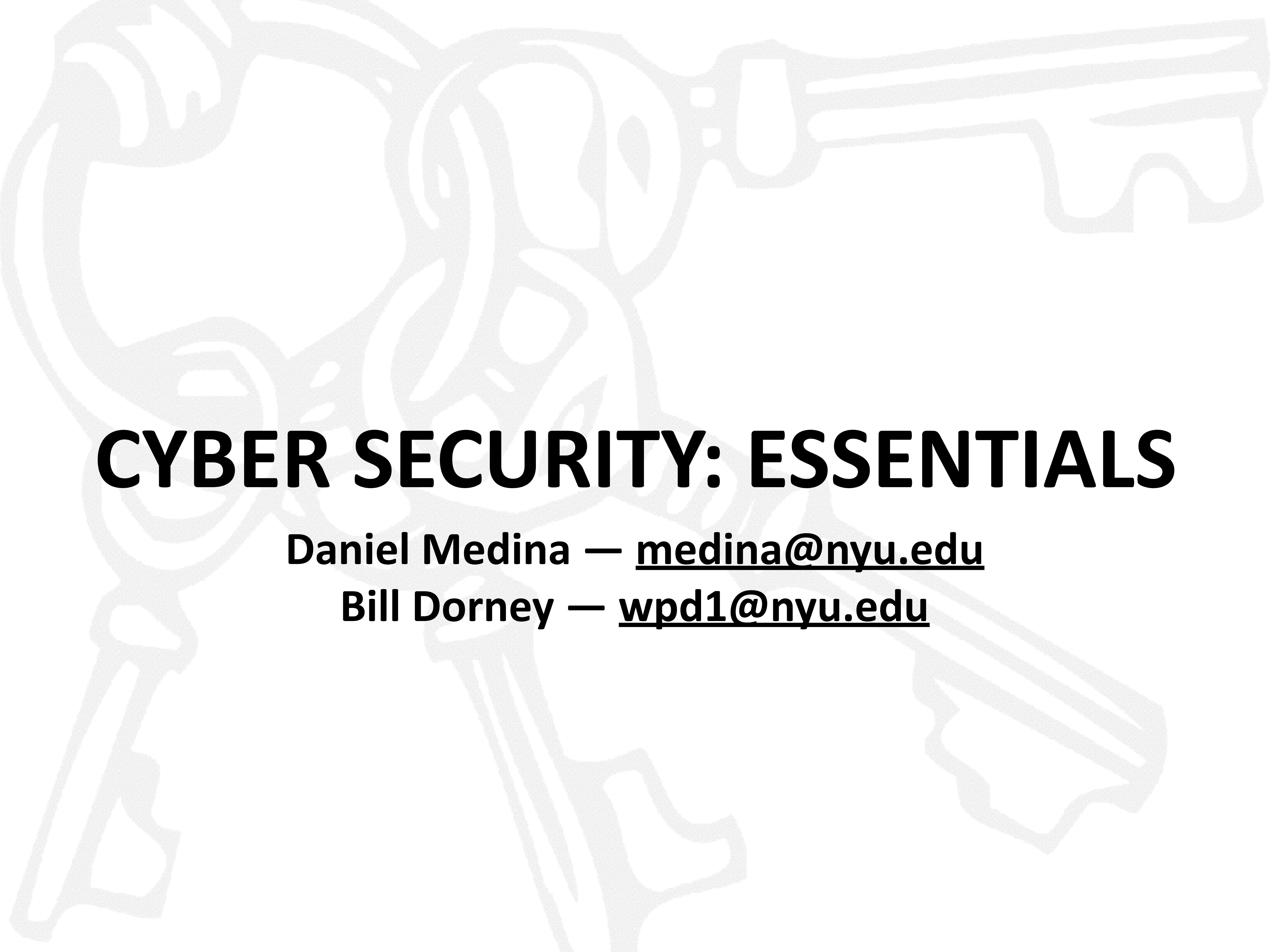
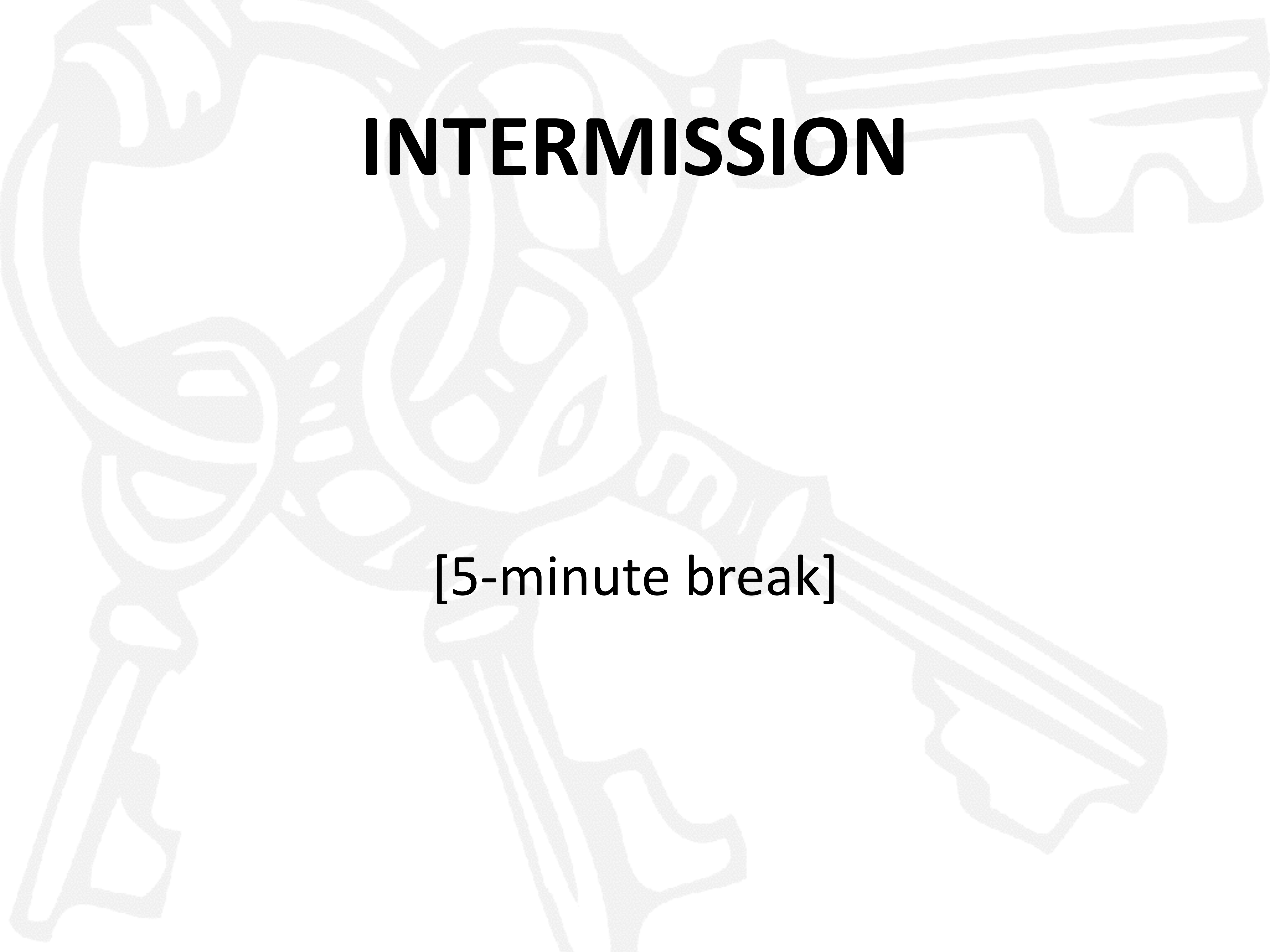


CYBER SECURITY: ESSENTIALS

Daniel Medina — medina@nyu.edu

Bill Dorney — wpd1@nyu.edu



INTERMISSION

[5-minute break]

