Number](#)

## Send an Email

We'll send an email containing a PIN number to the email address of yours that you select below. For your security, the full addresses are not listed.

- j...@o...g...edu
- j...@gatech.edu
- j...@m...g...edu
- j...@gmail.com

[Email Selected Address](#)

[None of these options work?](#)

## Reset Your GT Account Password

GT Account jrankin for Jesse V Rankin This isn't me

### Step 2 of 3: Confirm your ownership of this GT Account

#### Enter PIN Number

You should receive an sms text at (\*\*\*) \*\*\*-\*\*31 momentarily with a PIN number. Please enter the PIN number below to continue.

\* PIN Number

Submit PIN

Back

If you haven't received the PIN after more than a minute: [Resend text](#)

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

## Reset Your GT Account Password

GT Account `jrankin` for **Jesse V Rankin** [This isn't me](#)

### Step 2 of 3: Confirm your ownership of this GT Account

Please answer the question below to continue.

What are the last four digits of your Social Security Number?

Submit your answer

I don't know the answer to this question

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

## Reset Your GT Account Password

GT Account `jrankin` for **Jesse V Rankin** This isn't me

### Final Step: Set your GT Account password

Please enter the password you would like to use to access GT services. Note the password requirements below.

\* **New password**

\* **Confirm new password**

- Must be between 11 and 23 characters in length
- Must contain characters from at least 3 character classes (see below)
- Cannot contain your name or your GT Account username
- Can only contain characters printed on the computer's keyboard

Set password

#### Suggestions for picking a strong password:

1. Think of an easy-to-remember phrase
2. Combine the first letters of each word

## Reset Your GT Account Password

GT Account jrankin for Jesse V Rankin This isn't me

### Step 2 of 3: Confirm your ownership of this GT Account

We did not receive enough information to claim your account.

#### Try again

You can restart the verification process from the beginning if you'd like to try again.

[Restart the verification process now](#)

Or submit an image of your valid, government-issued photo ID

[Go to the photo ID submission form](#)

For assistance, please contact the [OIT Technology Support Center](#) at 404-894-7173 (Mon-Fri 8am-5pm EDT).

# Vetting Demo: PhotoID Upload

GT Account jrankin for Jesse V Rankin This isn't me

## Submit A Photo of Your ID

You can use the form below to submit a photo of a government-issued photo ID that we can use to confirm your identity.

- Please submit a photo of a government-issued photo ID (Some examples are your Drivers License, Passport, or State ID).
- Please ensure that the text on your id is clear and legible in your photo.
- File formats allowed are JPEG, PNG, and GIF.
- Uploaded files can be no larger than 2 MB.

**After you submit this form, we'll call you at a convenient time to complete the process.**

\* Contact phone number

\* When is a good time to call you?

(please specify timezone)

Must be within the operating hours of the Georgia Tech Technology Support Center, Monday - Friday 8am - 5pm Eastern Time

\* Your photo image file

No file chosen



0 of [redacted] required points

Accounts of faculty/staff/TechTemp employees must be at strength 80

**Phone Confirmation:** Please confirm the PIN that we send to your phone number.



**Option:**

+1 404 [redacted] 31

Call phone with PIN

Send PIN via SMS text

Value: [redacted]  
Difficulty: 1

**Last four of SSN:** What are the last four digits of your Social Security Number?



Enter answer

**Answer:** Not shown: Enter value to check

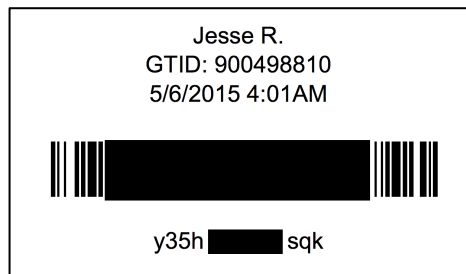
This question has been asked without a correct response 1 times:

Value: [redacted]  
Difficulty: 1

- Problem:
  - Applicants have lower vetting requirement than Students
  - Accounts don't magically become more secure
- Solution:
  - Piggyback on BuzzCard process: **ID Checking**
  - Mark account “vetting\_strength=100” after Student with PhotoID enters Password

## 1. Photo ID Check

- Barcoded receipt after PhotoID is checked



## 2. Kiosk

- User scans Receipt, enters Account Password

## 3. BuzzCard Desk

- Uses receipt, takes picture and prints card

- More data sources
  - Social & InCommon account binding
  - Browser cookies
  - ...
- Alumni: Full vs Partial Access
- Remote Students
- Security requirement
  - Compute from Account's privileges (instead of ePA)
  - Consider recent authentication requests
- MFA
  - (NOT: Using token as a recovery question)
  - Lower vetting requirements of MFA-protected accounts?
- BuzzCard issuance, v3
- Phone-a-friend

# Providing Comments on NIST 800-63-2

---

JACOB FARMER

CHAIR, ASSURANCE ADVISORY COMMITTEE



Please browse to:

[http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2\\_call-comments.html](http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html)


Or

<http://1.usa.gov/1CGNC8P>

(these go to the same page)



What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction?  
How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?



Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?





What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.



What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?



What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?



Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions?  
What form should that representation take?



What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

