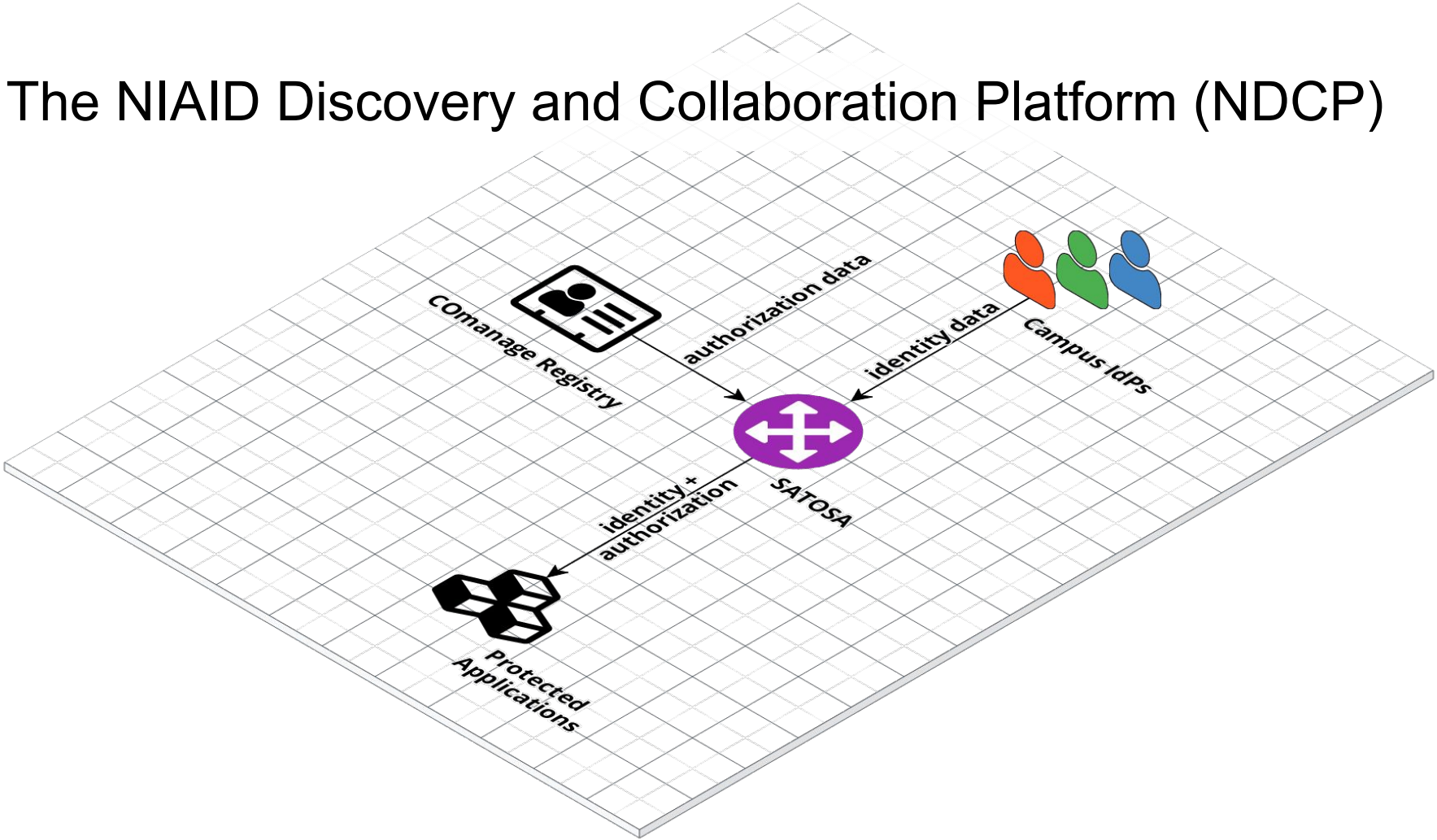
Dynamic MFA

privacyIDEA, SATOSA, and COmanage

The NIAID Discovery and Collaboration Platform (NDCP)



🤔 The Authenticator Assurance Challenge

Phishing is the most common form of cyber crime…

…that can be mitigated using multi-factor authentication…

…but many identity providers have yet to implement MFA.