NEWS

https://medina.github.io

RECAP

Lots of laws, regulations, and more

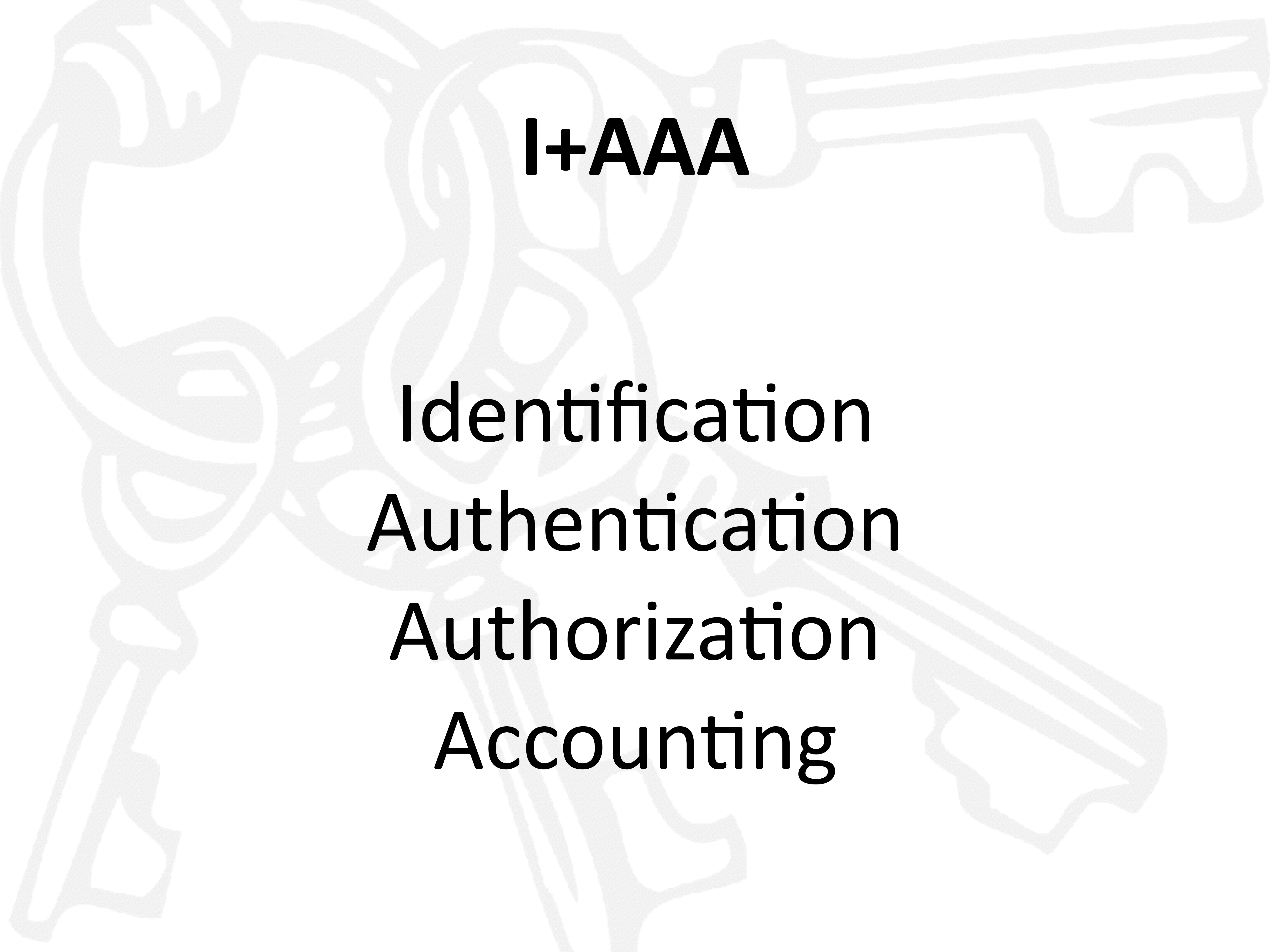
ADMINISTRATION

Have to talk about

final projects

make-up class

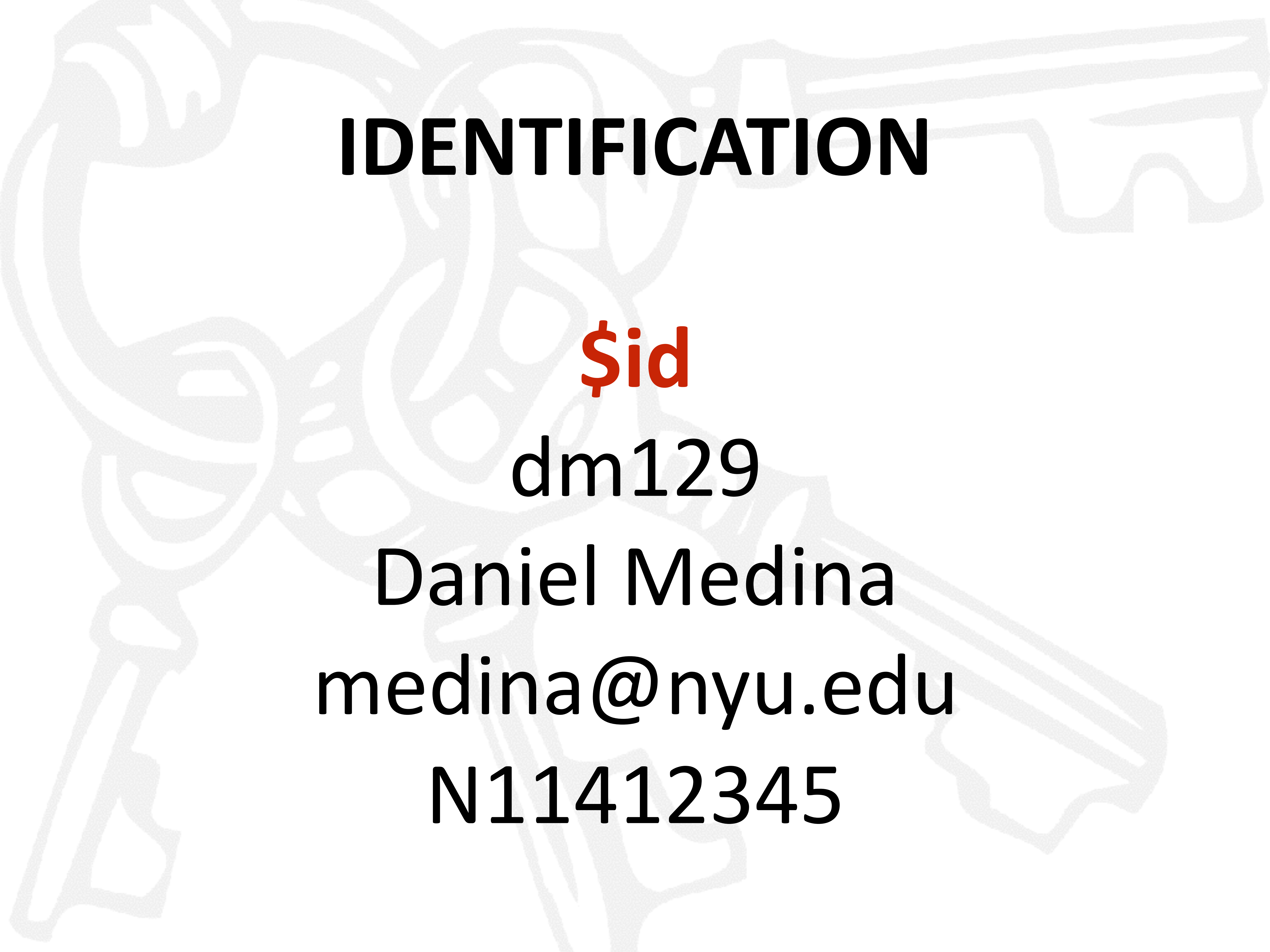
ACCESS CONTROLS



I+AAA

Identification
Authentication
Authorization
Accounting

IDENTIFICATION



$id

dm129

Daniel Medina

medina@nyu.edu

N11412345

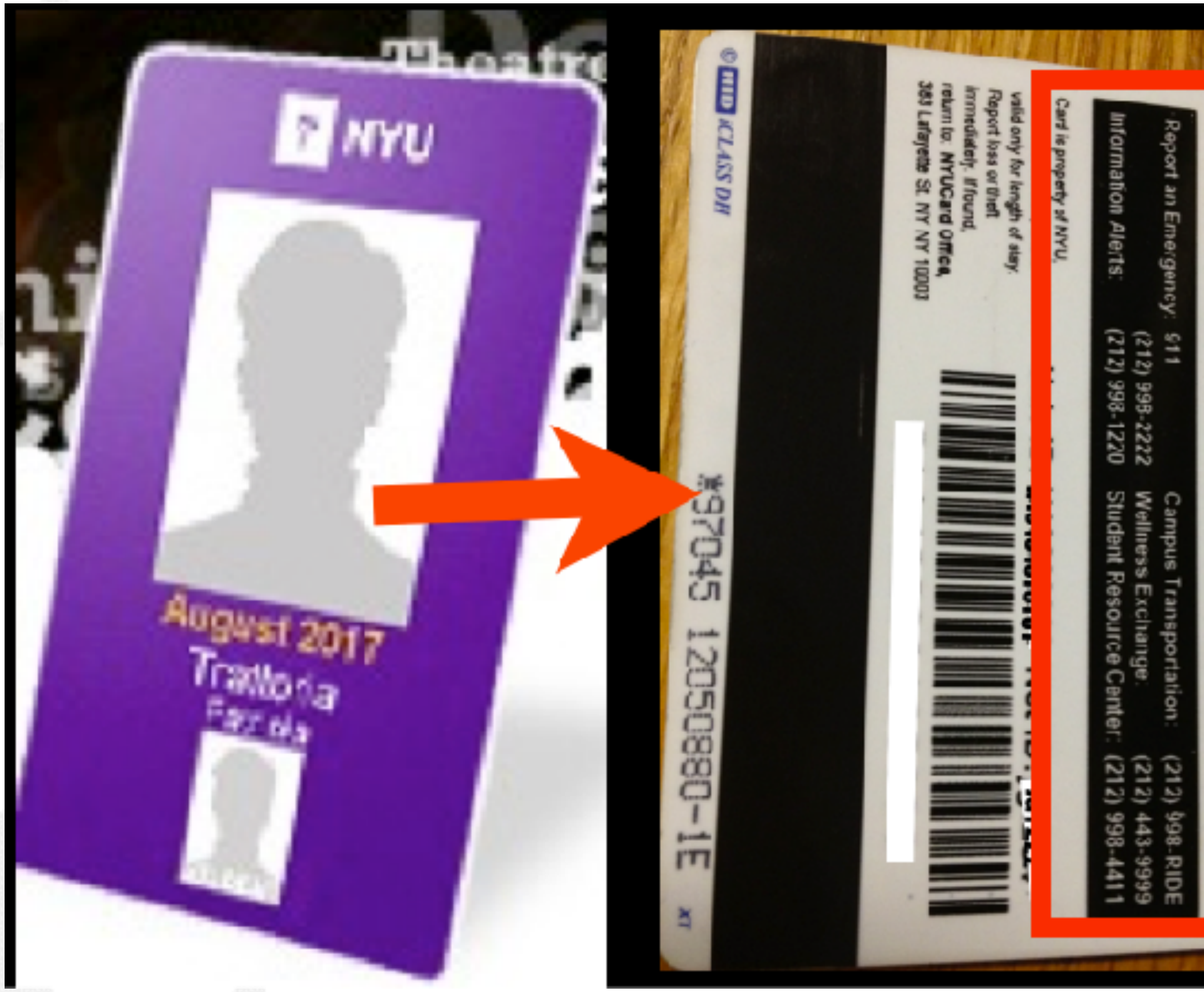
ASIDE: NYU ID

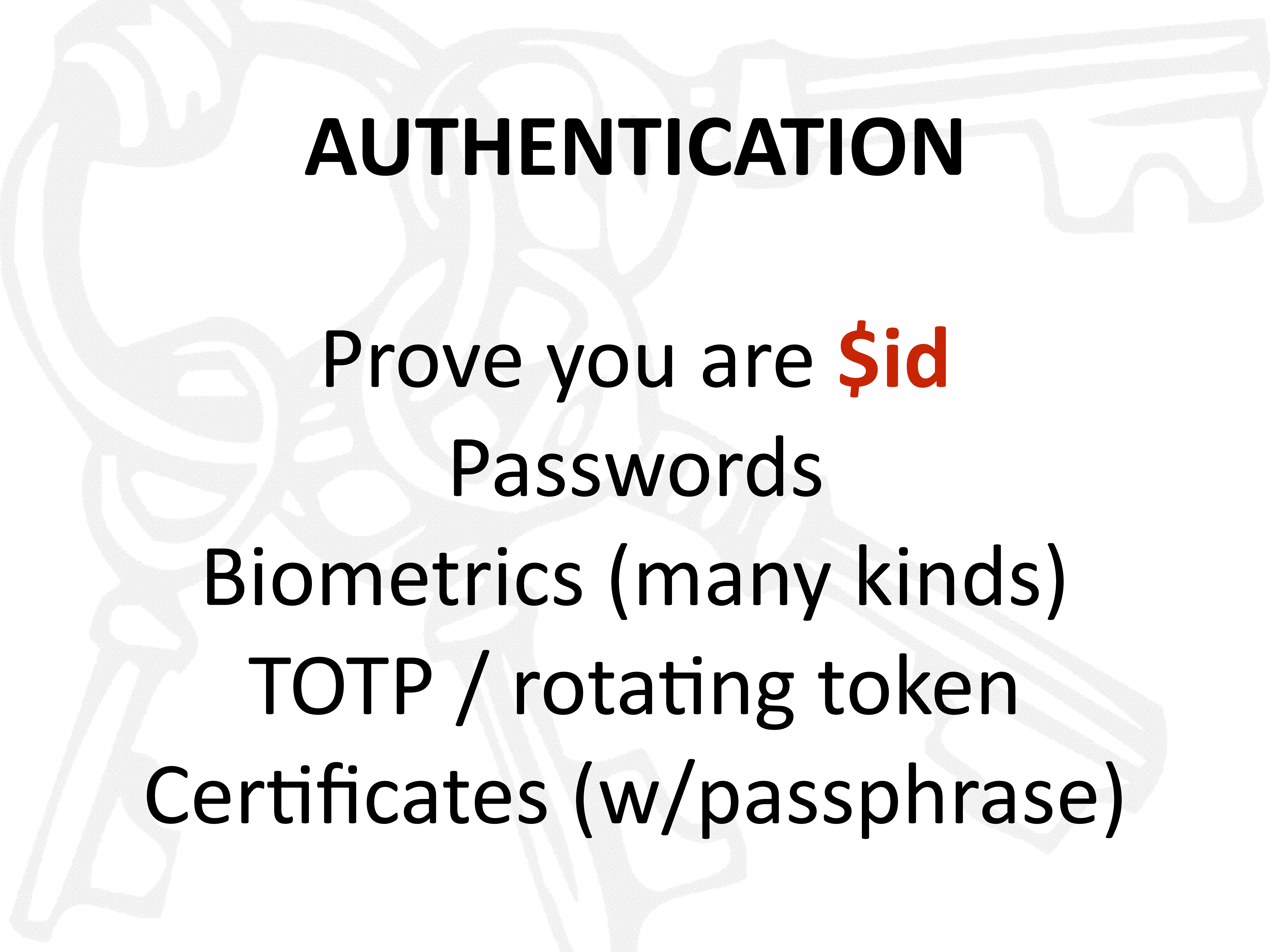
NYU Policy on PIN

What is this data?

CODABAR barcode

HID Card


NYU
August 2017
HID iCLASS DH
*97045 12050880-1E
Card is property of NYU.
valid only for length of stay.
Report loss or theft
immediately. If found,
return to: NYUCard Office,
383 Lafayette St. NY NY 10003
Report an Emergency: 911
(212) 998-2222
Information Alerts: (212) 998-1220
Campus Transportation: (212) 998-RIDE
Wellness Exchange: (212) 443-9999
Student Resource Center: (212) 998-4411
[redacted]



AUTHENTICATION

Prove you are **$id**

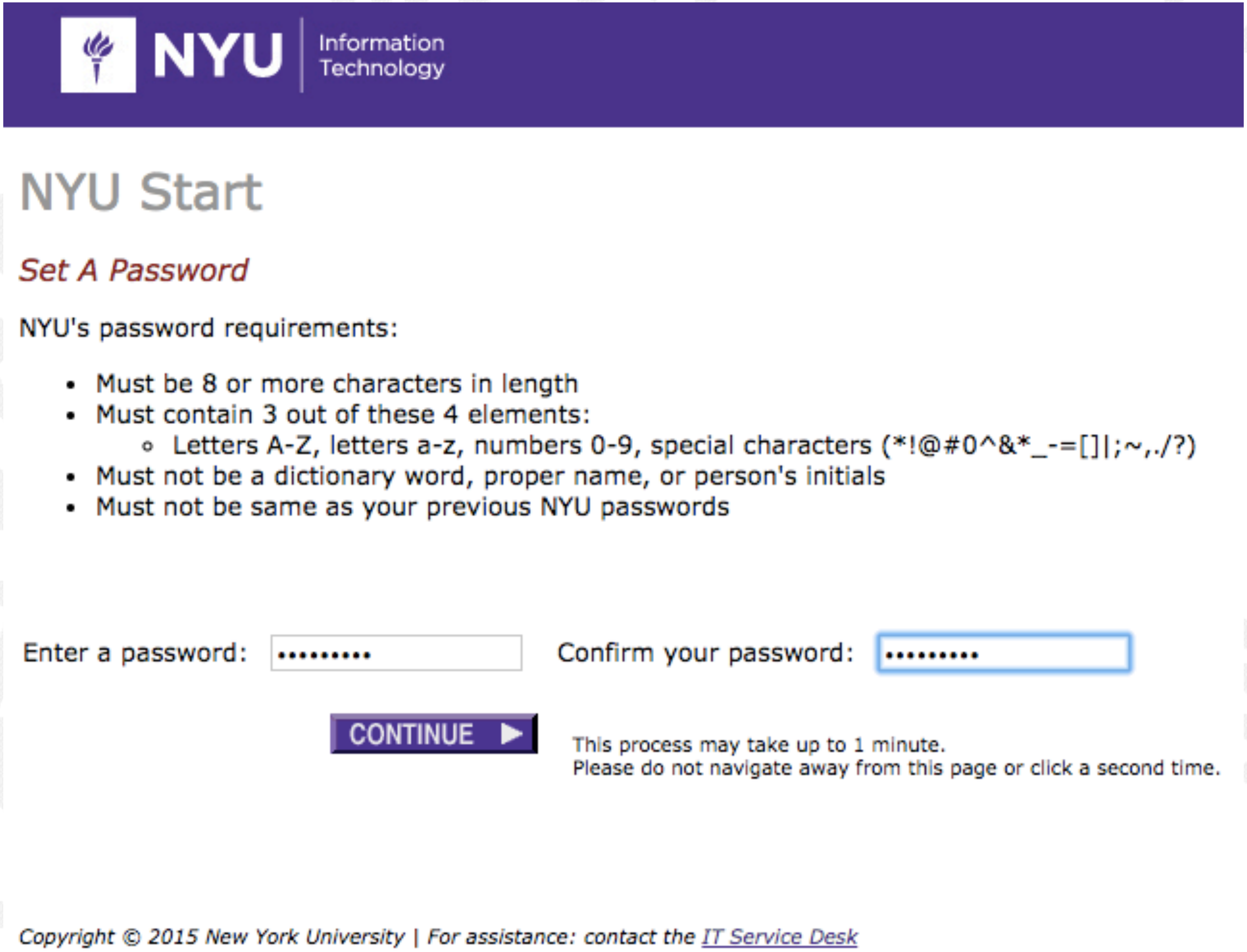
Passwords

Biometrics (many kinds)

TOTP / rotating token

Certificates (w/passphrase)

UGH, PASSWORDS



NYU Start

Set A Password

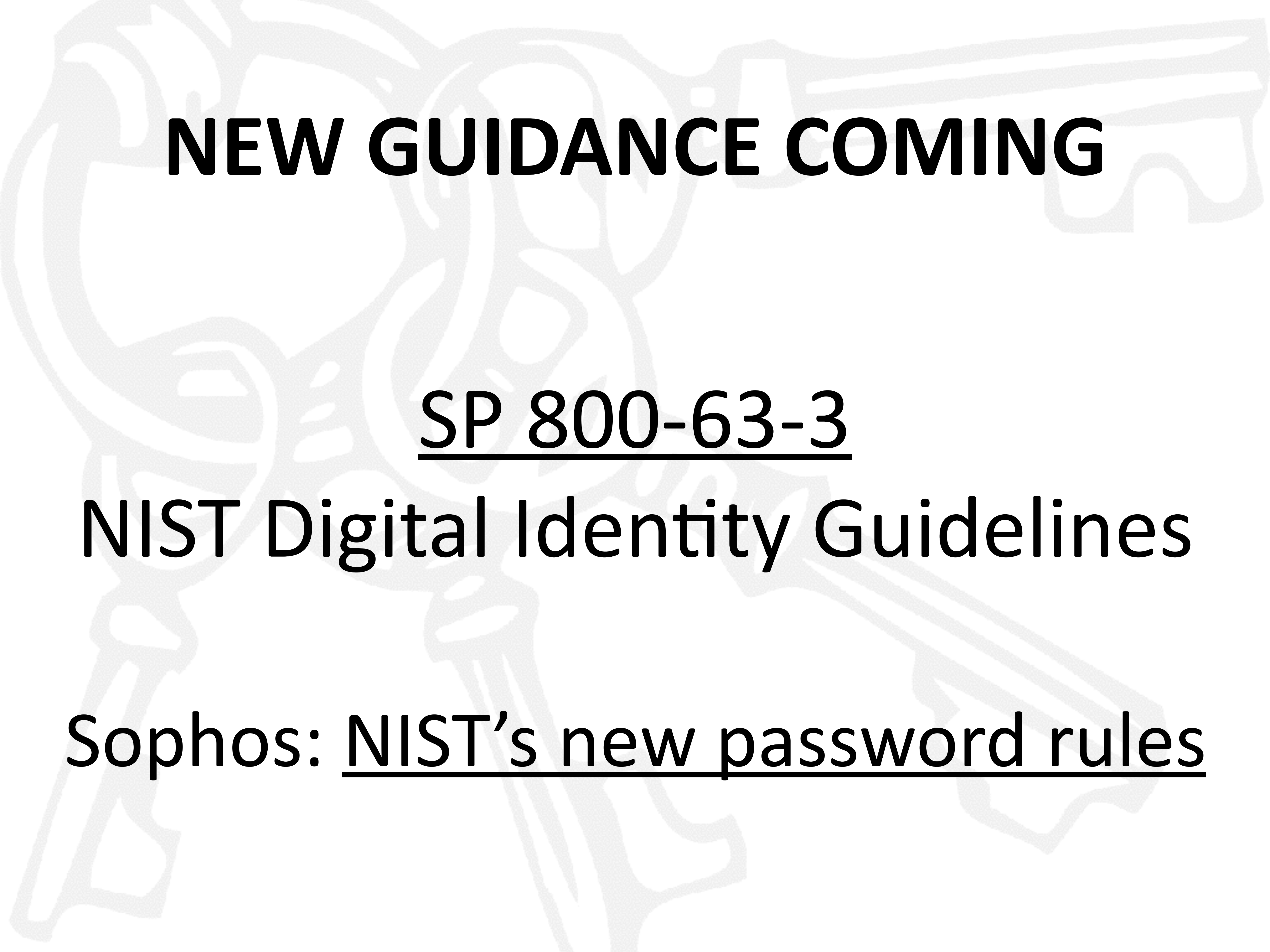
NYU's password requirements:

- Must be 8 or more characters in length
- Must contain 3 out of these 4 elements:
  - Letters A-Z, letters a-z, numbers 0-9, special characters (*!@#0^&*_-=[]|;~,./?)
- Must not be a dictionary word, proper name, or person's initials
- Must not be same as your previous NYU passwords

Enter a password: •••••••••• Confirm your password: ••••••••••

This process may take up to 1 minute.
Please do not navigate away from this page or click a second time.

