SAND2023-07687C

Sandia National Laboratories

Exceptional service in the national interest

Journey to Azure B2B

Presenters

Valerie Silva, *Enterprise Cloud Services* | *vrsilva@sandia.gov*

Marc Sanchez, *Enterprise Cloud Services* | *msanch7@sandia.gov*

SAND2023-05218PE

Agenda

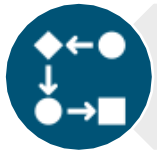
1. Collaboration challenges
2. What is Azure B2B?
3. Sandia's approach to B2B
4. Architecture
5. Workflow

B2B at Sandia

Collaboration Requirements

Must vet all users

Requires trusted identity source (OneID)



Access must use an approval process

Two-factor authentication must be verifiable (CBA)

Guest access is granular and must be timebound

Guest access must be validated daily

What is Azure B2B?

Microsoft Provides two forms of B2B Collaboration

Azure B2B Collaboration

- Allows external users to use their own identity provider such as Azure AD. Applications registered with your Azure AD tenant can be made available for access. A guest account will be created in your tenant.

Azure B2B Direct Connection

(Teams Shared Channel)

- A mutual two-way trust relationship between Azure AD tenants that allows seamless collaboration. No guest account is created in the resource tenant. The feature only supports Teams shared channels.

Azure B2C - Allows the creation of a tenant to support a SaaS or custom app to collaborate with external users. All accounts used for collaboration are guest accounts in the Azure B2C tenant.

