

# Identity Verification


## Identity Verification

Identity Verification is a bootstrapping process for InCommon Executives, Site Administrators (SAs), and Registration Authority Officers (RAOs). Initially, when an organization joins InCommon, the Executive identifies SAs and RAOs by securely providing us with their email addresses and phone numbers, but before an SA can administer metadata or an RAO can issue certificates, the administrator must **verify their identity**. That is, an SA or RAO has to prove they control the email address and phone number given to us by the Executive. This page describes that process in detail.

To verify your identity, follow these steps while in the vicinity of your designated phone:

1. Verify your email address:
  - a. **Request an email invitation** by entering your email address at the prompt and pressing the button. ([screen shot](#))
  - b. **Click the link in the email** to launch a secure landing page in a browser window. ([screen shot](#))
2. Verify your phone number:
  - a. **Request an one-time PIN** by pressing a button that sends a PIN via an automated voice message to your phone number. ([screen shot](#))
  - b. **Verify the one-time PIN** by entering it on the web page and pressing the button. ([screen shot](#))

This completes the two-step identity verification process. If identity verification is successful, you will receive an email notification. Please report any problems or make suggestions for improvement by contacting us at [admin@incommon.org](mailto:admin@incommon.org)

 If your email address or phone number ever changes, talk to your Executive. Only your InCommon Executive may change an address of record.

## How It Works


The process of clicking a link in an email message is actually a type of federated login. Specifically, we implement a protocol called *Simple Authentication for the Web* [1] or SAW. You have probably used a simplified form of SAW to reset a password at one time or another on the web. It is the most common method of password reset in existence today. By itself, however, SAW is only as strong as the email account it depends on.

The [Duo Verify API](#) is used to generate the one-time PIN (OTP) sent to your phone. The system sends an OTP in a recorded voice message. (Duo Verify also has the ability to send an OTP to a mobile phone via SMS but the web app doesn't support that yet.)

Used together, SAW and Duo Verify provide **strong, two-step identity verification** capabilities.


## Phone Policy

Your verified phone number should not correspond to a mobile phone since mobile phones can be lost or stolen. In particular, if your verified phone number corresponds to a smartphone with email capability, and that phone is lost or stolen, a bad guy potentially has everything s/he needs to verify your identity. For this reason, we have the following policy:

 **InCommon Operations Phone Policy**

- It is strongly RECOMMENDED that your verified phone number correspond to an office phone with limited physical access and with no email capabilities.
- Your verified phone number SHOULD NOT be associated with a mobile device, especially one with email capabilities.
- If your verified phone is associated with a mobile device with email capability (which is strongly NOT RECOMMENDED), access to the mobile device MUST be locked with a passcode.

Once we roll out two-factor authentication on your login account itself, you will be asked to enroll a mobile device for authentication purposes. In most cases this device will be a smartphone. Assuming the device is a smartphone, **the phone number of the device used for two-factor authentication on your login account SHOULD NOT be the same as your verified phone number**. This is yet another reason why your verified phone number should not correspond to a mobile phone.

 To change your verified phone number, talk to your Executive. Only your InCommon Executive may change your contact information.

## References

[1] T. W. van der Horst and K. E. Seamons, "Simple Authentication for the Web," in *Intl. Conf. on Security and Privacy in Communications Networks*, 2007, pp. 473--482. <http://www.cs.bham.ac.uk/~tpc/cwi/Teaching/MASPPapers/EmailAuth.pdf>

File	Modified
PNG File demo-page-4.png	Jun 28, 2013 by <a href="mailto:trscavo@internet2.edu">trscavo@internet2.edu</a>

PNG File demo-page-1.png	Jun 28, 2013 by trscavo@internet2.edu
PNG File demo-page-2.png	Jun 28, 2013 by trscavo@internet2.edu
PNG File demo-page-3.png	Jun 28, 2013 by trscavo@internet2.edu
HTML File demo-page-4.html	Jun 28, 2013 by trscavo@internet2.edu
HTML File demo-page-1.html	Jun 28, 2013 by trscavo@internet2.edu
HTML File demo-page-2.html	Jun 28, 2013 by trscavo@internet2.edu
HTML File demo-page-3.html	Jun 28, 2013 by trscavo@internet2.edu

[Download All](#)