Copyright © 2015 New York University | For assistance: contact the IT Service Desk



NEW GUIDANCE COMING

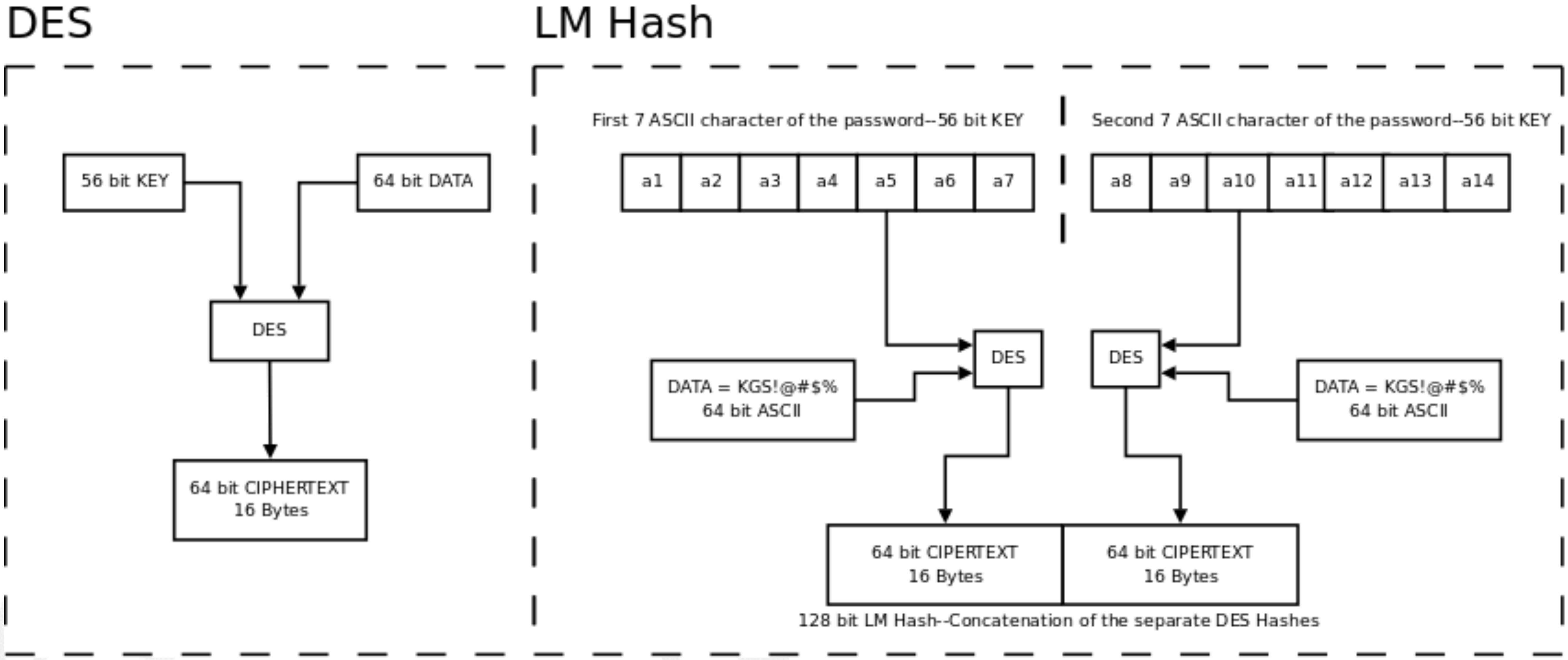
SP 800-63-3

NIST Digital Identity Guidelines

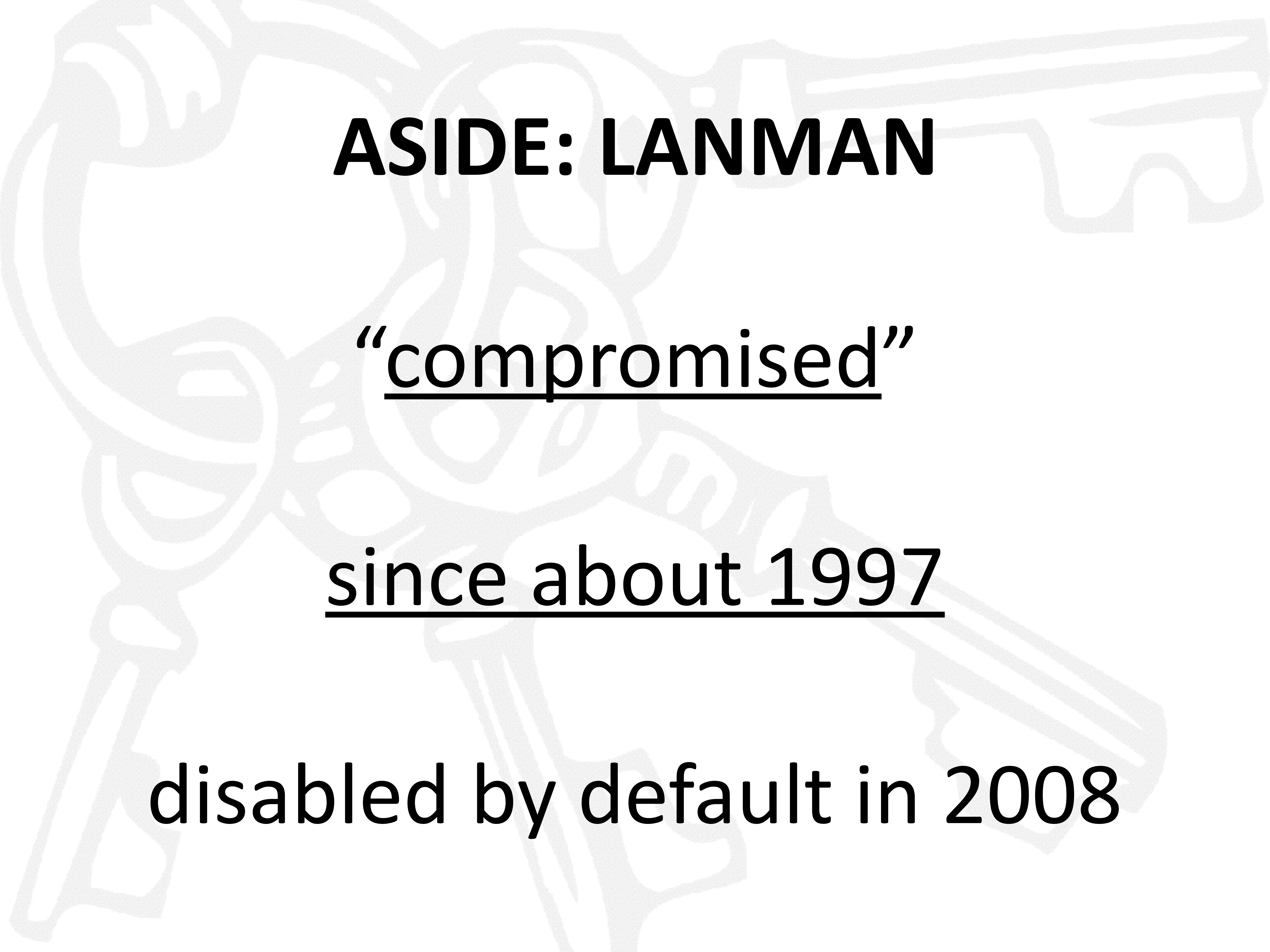
Sophos: NIST’s new password rules

ASIDE: LANMAN

Brute Force Search of a DES Keyspace:
Defeating LM Hashes



ASIDE: LANMAN



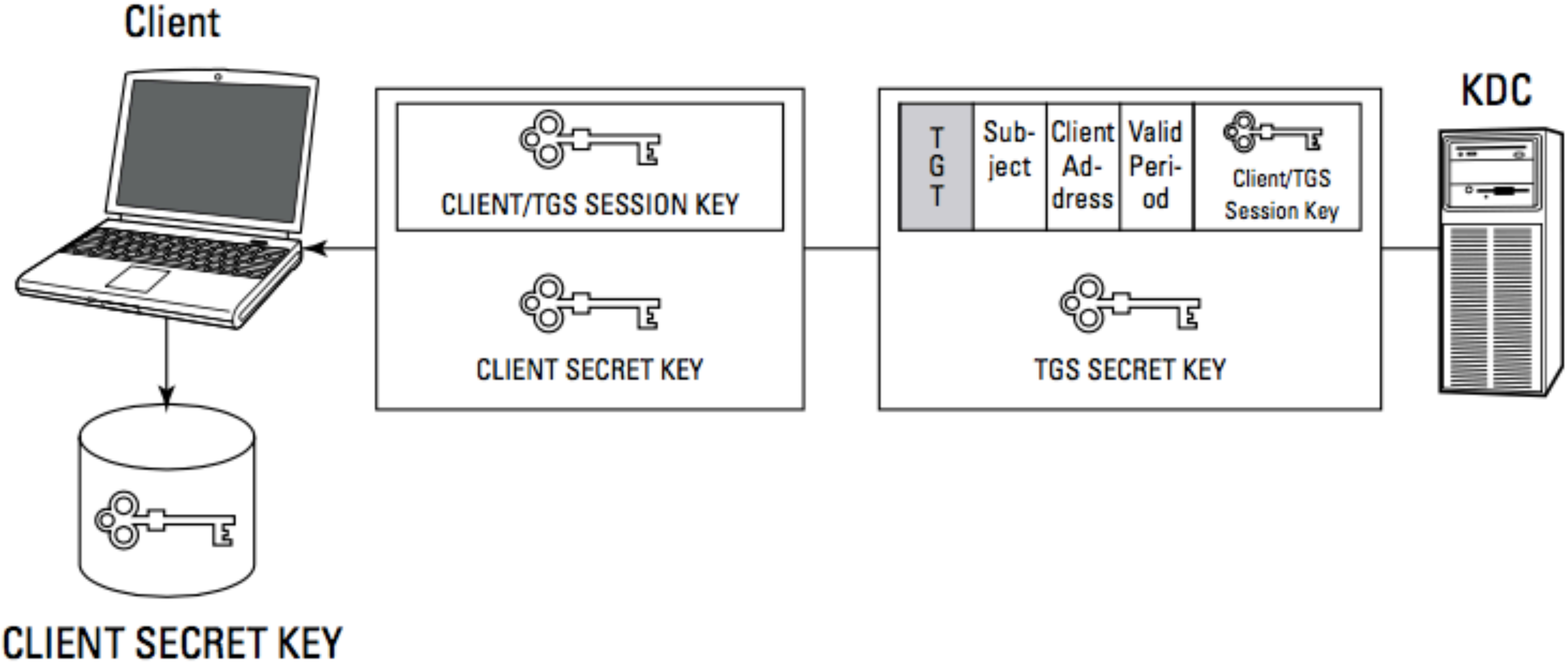
“compromised”