Sandia's approach to B2B

Self-Service Model

- The design must be self-service

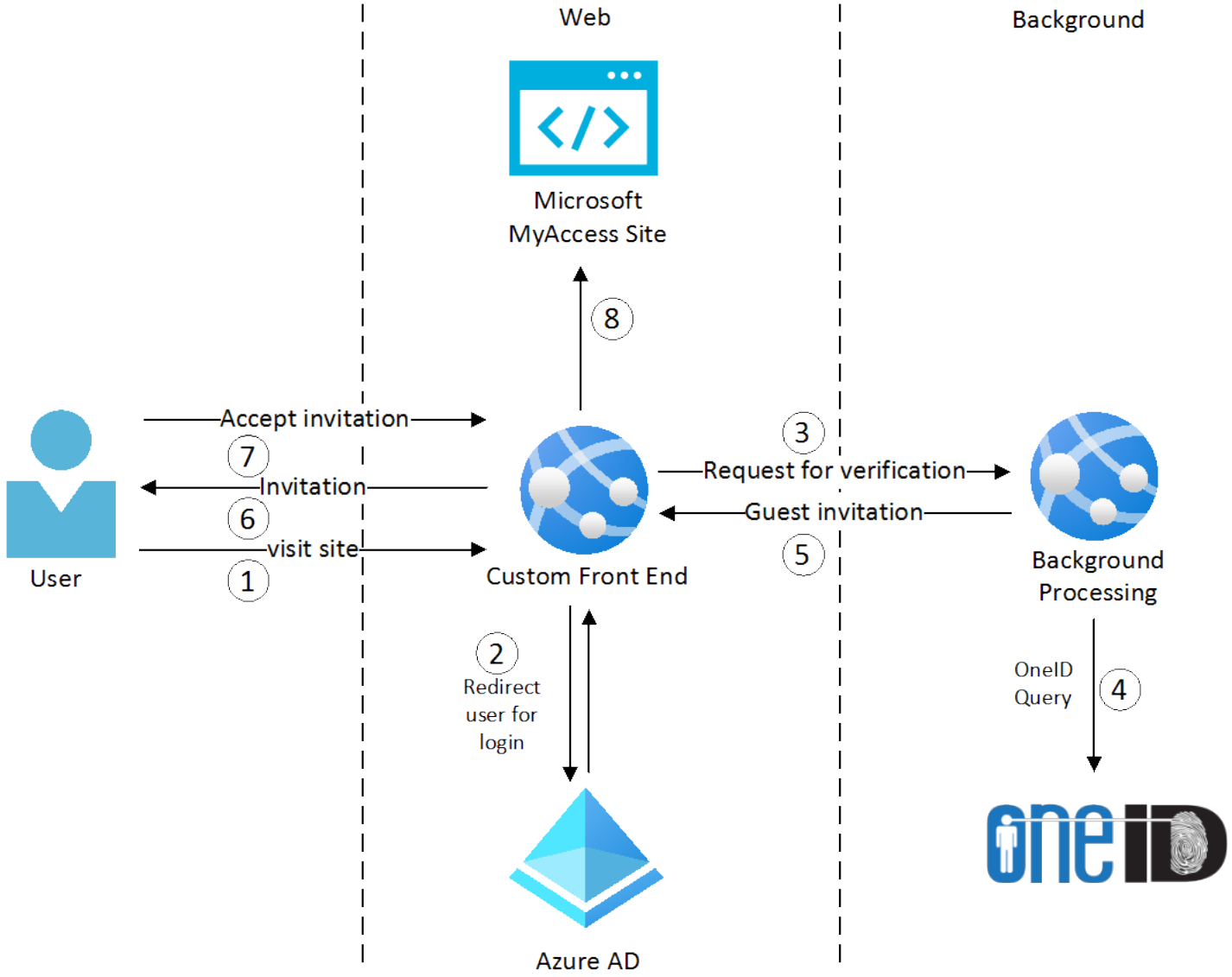
OneID Integration

- Use OneID as a trusted source

Micro-segmentation

- Access Packages provide granular access

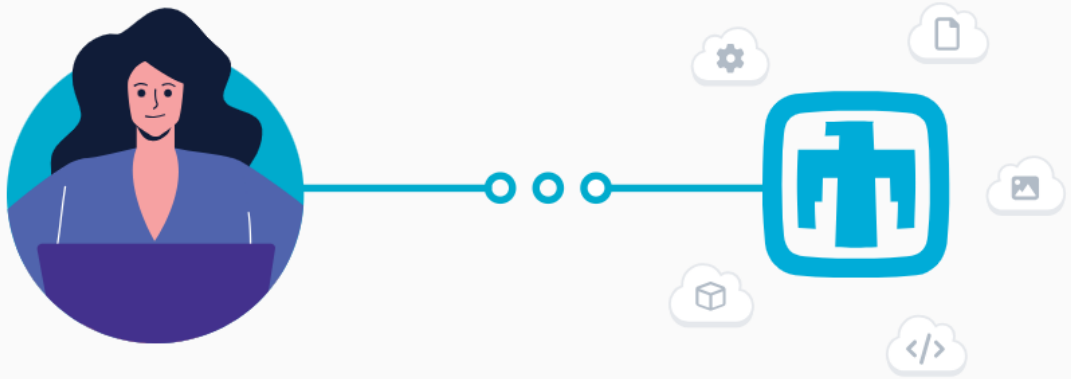