Dynamically determine whether to
implement step-up MFA
on a per-identity basis
using free/libre/open source software.

Our Approach

Inspect the context of all successful authentication responses for supported MFA authentication contexts (e.g., REFEDS MFA).

Our Approach

Inspect the context of all successful authentication responses for supported MFA authentication contexts (e.g., REFEDS MFA).

Redirect users to a second identity provider for multi-factor authentication (e.g., TOTP).

Our Approach

Inspect the context of all successful authentication responses for supported MFA authentication contexts (e.g., REFEDS MFA).

Redirect users to a second identity provider for multi-factor authentication (e.g., TOTP).

Control which services require MFA.

Our Approach

Inspect the context of all successful authentication responses for supported MFA authentication contexts (e.g., REFEDS MFA).

Redirect users to a second identity provider for multi-factor authentication (e.g., TOTP).

Control which services require MFA.

Control which users must use MFA.

Our Approach

Inspect the context of all successful authentication responses for supported MFA authentication contexts (e.g., REFEDS MFA).

Redirect users to a second identity provider for multi-factor authentication (e.g., TOTP).

Control which services require MFA.

Control which users must use MFA.

Give new users thirty days to enroll in step-up MFA.

Dynamic MFA =

COmanage

(MeemEnroller + PrivacyIdeaAuthenticator)

+ privacyIDEA (TOTP)