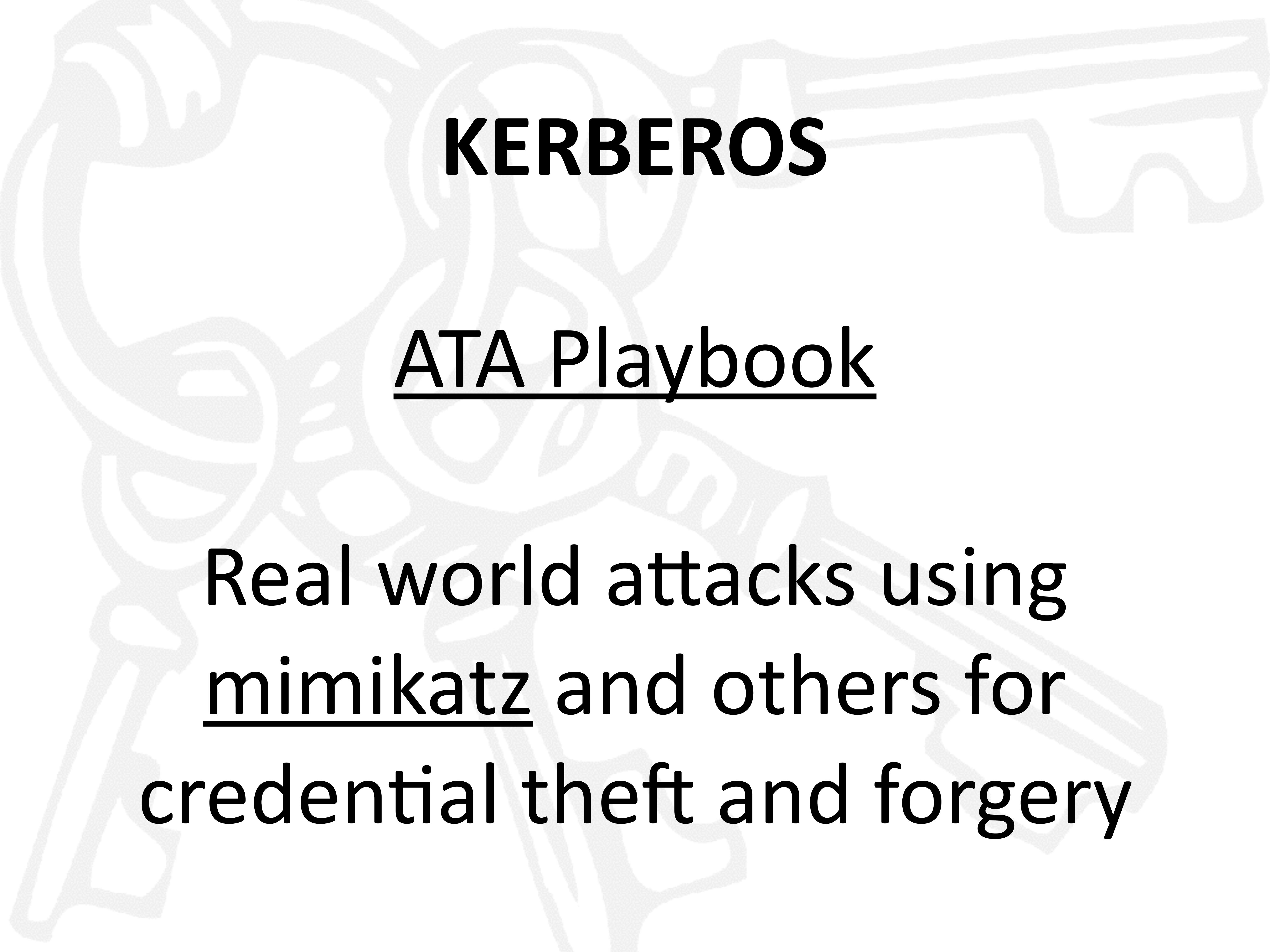
since about 1997

disabled by default in 2008

KERBEROS

Windows Active Directory

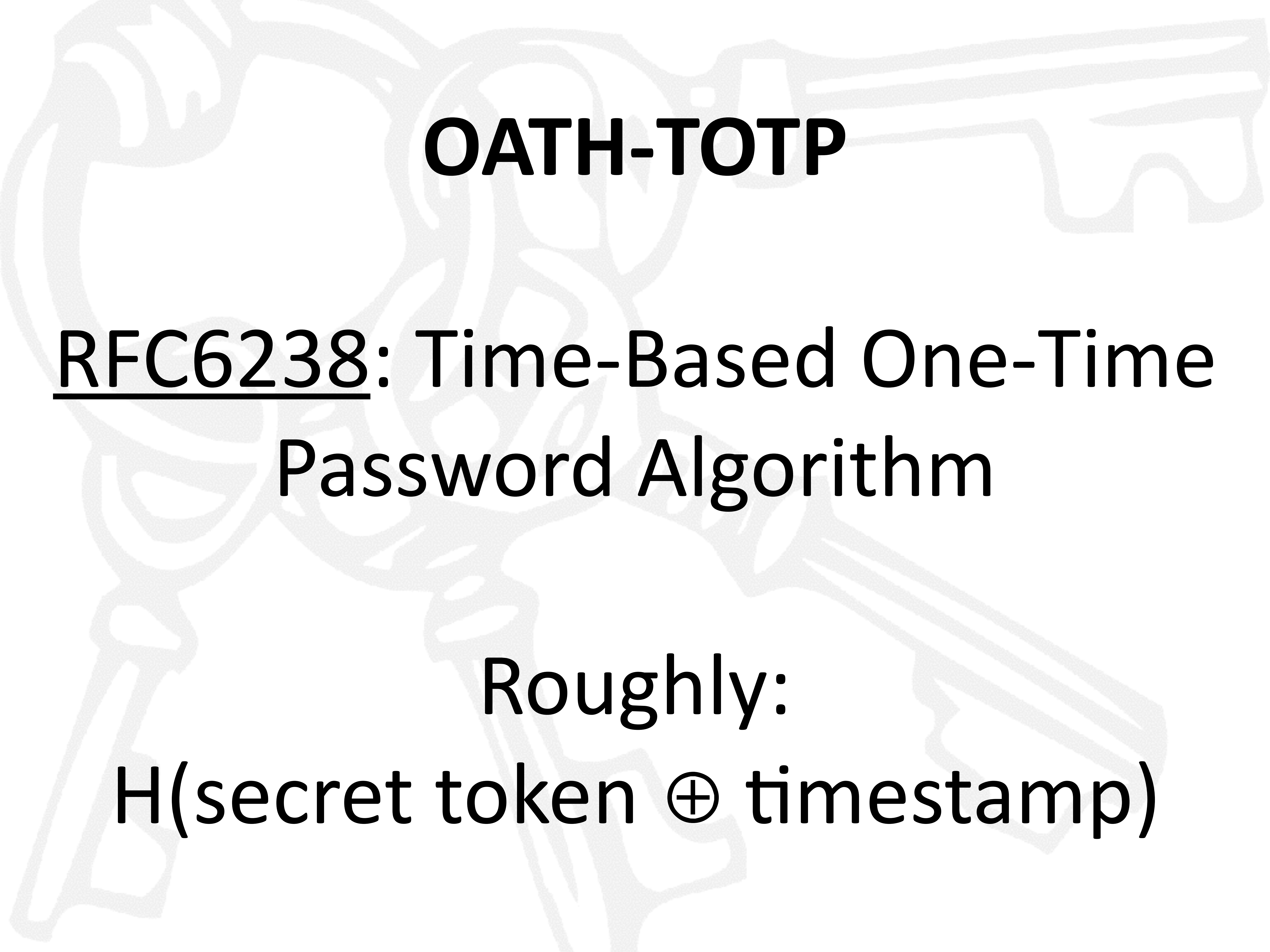




KERBEROS

ATA Playbook

Real world attacks using mimikatz and others for credential theft and forgery

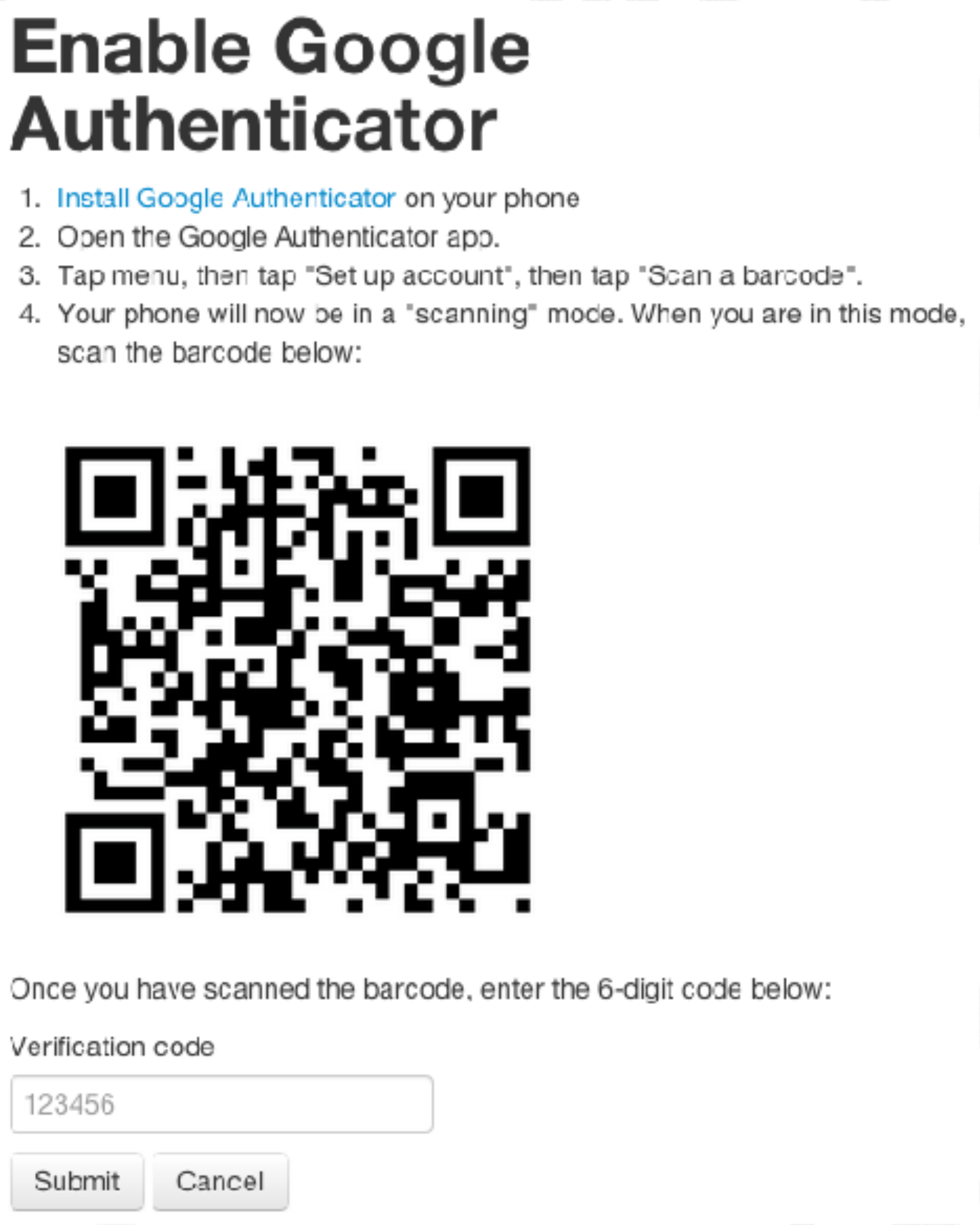


OATH-TOTP

RFC6238: Time-Based One-Time Password Algorithm

Roughly:
H(secret token ⊕ timestamp)

OATH-TOTP



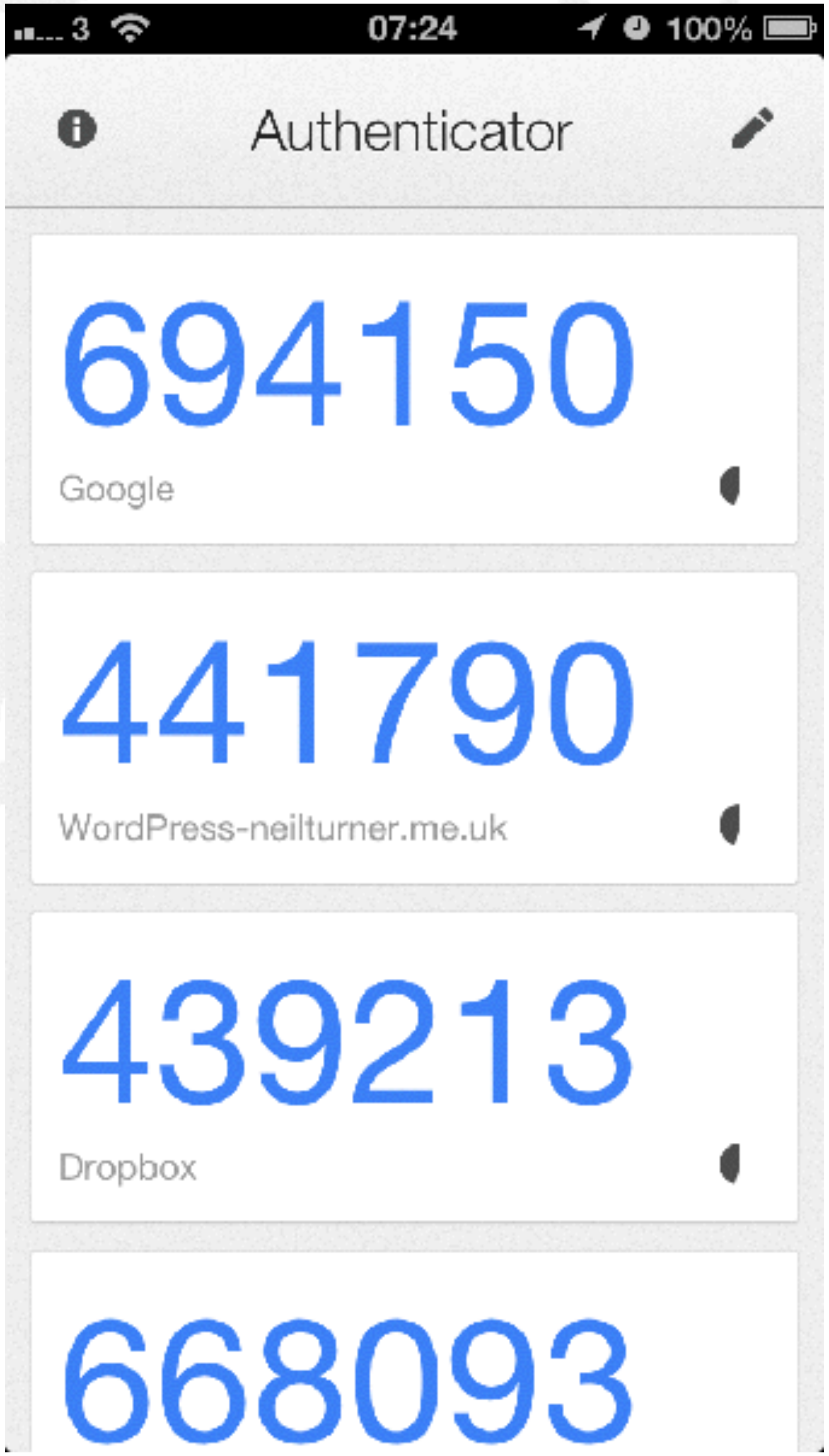
Enable Google Authenticator

1. Install Google Authenticator on your phone
2. Open the Google Authenticator app.
3. Tap menu, then tap "Set up account", then tap "Scan a barcode".
4. Your phone will now be in a "scanning" mode. When you are in this mode, scan the barcode below:

Once you have scanned the barcode, enter the 6-digit code below:

Verification code

123456



Authenticator

694150
Google

441790
WordPress-neilturner.me.uk

439213
Dropbox

668093

RSA SECURID

PIN + Proprietary TOTP

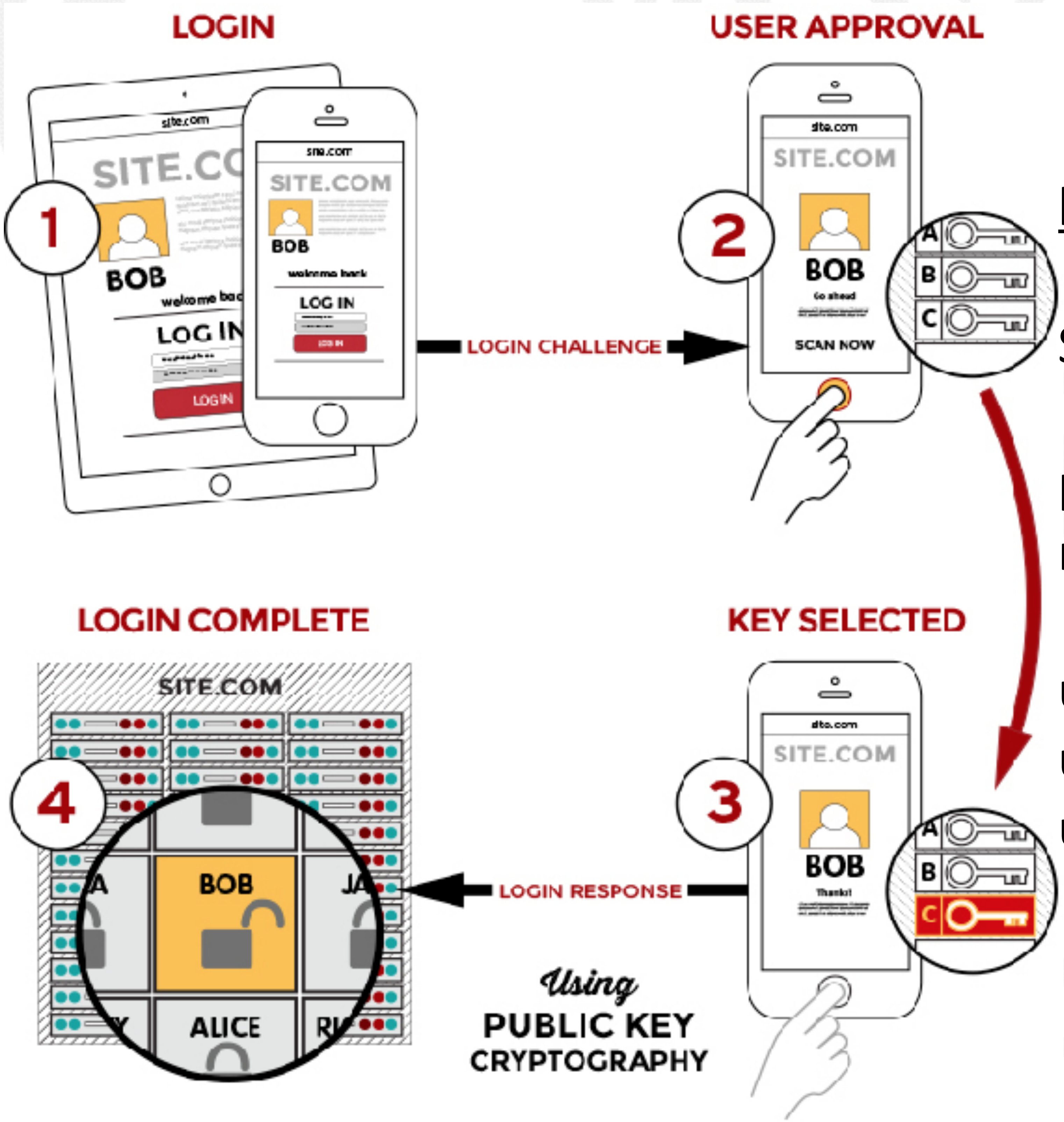
(Something you know + Something you have)

Failed Login Counter, Clock Drift Adjustment, other features

2011 RSA Token Seed Compromise

http://arstechnica.com/security/2011/06/rsa-finally-comes-clean-securid-is-compromised/