Onboarding Process



Walkthrough

Sandia National Laboratories

Sandia External Collaboration



Collaborate with Sandia National Laboratories

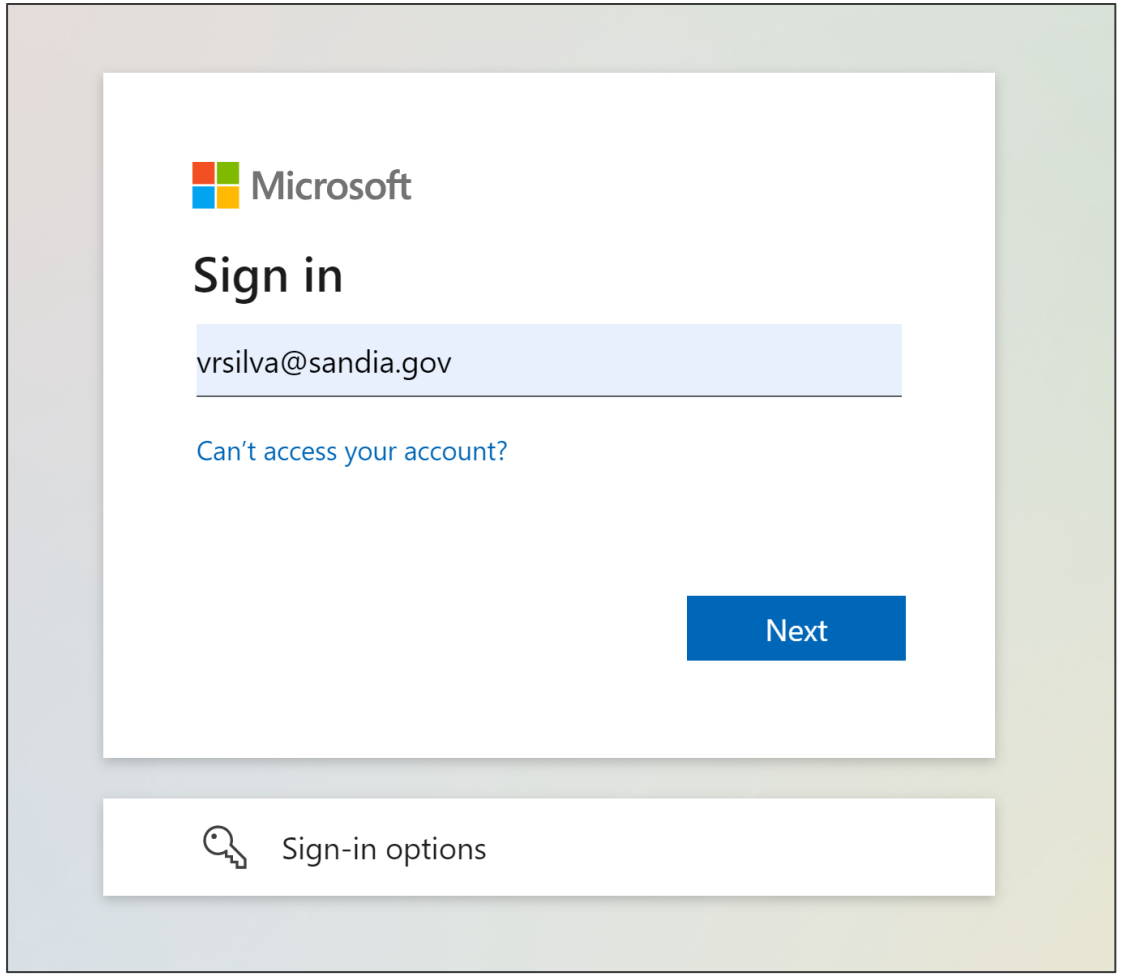
Please login with your work account in order to request access to Sandia resources.