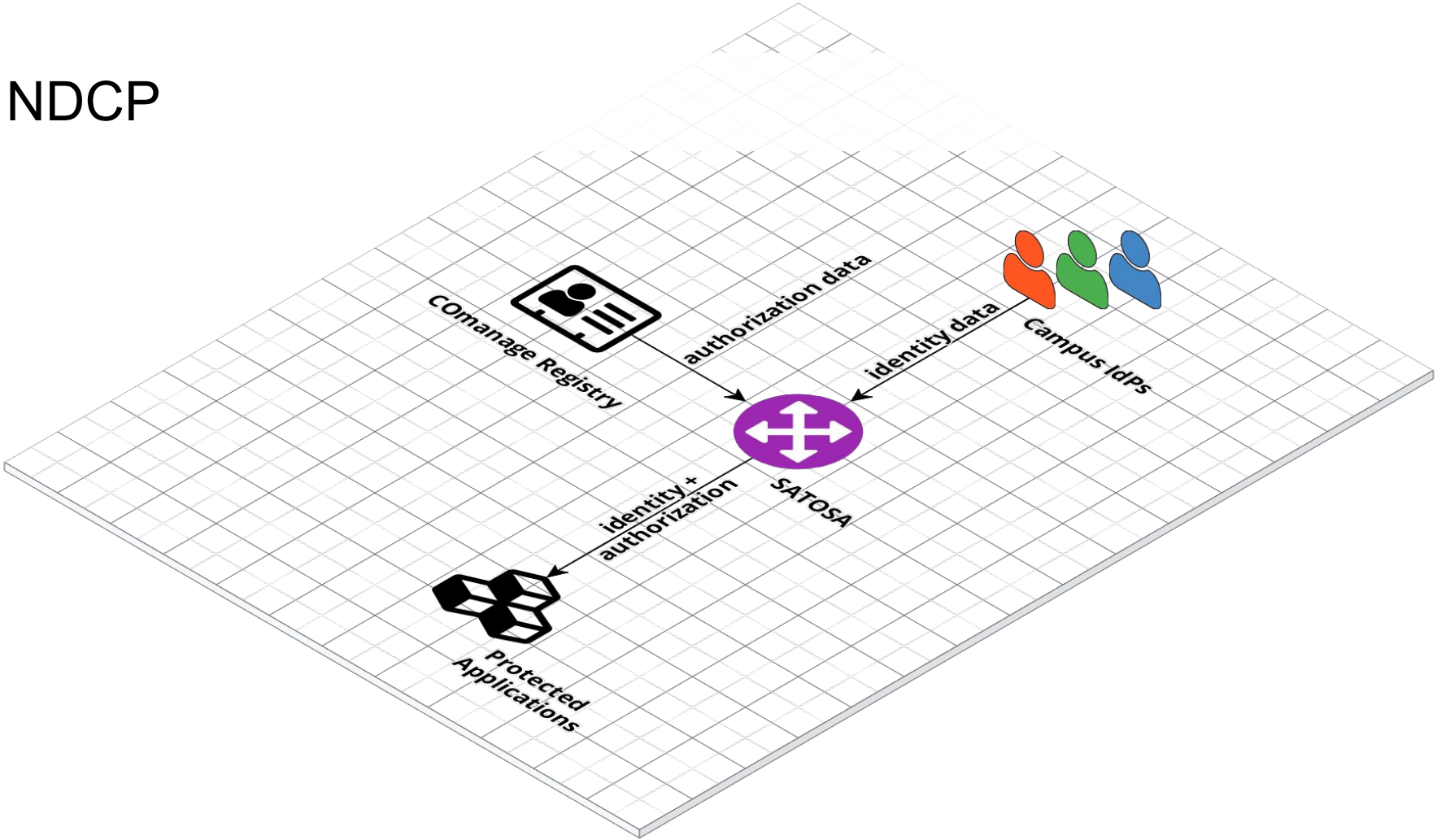
+ SATOSA

(stepup + comanage_meem_enroller)