FIDO



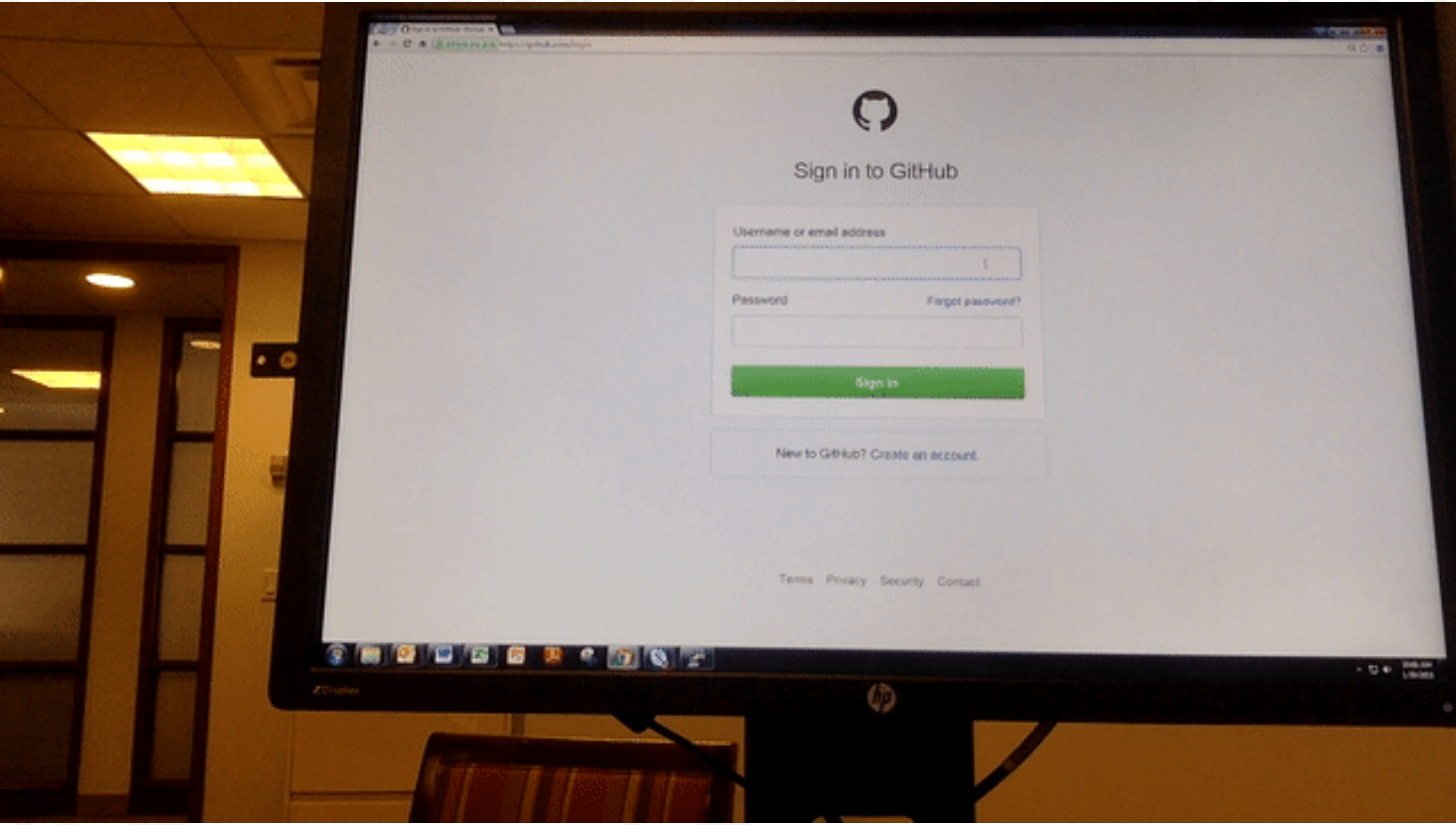
http://fidoalliance.org

Supplement or eliminate passwords

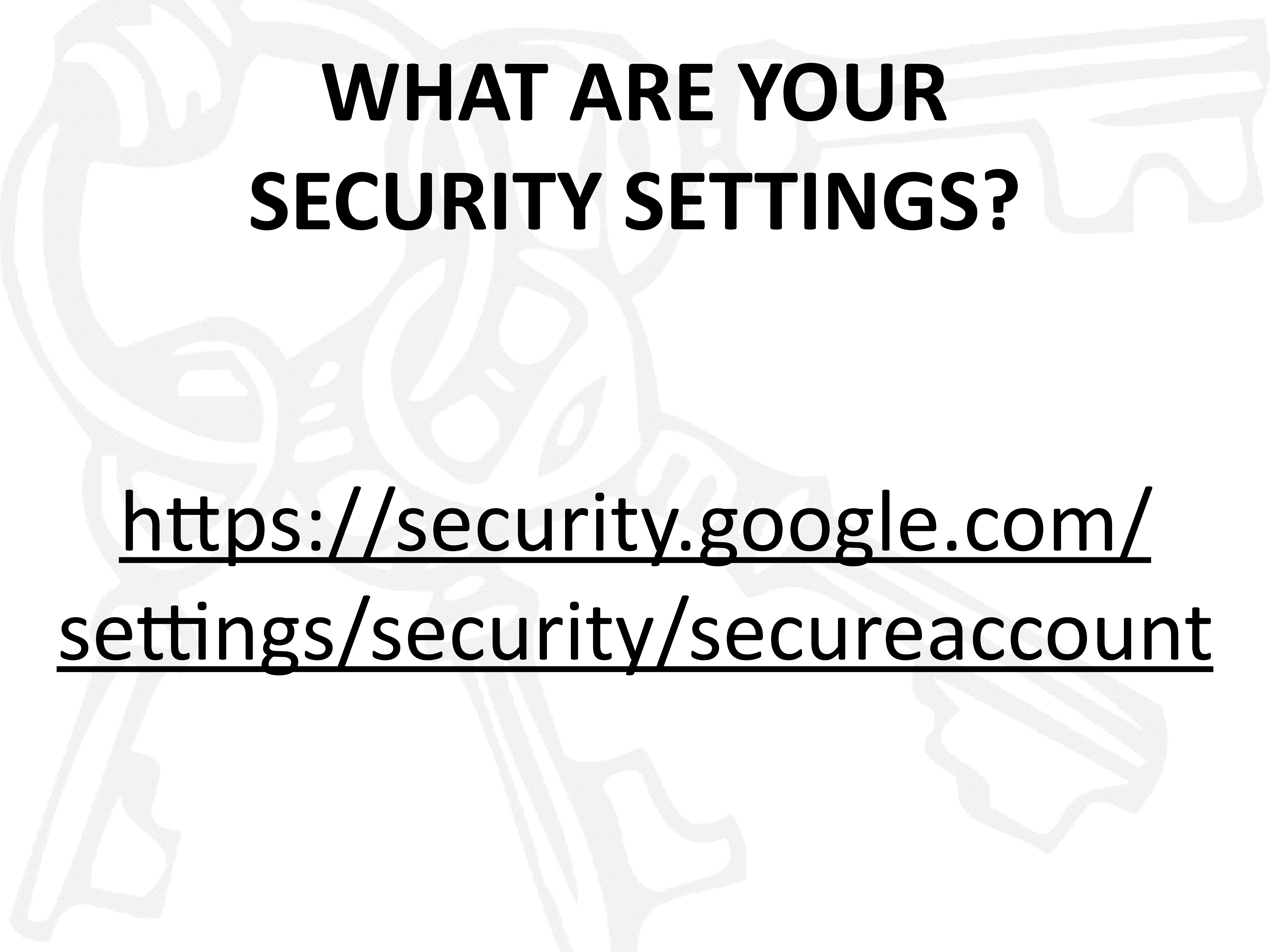
public / private key pair
register public key

use “local verification”
use private key to sign challenge
use public key to verify challenge

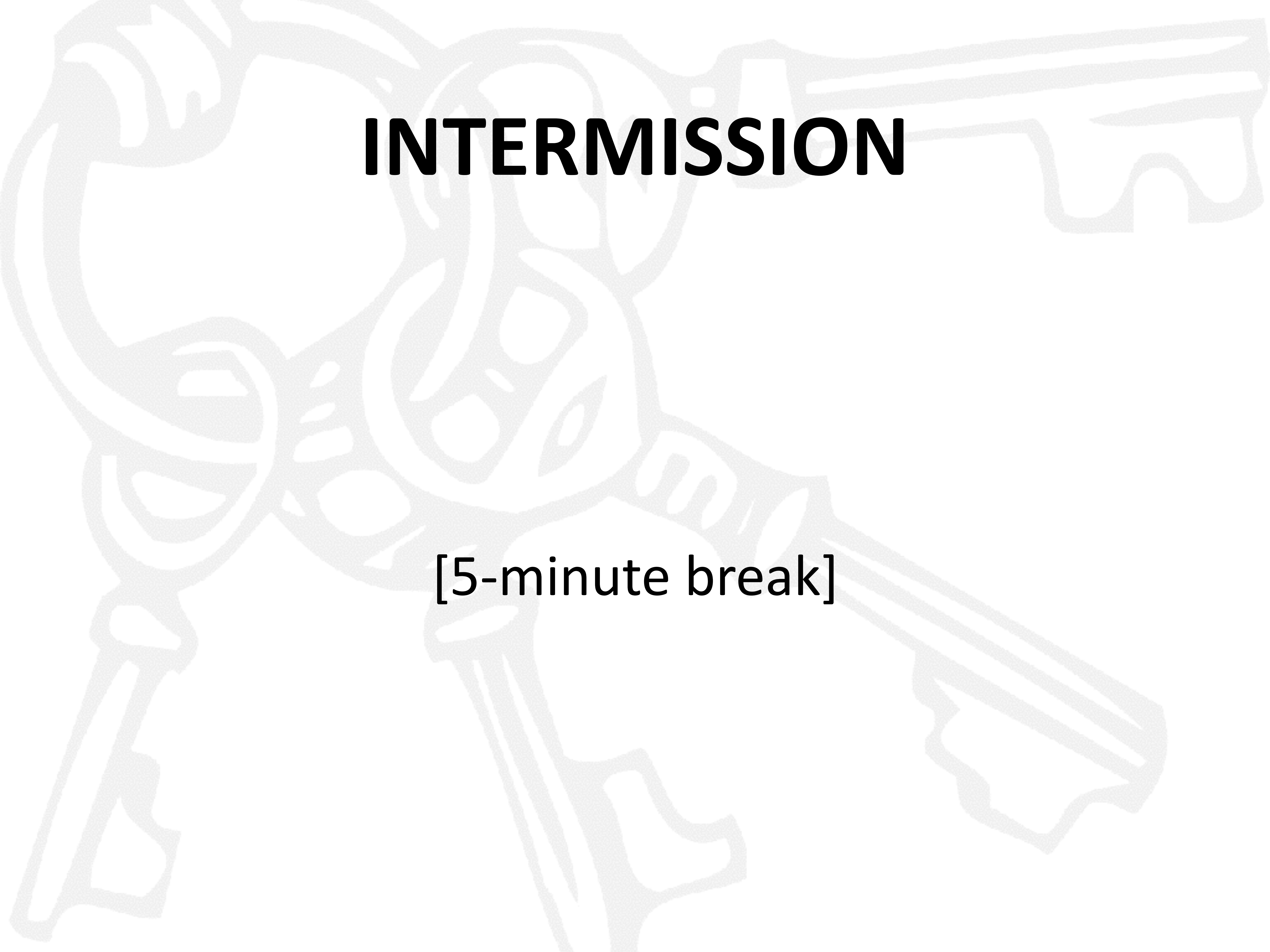
FIDO IN ACTION



WHAT ARE YOUR SECURITY SETTINGS?

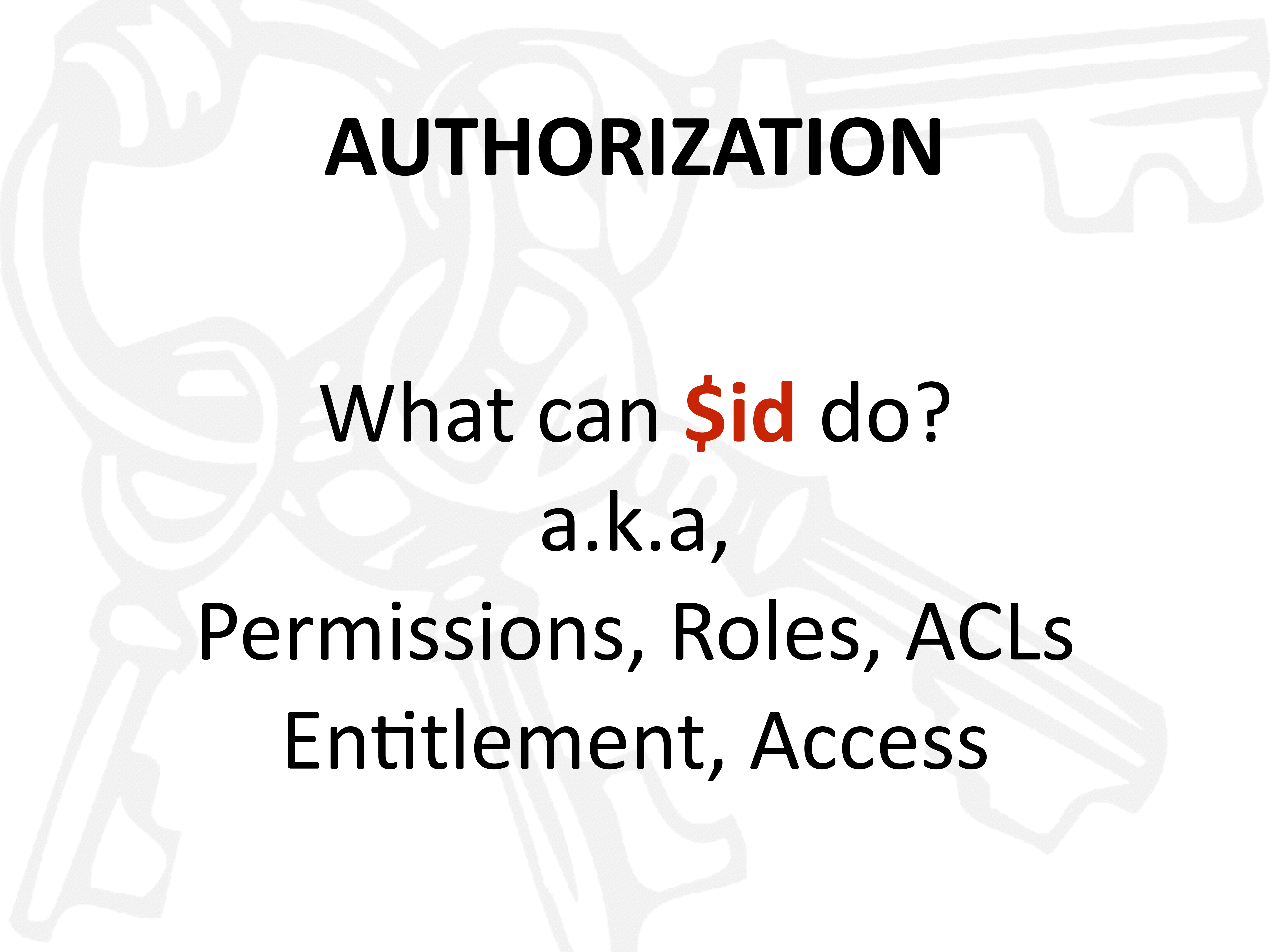


https://security.google.com/settings/security/secureaccount



INTERMISSION

[5-minute break]