Login

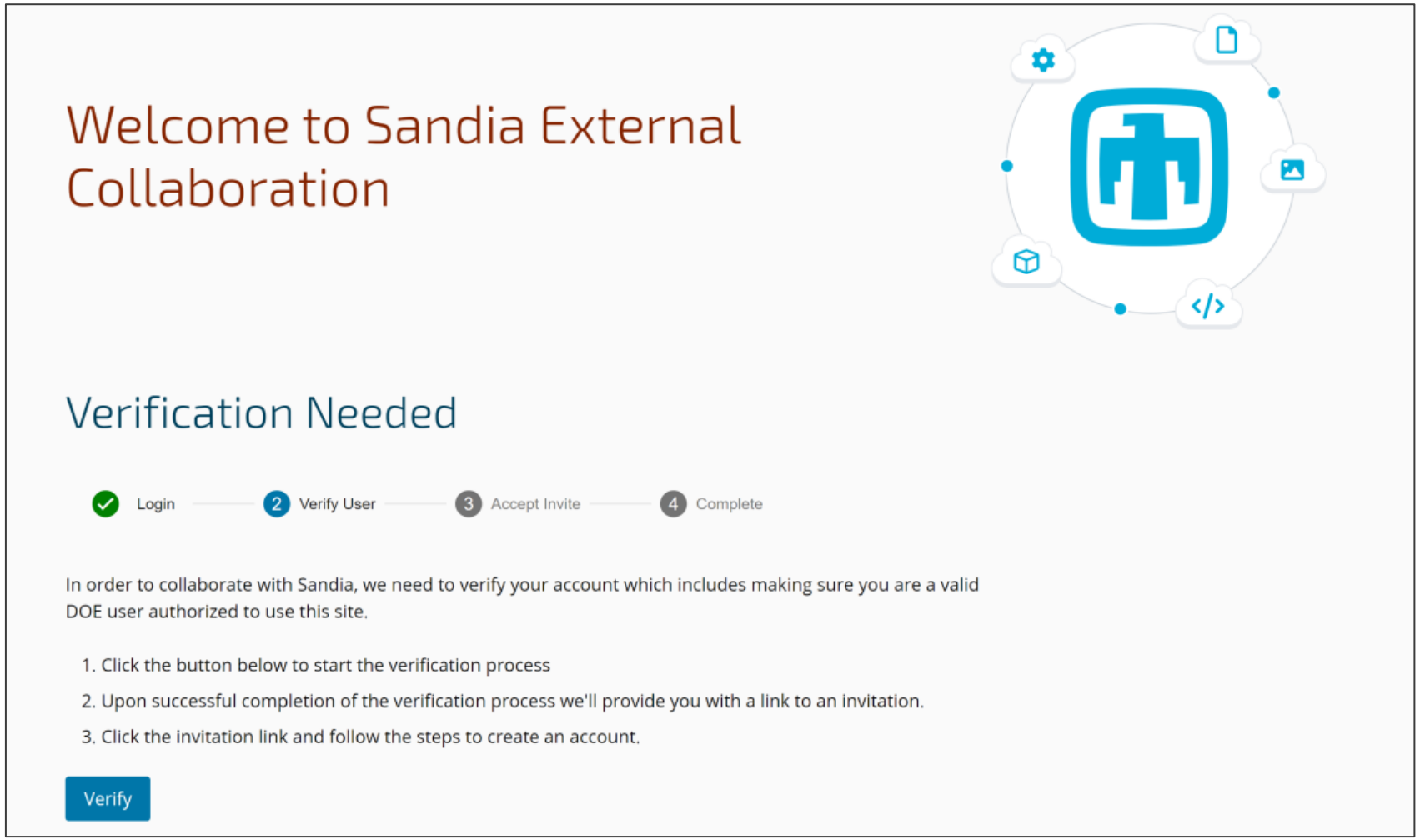
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Learn about the Department of Energy's Vulnerability Disclosure Program