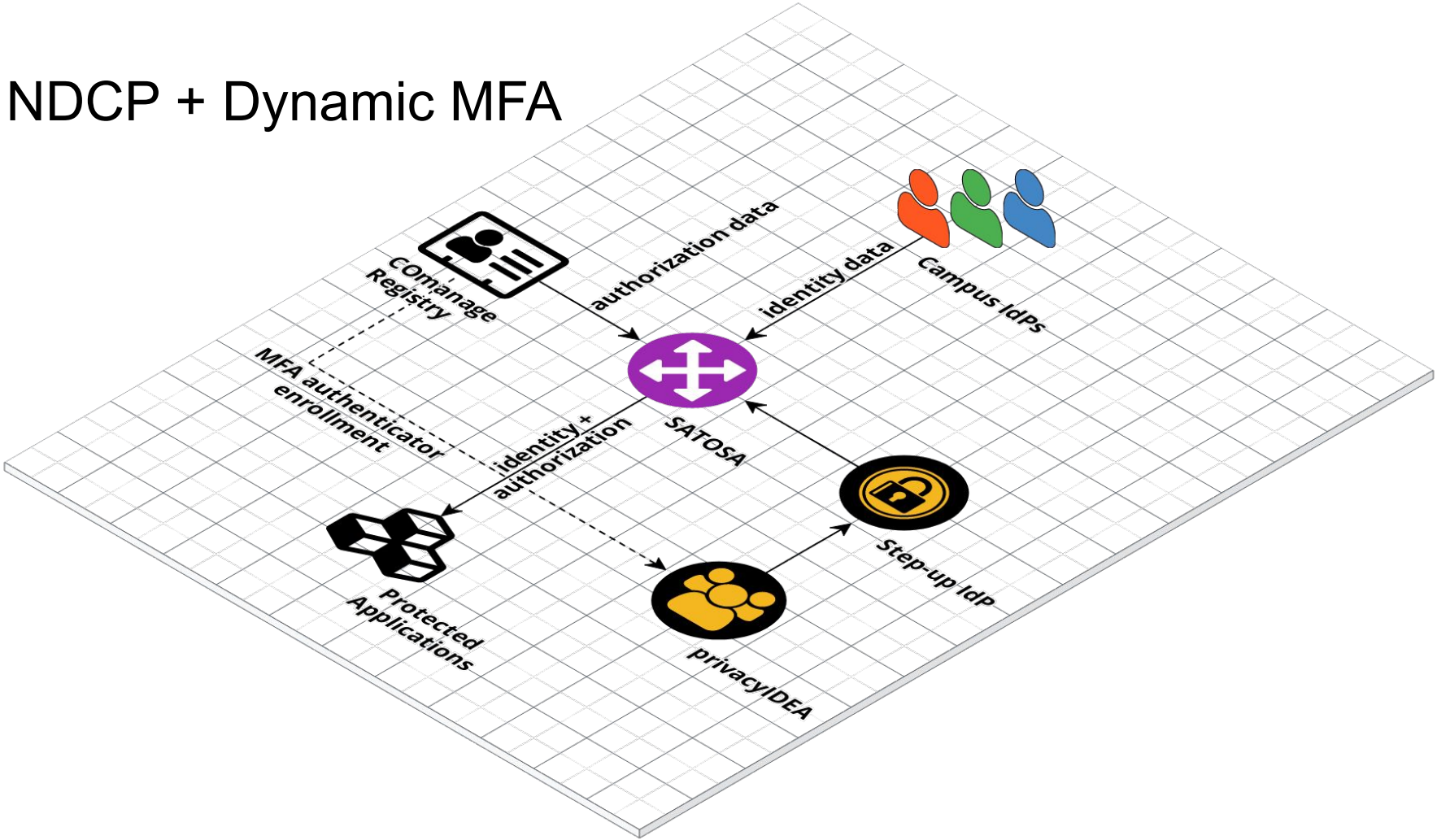
+ voPerson

+ python-stepup-idp (pysaml2)

NDCP


COmanage Registry
authorization data
identity data
Campus IdPs
SATOSA
identity +
authorization
Protected
Applications

NDCP + Dynamic MFA



MeemEnroller

COmanage Registry plugin: MFA Enrollment and Exemption Manager

MeemEnroller

COmanage Registry plugin: MFA Enrollment and Exemption Manager

During an Enrollment Flow, the Proxy signals to MeemEnroller if MFA was asserted (via env variables)

MeemEnroller

COmanage Registry plugin: MFA Enrollment and Exemption Manager

During an Enrollment Flow, the Proxy signals to MeemEnroller if MFA was asserted (via env variables)

If not, the Enrollee may optionally be added to a exemption CO Group for a configurable duration

MeemEnroller

COmanage Registry plugin: MFA Enrollment and Exemption Manager

During an Enrollment Flow, the Proxy signals to MeemEnroller if MFA was asserted (via env variables)

If not, the Enrollee may optionally be added to a exemption CO Group for a configurable duration

After the main Enrollment Flow is complete, the enrollee is offered the option to set up MFA. (In this case, via PrivacyIdeaAuthenticator with TOTP tokens.)

MeemEnroller

COmanage Registry plugin: MFA Enrollment and Exemption Manager

During an Enrollment Flow, the Proxy signals to MeemEnroller if MFA was asserted (via env variables)

If not, the Enrollee may optionally be added to a exemption CO Group for a configurable duration

After the main Enrollment Flow is complete, the enrollee is offered the option to set up MFA. (In this case, via PrivacyIdeaAuthenticator with TOTP tokens.)

At authentication run time, the Proxy can determine whether the user has enrolled in MFA (via the voPersonToken attribute), and if not send them to a reminder page

🛠️ Deploying Dynamic MFA

Three groups control MFA following the principle of **management by exception**:

- Require multi-factor authentication
- Temporarily allow single-factor authentication (bypasses MFA for 30 days)
- Always allow single-factor authentication (bypass MFA permanently)

🛠️ Deploying Dynamic MFA

Deploy following the principle of **progressive enhancement**:

1. Add test users to the “Require MFA” group.
2. Enroll new users in both “Require MFA” and “Temporarily bypass MFA”.
3. Add existing users to “Require MFA” in batches (e.g., by COU).

🎓 Lessons Learned

User experience is the key to success.

Some campus IdPs implement MFA but do not signal it.

Be on the lookout for non-standard authentication context classes (e.g., urn:gov:gsa:ac:classes:sp:PasswordProtectedTransport:duo).

 Experience with privacyIDEA

The LDAP Backend is not paginated, and the administrative frontend will not scale to very large deployments.

The admin UI does not support search by user or token serial number.

It is not possible to deep link to a user or token from an external application (such as the Registry Authenticator management interface).

API tokens expire after 1 year with no warning in the administrative interface.

🔮 Planned Enhancements

Enforce MFA for all services and all users.

Add support for backup codes, WebAuthn, privacyIDEA app.

Better document the step-up MFA on-boarding process.

Migrate step-up IdP and privacyIDEA to GitOps.