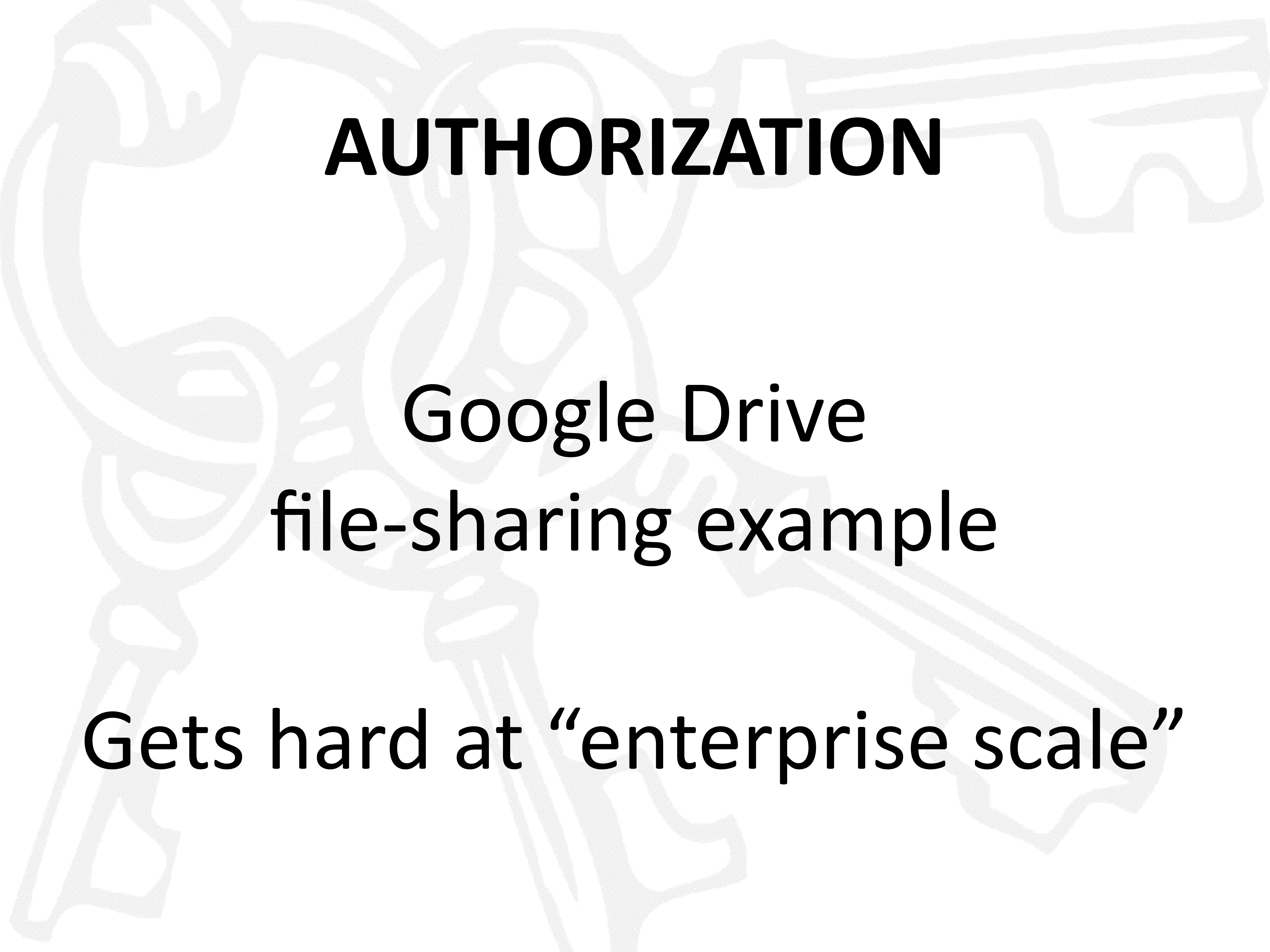
AUTHORIZATION

What can **$id** do?

a.k.a,

Permissions, Roles, ACLs

Entitlement, Access

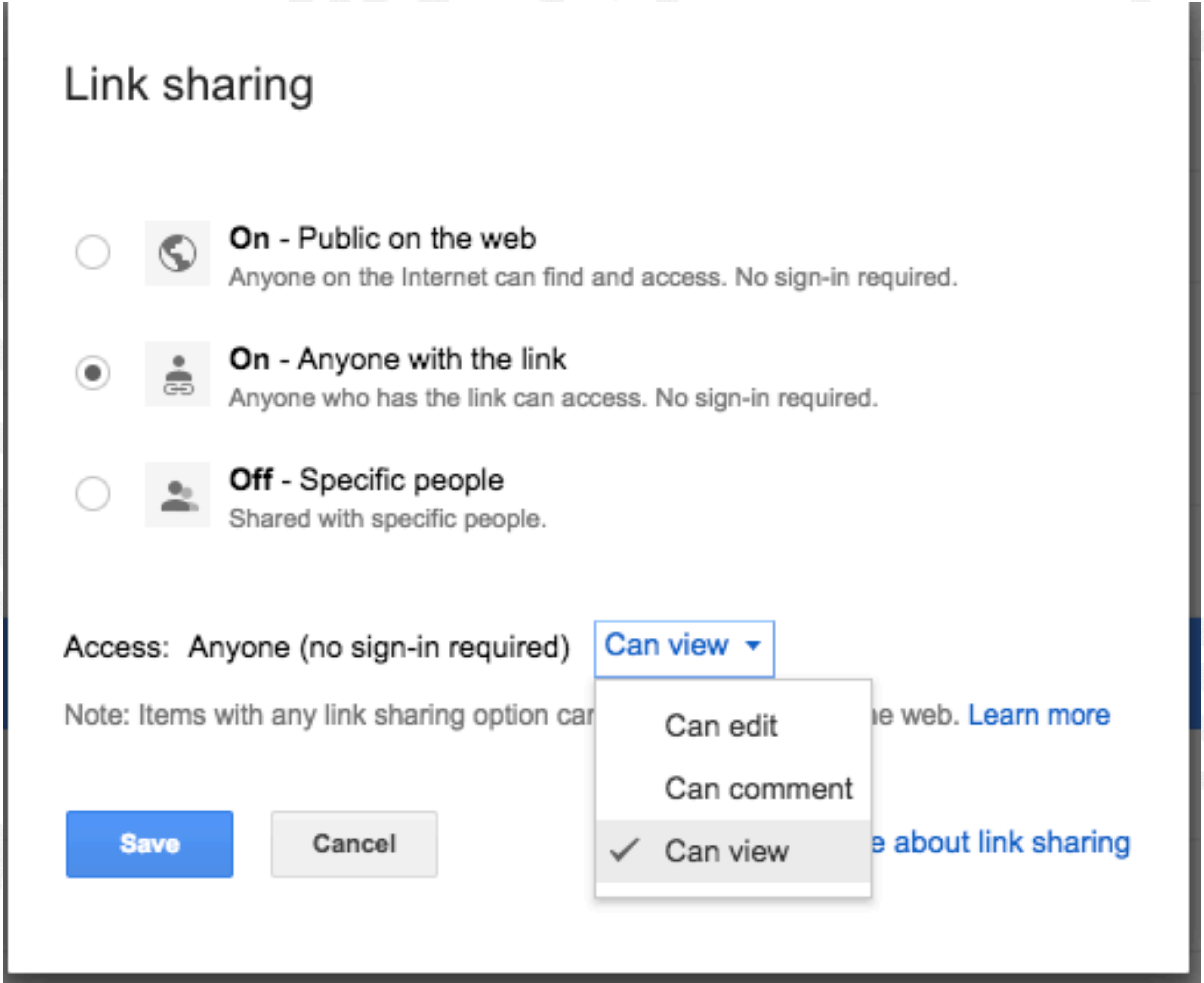


AUTHORIZATION

Google Drive
file-sharing example

Gets hard at “enterprise scale”

AUTHORIZATION



Link sharing

○ **On** - Public on the web
Anyone on the Internet can find and access. No sign-in required.

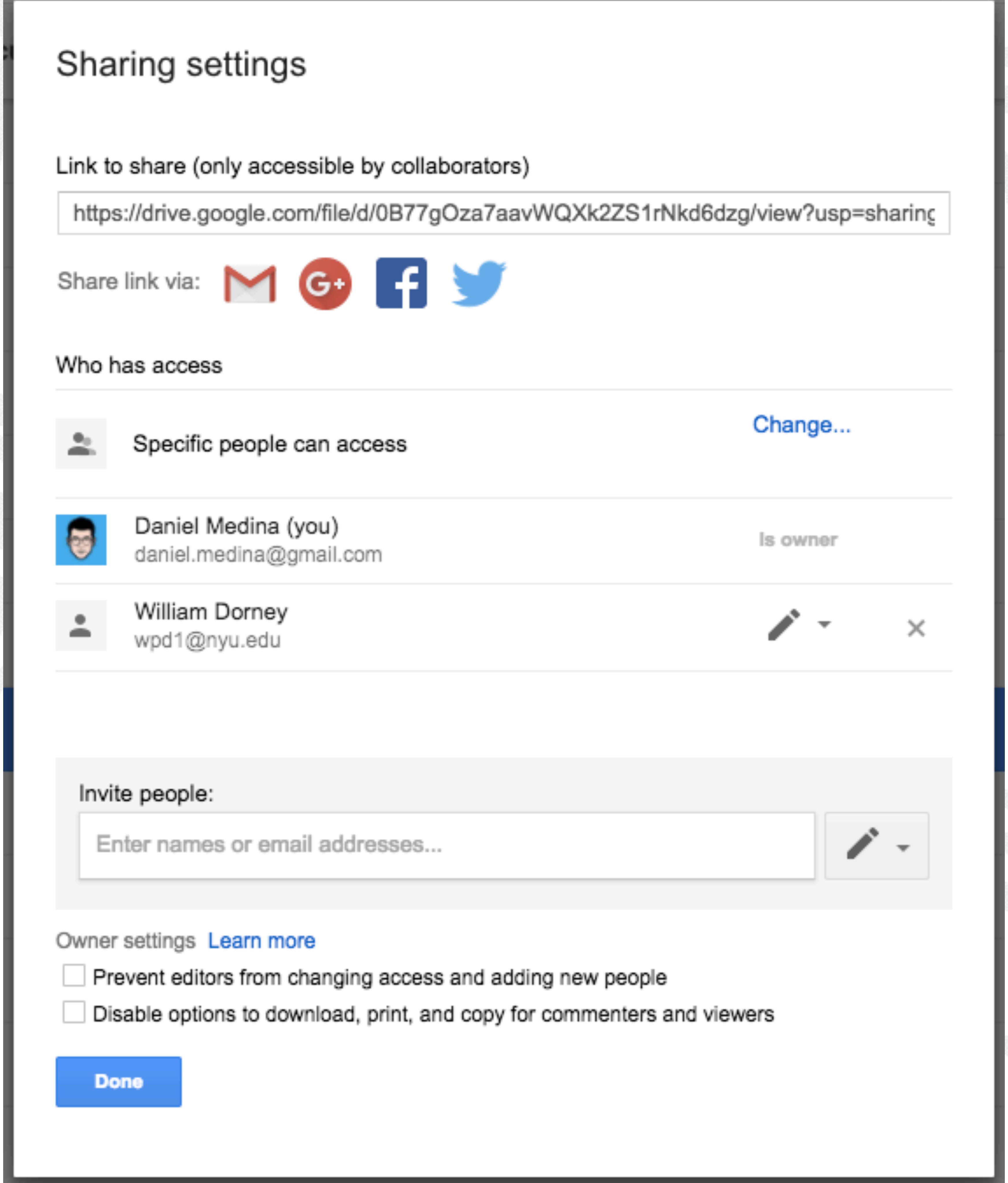
● **On** - Anyone with the link
Anyone who has the link can access. No sign-in required.

○ **Off** - Specific people
Shared with specific people.

Access: Anyone (no sign-in required) Can view

Note: Items with any link sharing option car e web. Learn more

e about link sharing



Sharing settings

Link to share (only accessible by collaborators)

https://drive.google.com/file/d/0B77gOza7aavWQXk2ZS1rNkd6dzg/view?usp=sharing

Share link via:

Who has access

Specific people can access

Daniel Medina (you)
daniel.medina@gmail.com
Is owner

William Dorney
wpd1@nyu.edu

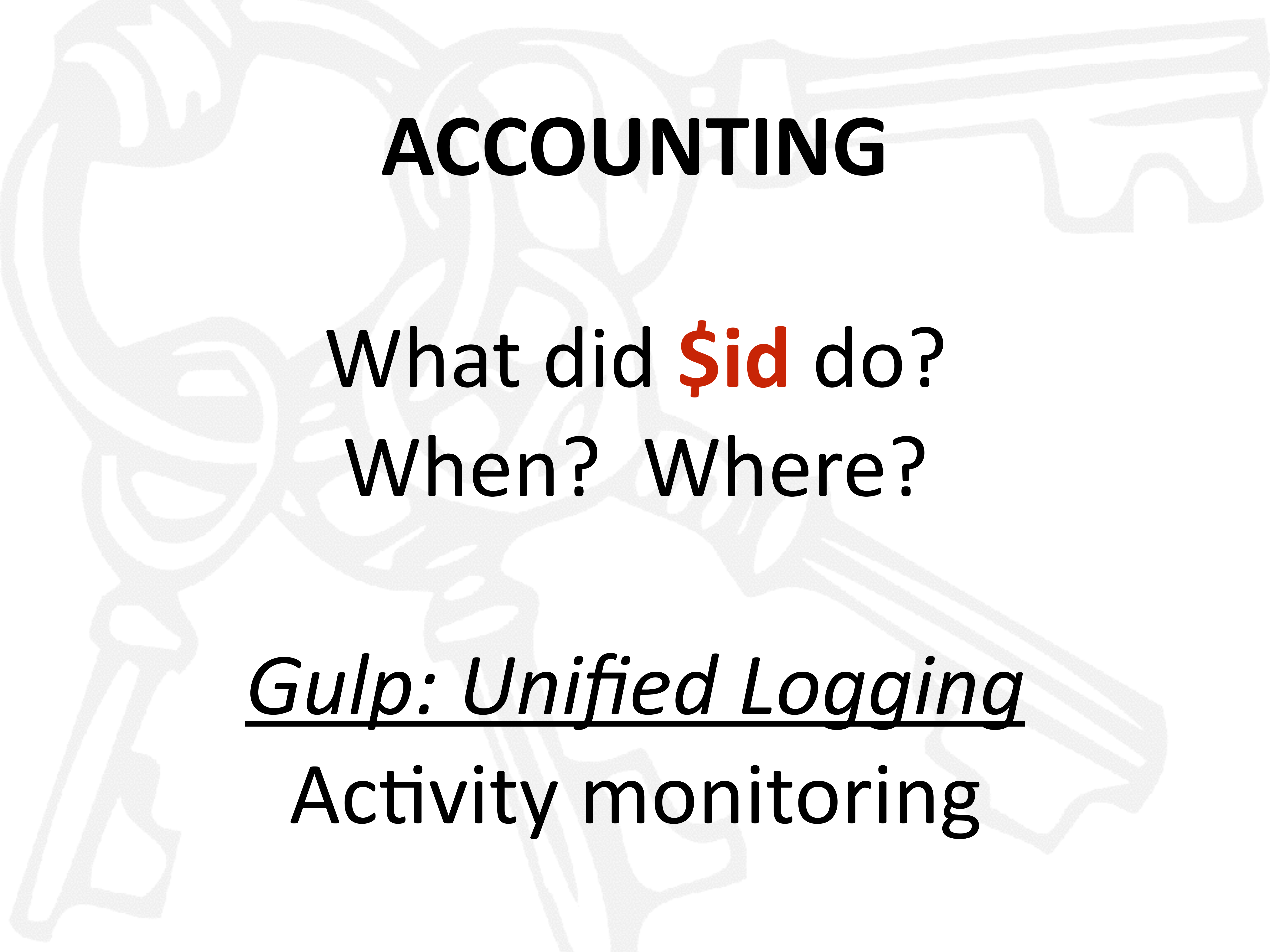
Invite people:

Enter names or email addresses...

Owner settings Learn more

□ Prevent editors from changing access and adding new people

□ Disable options to download, print, and copy for commenters and viewers



ACCOUNTING

What did **$id** do?
When? Where?