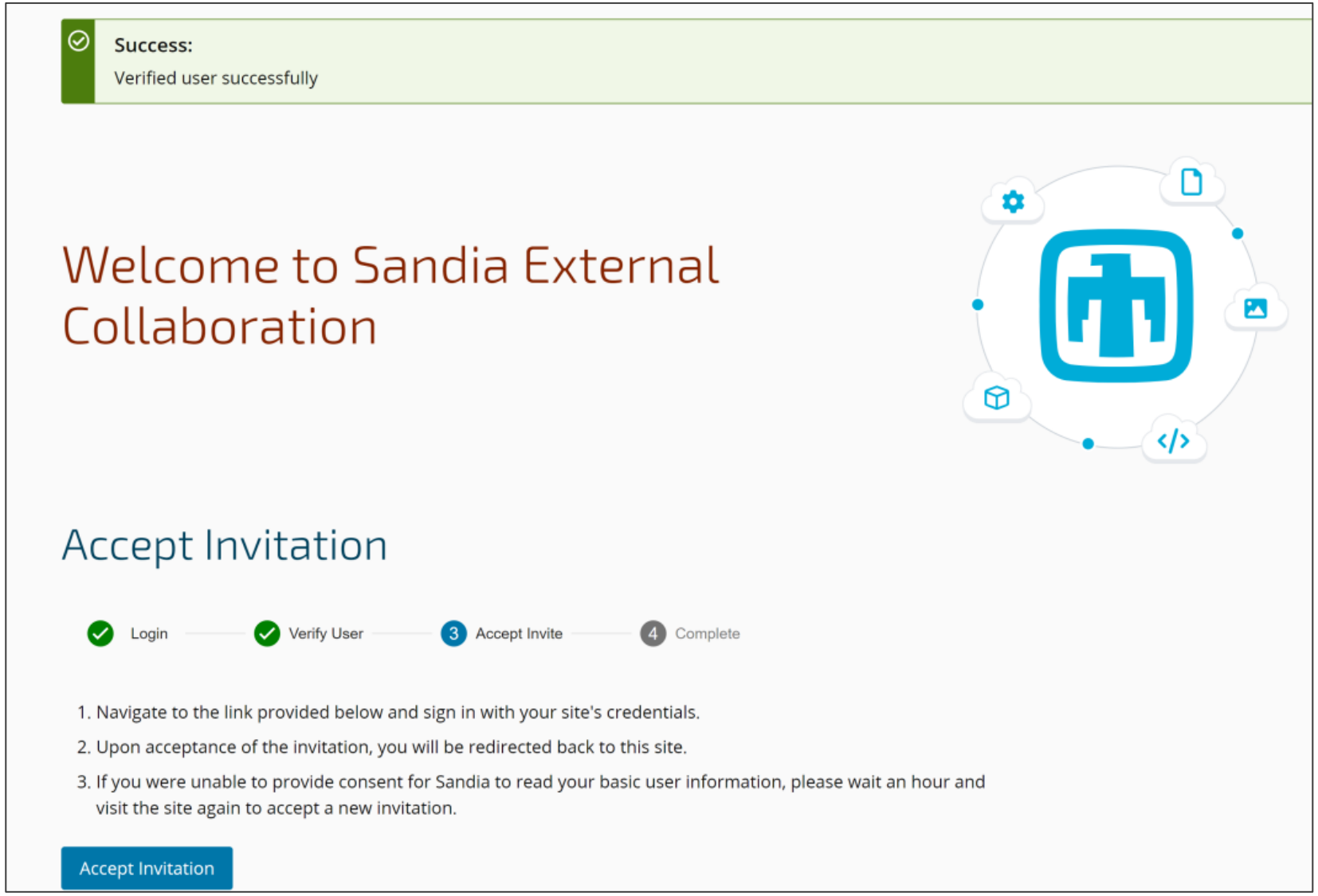
Onboarding B2B Accounts



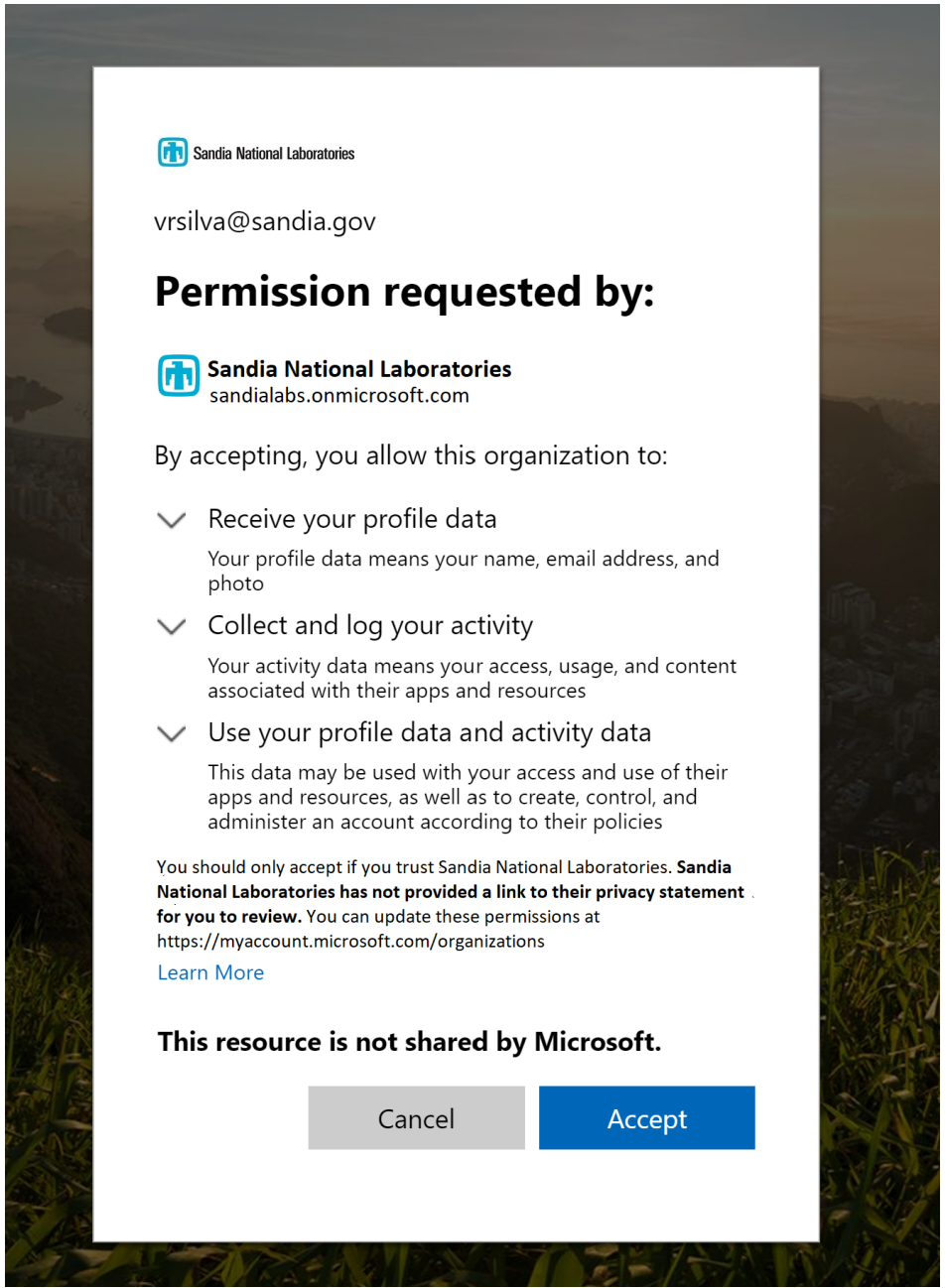
Onboarding B2B Accounts



Onboarding B2B Accounts



Onboarding B2B Accounts



Onboarding B2B Accounts

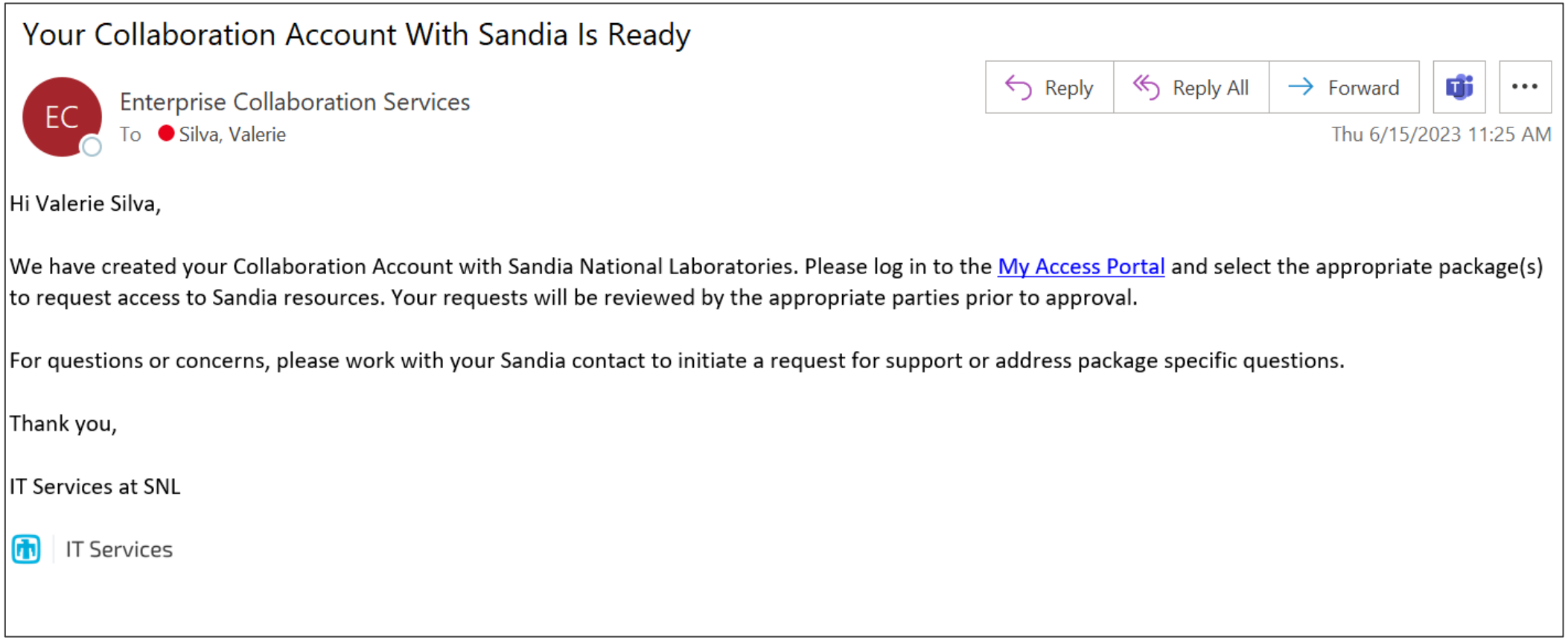
Welcome to Sandia External Collaboration

Thank you for collaborating with Sandia!

What to expect:

- Look out for an email from noreply-ecs@sandia.gov within the next hour with instructions detailing how to access Sandia resources.