Step-up Identity Proofing

🙌 Acknowledgements

NIAID:

- Michael Tartakovsky
- Matt Eisenberg
- Chris Whalen

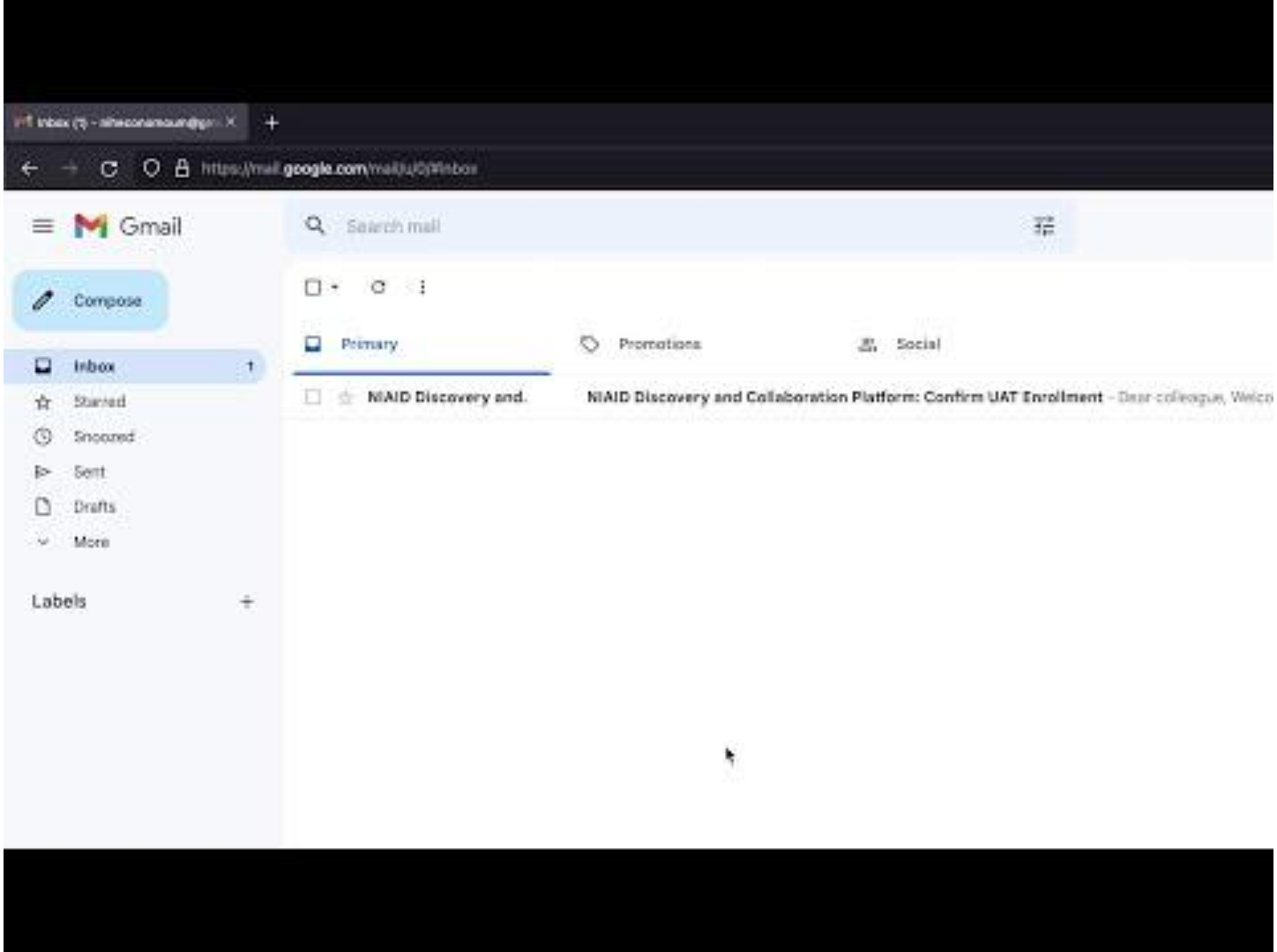
SCG:

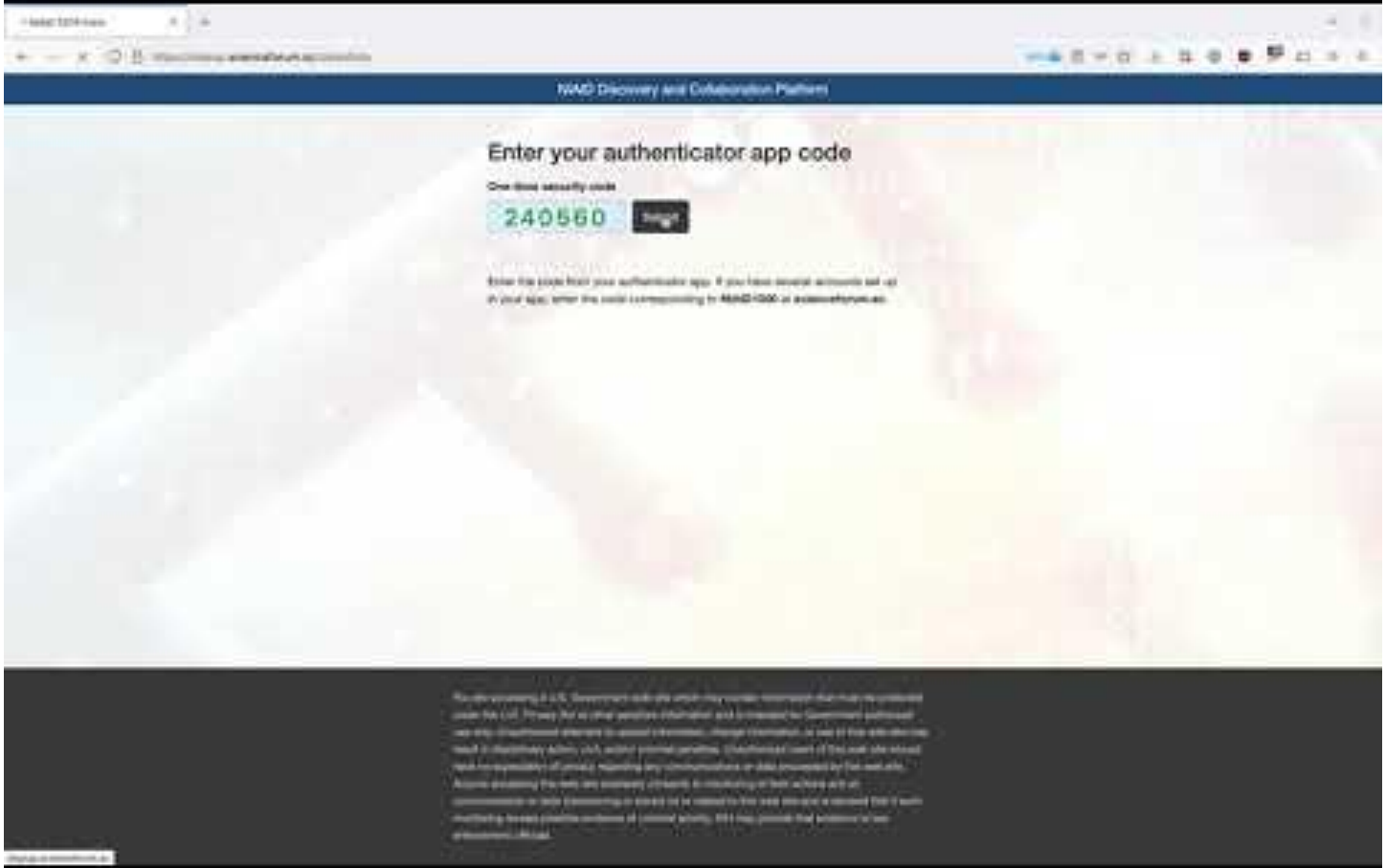
- Scott Koranda
- Shayna Atkinson
- Arlen Johnson

The privacyIDEA project

SAMLtest:

- Nate Klingenstein and team at SIGNET


https://mail.google.com/mail/u/0/#inbox
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
Primary
Promotions
Social
NIAID Discovery and.
NIAID Discovery and Collaboration Platform: Confirm UAT Enrollment - Dear colleague, Welco


NIAID Discovery and Collaboration Platform
Enter your authenticator app code
One-time security code
240560
Submit

fin

MeemEnroller