Gulp: Unified Logging
Activity monitoring

ATTACKING

Identification
Authentication
Authorization
Accounting

ATTACKING

Brute-force

Dictionaries

Rainbow Tables

Man In The Middle (MITM)

Offline vs Online, Active vs Passive

CRACKERS

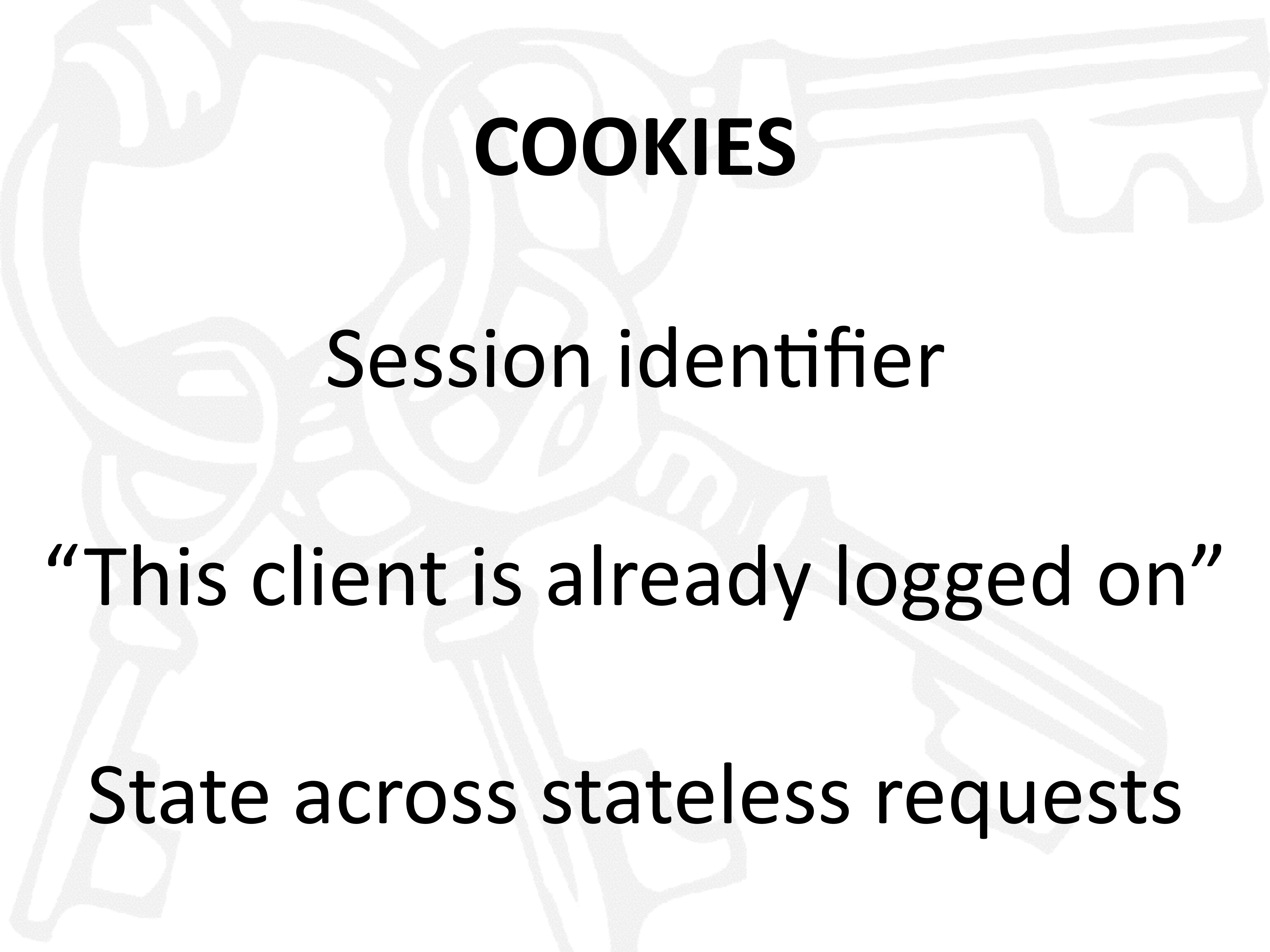
John the Ripper, http://www.openwall.com/john

```
# c/s = "combinations per second"
$ run/john  crypted
Loaded 6 password hashes with 5 different salts (DES)
test                (test)
daniel2             (medinad)
medina1             (medina)
password            (utility)
guesses: 4  time: 0:00:02:02 (3)  c/s: 1355K
trying: dmorai7 - dmokOUM
```

For Windows: http://ophcrack.sourceforge.net/

WEB SECURITY

Cookies and TLS



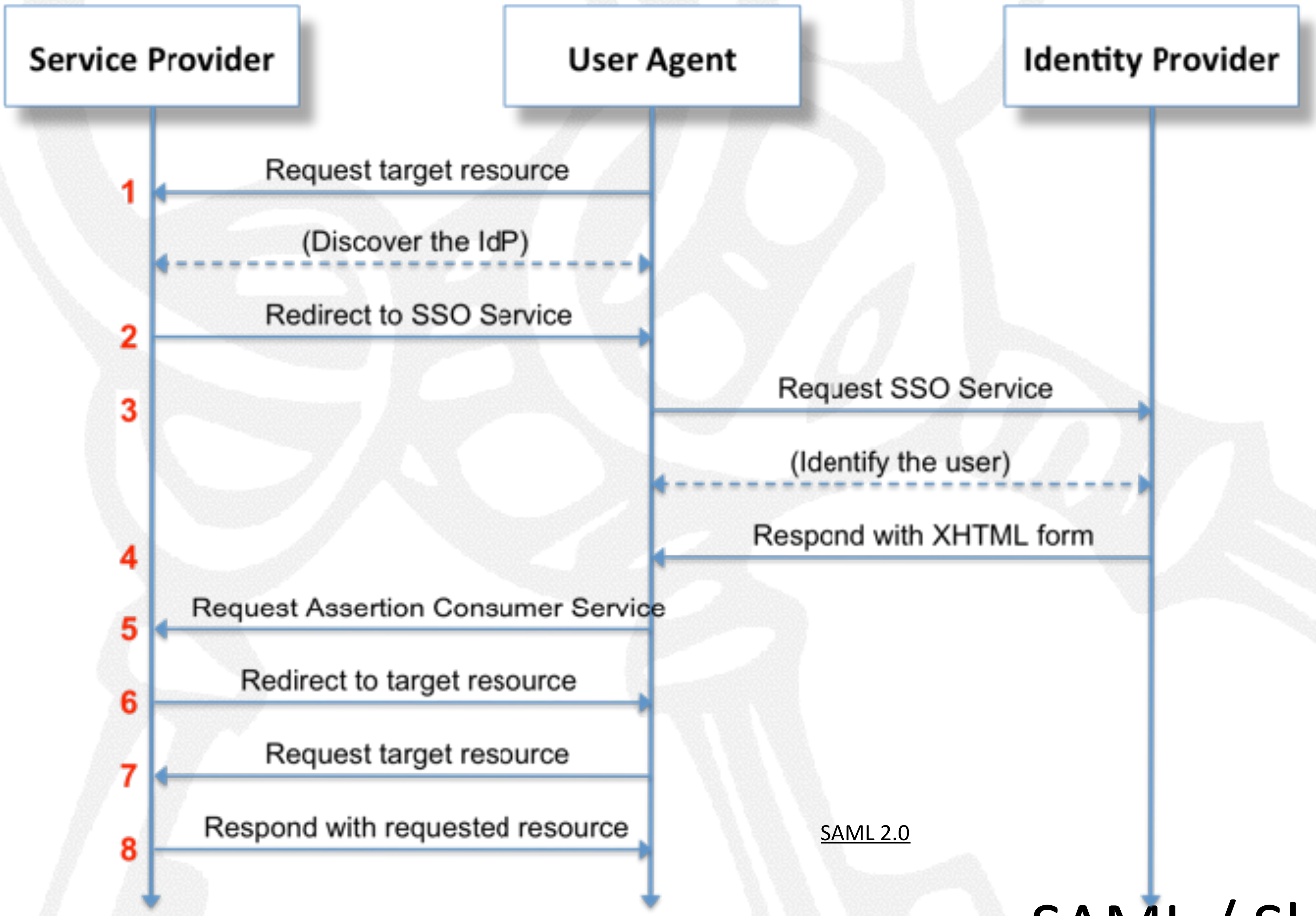
COOKIES

Session identifier

“This client is already logged on”

State across stateless requests

ASIDE: ENTERPRISE SSO

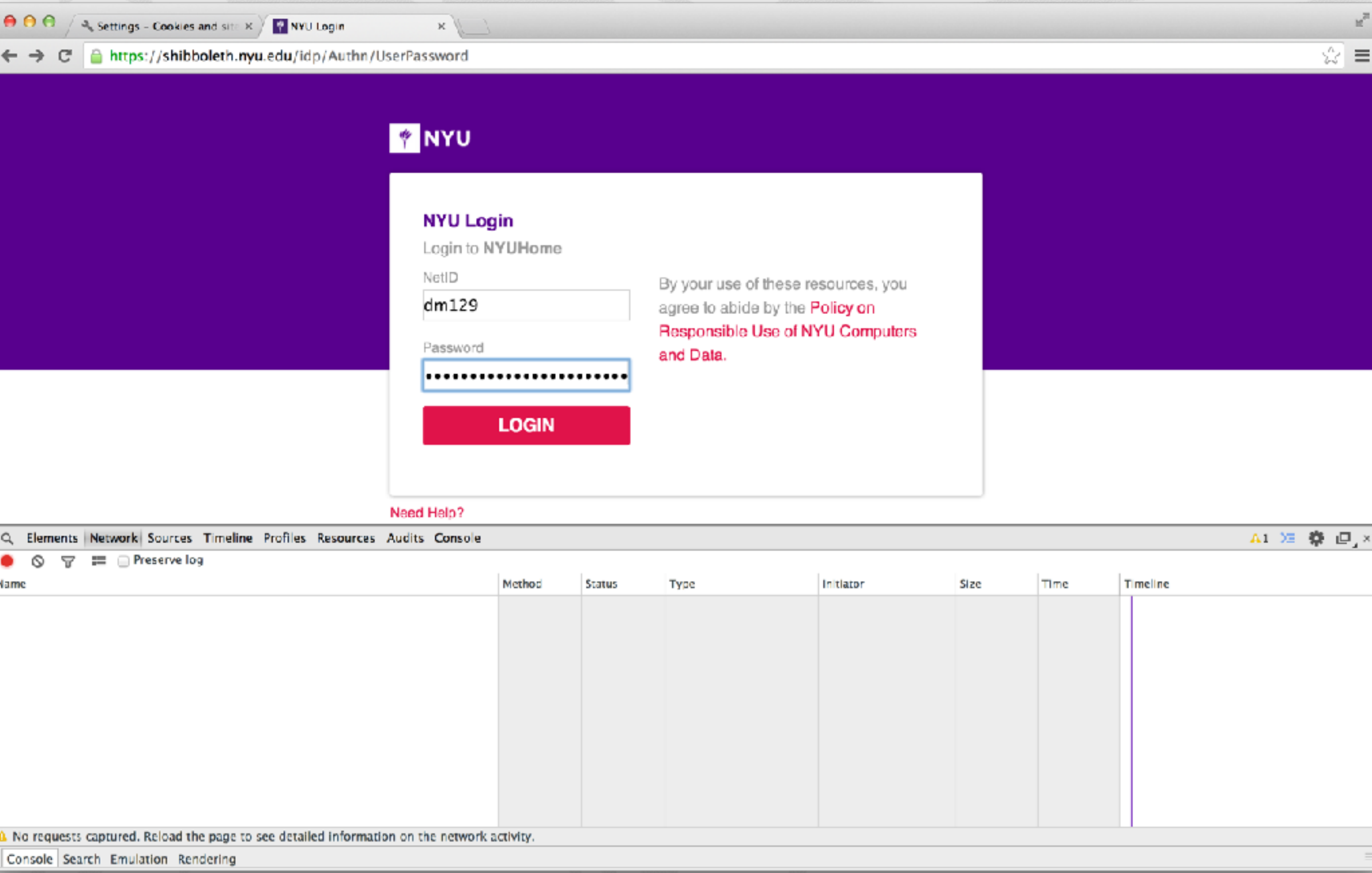


SAML 2.0

SAML / Shibboleth (NYU uses)
OpenID Connect
OAuth2 (Google, Facebook, etc.)

COOKIES

Let’s get some cookies



https://shibboleth.nyu.edu/idp/Authn/UserPassword

NYU

NYU Login

Login to NYUHome

NetID: dm129

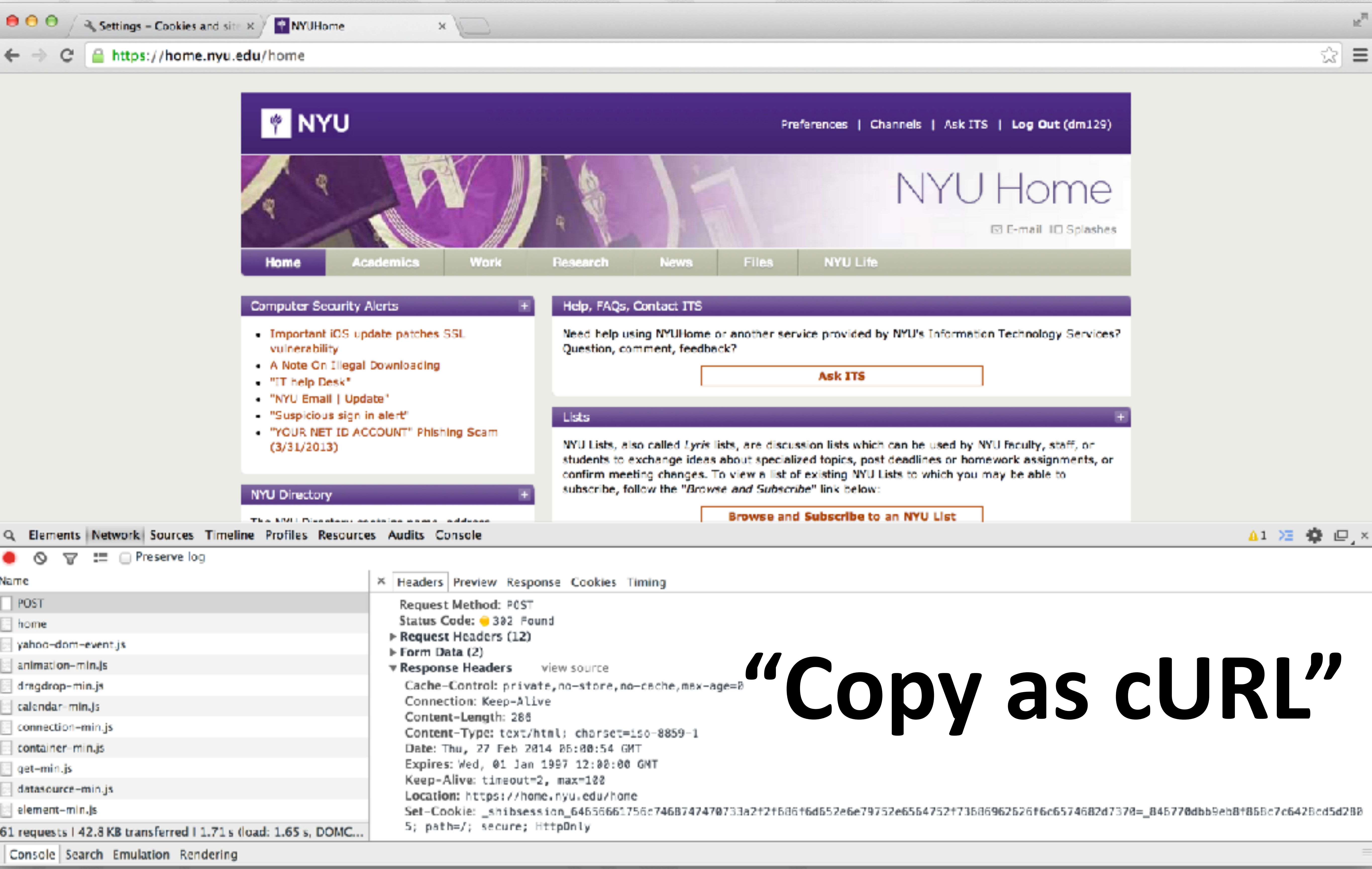
Password: ••••••••••••••••••••••••

LOGIN

By your use of these resources, you agree to abide by the Policy on Responsible Use of NYU Computers and Data.

Need Help?

No requests captured. Reload the page to see detailed information on the network activity.



NYU

Preferences | Channels | Ask ITS | Log Out (dm129)

NYU Home

Computer Security Alerts

- Important iOS update patches SSL vulnerability
- A Note On Illegal Downloading
- "IT help Desk"
- "NYU Email | Update"
- "Suspicious sign in alert"
- "YOUR NET ID ACCOUNT" Phishing Scam (3/31/2013)

Help, FAQs, Contact ITS

Need help using NYUHome or another service provided by NYU's Information Technology Services? Question, comment, feedback?

Ask ITS

Lists

NYU Lists, also called *Lyris* lists, are discussion lists which can be used by NYU Faculty, staff, or students to exchange ideas about specialized topics, post deadlines or homework assignments, or confirm meeting changes. To view a list of existing NYU Lists to which you may be able to subscribe, follow the "*Browse and Subscribe*" link below:

Browse and Subscribe to an NYU List

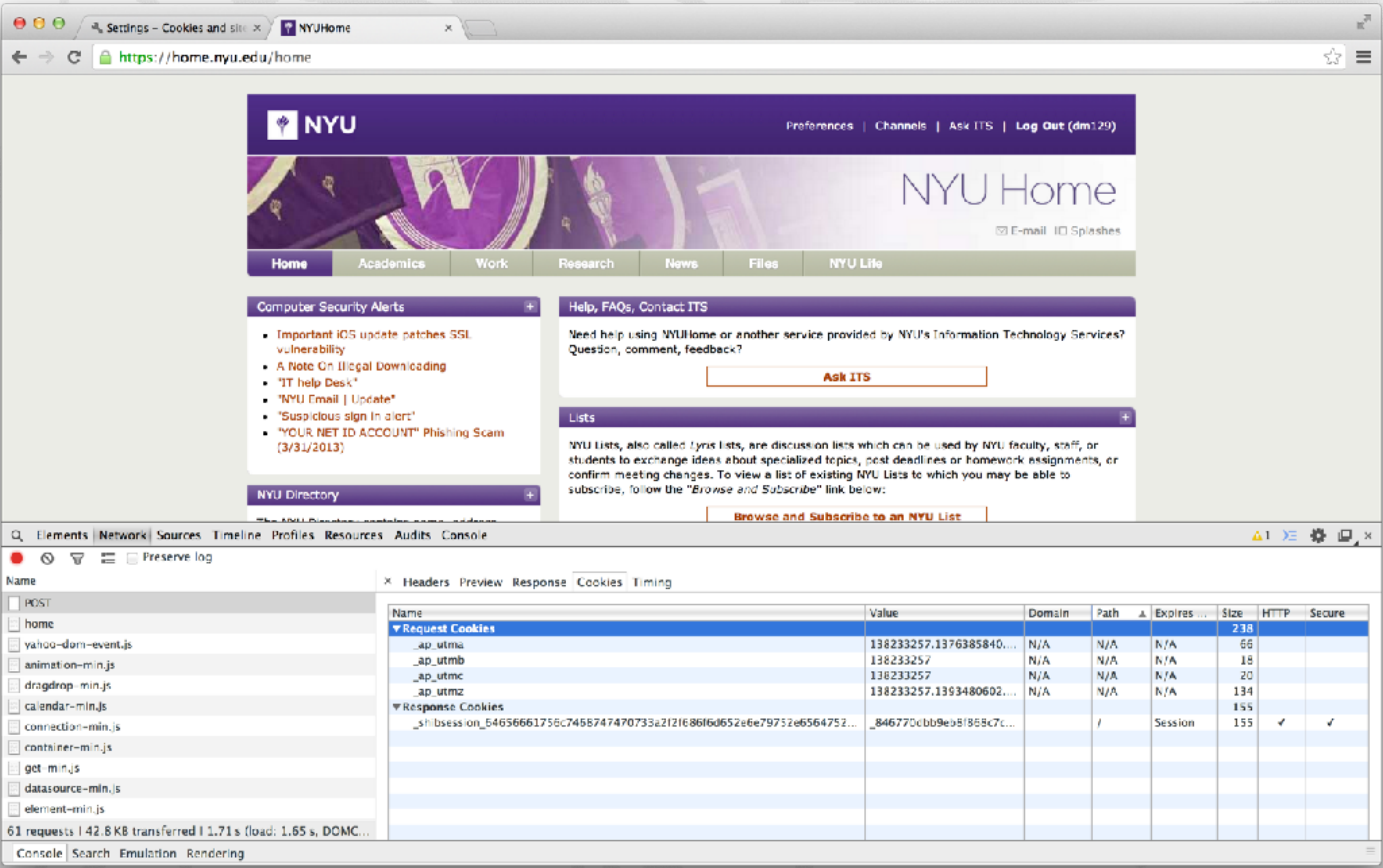
NYU Directory

The NYU Directory contains name, address

```
POST
home
yahoo-dom-event.js
animation-min.js
dragdrop-min.js
calendar-min.js
connection-min.js
container-min.js
get-min.js
datasource-min.js
element-min.js
61 requests | 42.8 KB transferred | 1.71 s (load: 1.65 s, DOMC...
```

```
Request Method: POST
Status Code: ● 302 Found
▶ Request Headers (12)
▶ Form Data (2)
▼ Response Headers     view source
  Cache-Control: private,no-store,no-cache,max-age=0
  Connection: Keep-Alive
  Content-Length: 288
  Content-Type: text/html; charset=iso-8859-1
  Date: Thu, 27 Feb 2014 05:00:54 GMT
  Expires: Wed, 01 Jan 1997 12:00:00 GMT
  Keep-Alive: timeout=2, max=100
  Location: https://home.nyu.edu/home
  Set-Cookie: _shibsession_64656661756c7468747470733a2f2f686f6d652e6e79752e6564752f73686962626f6c6574682d7370=_846770dbb9eb8f868c7c6428cd5d2885; path=/; secure; HttpOnly
```

“Copy as cURL”



Settings - Cookies and site
NYUHome
https://home.nyu.edu/home
NYU
Preferences | Channels | Ask ITS | Log Out (dm129)
NYU Home
E-mail ID Splashes
Home
Academics
Work
Research
News
Files
NYU Life

Computer Security Alerts

- Important iOS update patches SSL vulnerability
- A Note On Illegal Downloading
- "IT help Desk"
- "NYU Email | Update"
- "Suspicious sign In alert"
- "YOUR NET ID ACCOUNT" Phishing Scam (3/31/2013)

NYU Directory

Help, FAQs, Contact ITS

Need help using NYUHome or another service provided by NYU's Information Technology Services? Question, comment, feedback?

Ask ITS

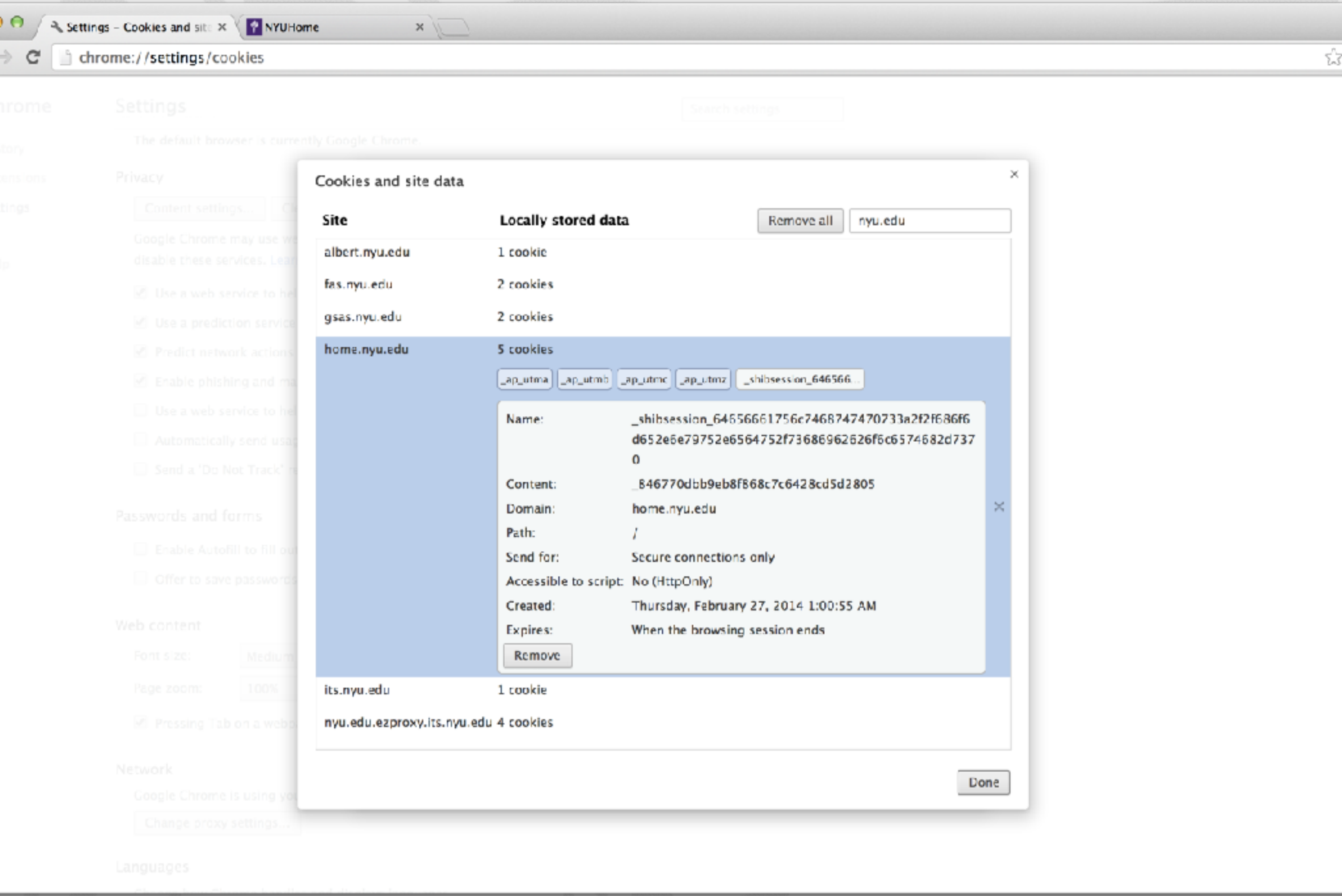
Lists

NYU Lists, also called *Lyris Lists*, are discussion lists which can be used by NYU faculty, staff, or students to exchange ideas about specialized topics, post deadlines or homework assignments, or confirm meeting changes. To view a list of existing NYU Lists to which you may be able to subscribe, follow the "*Browse and Subscribe*" link below:

Browse and Subscribe to an NYU List

61 requests | 42.8 KB transferred | 1.71 s (load: 1.65 s, DOMC…

Name	Value	Domain	Path	Expires …	Size	HTTP	Secure
▼Request Cookies					238		
_ap_utma	138233257.1376385840.…	N/A	N/A	N/A	66		
_ap_utmb	138233257	N/A	N/A	N/A	18		
_ap_utmc	138233257	N/A	N/A	N/A	20		
_ap_utmz	138233257.1393480602.…	N/A	N/A	N/A	134		
▼Response Cookies					155		
_shibsession_64656661756c7468747470733a2f2f686f6d652e6e79752e6564752…	_846770dbb9eb5f868c7c…		/	Session	155	✓	✓



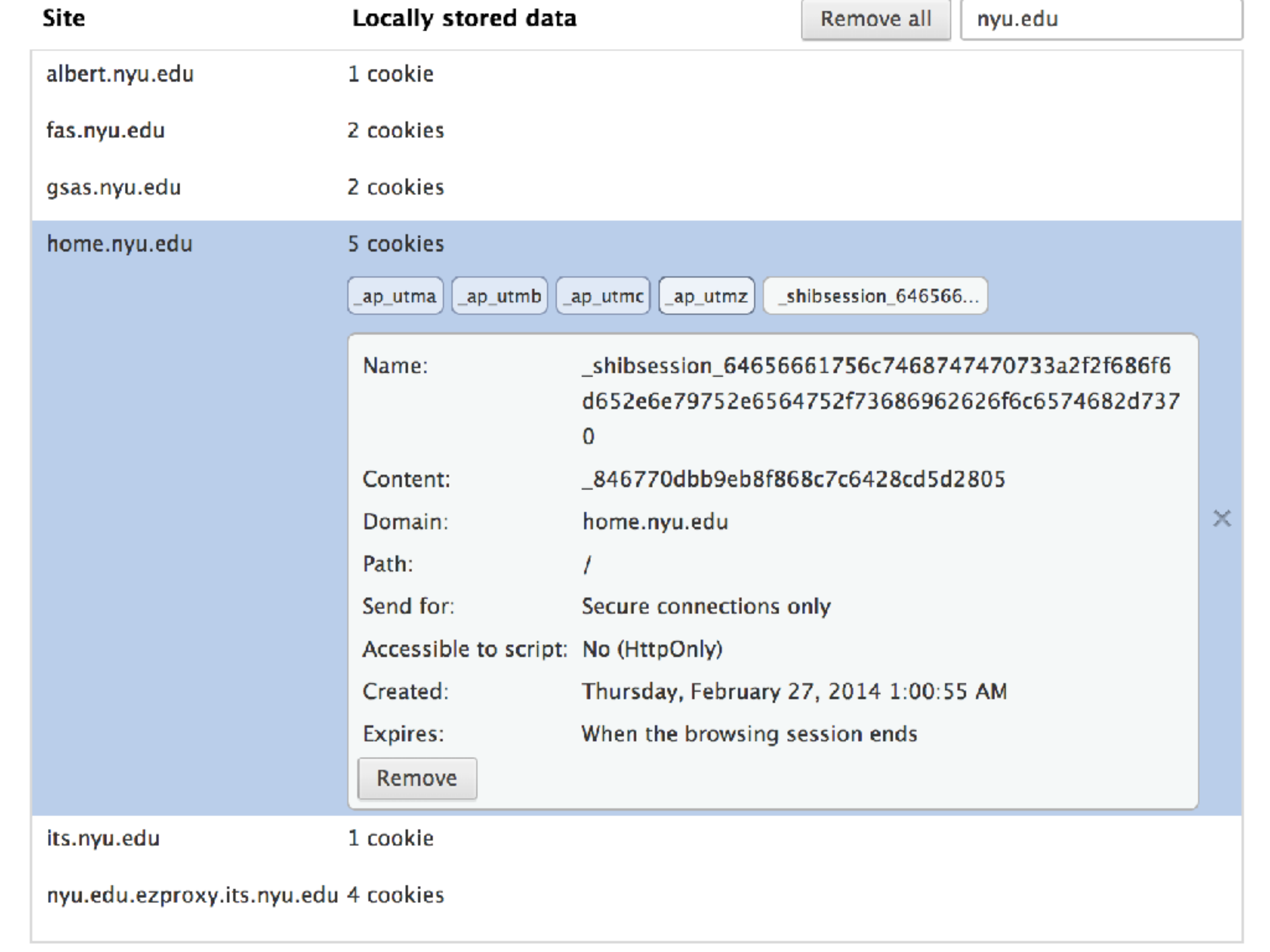
Cookies and site data

Remove all · nyu.edu

Site	Locally stored data
albert.nyu.edu	1 cookie
fas.nyu.edu	2 cookies
gsas.nyu.edu	2 cookies
home.nyu.edu	5 cookies
its.nyu.edu	1 cookie
nyu.edu.ezproxy.its.nyu.edu	4 cookies

_ap_utma · _ap_utmb · _ap_utmc · _ap_utmz · _shibsession_646566...

Name:	_shibsession_64656661756c7468747470733a2f2f686f6d652e6e79752e6564752f73686962626f6c6574682d7370
Content:	_846770dbb9eb8f868c7c6428cd5d2805
Domain:	home.nyu.edu
Path:	/
Send for:	Secure connections only
Accessible to script:	No (HttpOnly)
Created:	Thursday, February 27, 2014 1:00:55 AM
Expires:	When the browsing session ends



Site	Locally stored data
albert.nyu.edu	1 cookie
fas.nyu.edu	2 cookies
gsas.nyu.edu	2 cookies
home.nyu.edu	5 cookies
its.nyu.edu	1 cookie
nyu.edu.ezproxy.its.nyu.edu	4 cookies

Name: _shibsession_64656661756c7468747470733a2f2f686f6d652e6e79752e6564752f73686962626f6c6574682d7370

Content: _846770dbb9eb8f868c7c6428cd5d2805

Domain: home.nyu.edu

Path: /

Send for: Secure connections only

Accessible to script: No (HttpOnly)

Created: Thursday, February 27, 2014 1:00:55 AM

Expires: When the browsing session ends