- If you were unable to complete the entire invitation process, please wait an hour and visit this site again to generate a new invitation.

Onboarding B2B Accounts



Your Collaboration Account With Sandia Is Ready

EC

Enterprise Collaboration Services

To Silva, Valerie

Reply | Reply All | Forward

Thu 6/15/2023 11:25 AM

Hi Valerie Silva,

We have created your Collaboration Account with Sandia National Laboratories. Please log in to the My Access Portal and select the appropriate package(s) to request access to Sandia resources. Your requests will be reviewed by the appropriate parties prior to approval.

For questions or concerns, please work with your Sandia contact to initiate a request for support or address package specific questions.

Thank you,

IT Services at SNL

IT Services

Onboarding B2B Accounts

Welcome to Sandia External Collaboration

Your collaboration account is ready!

Login — Verify User — Accept Invite — Complete

Please visit the My Access Portal: to start collaborating!

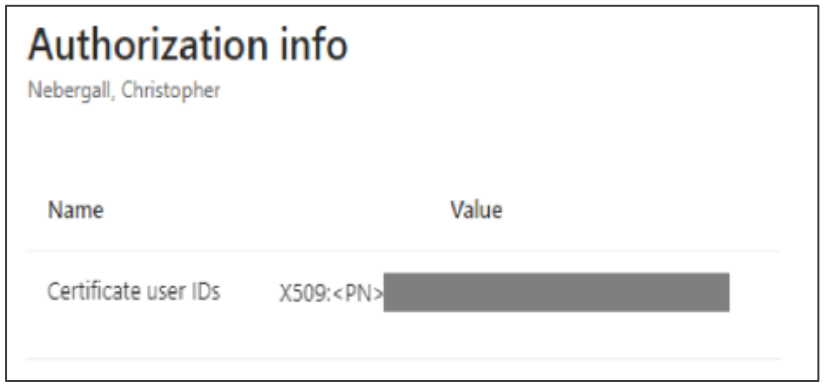
CBA Configuration

Certificate Mapping on Guest Accounts

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username binding.

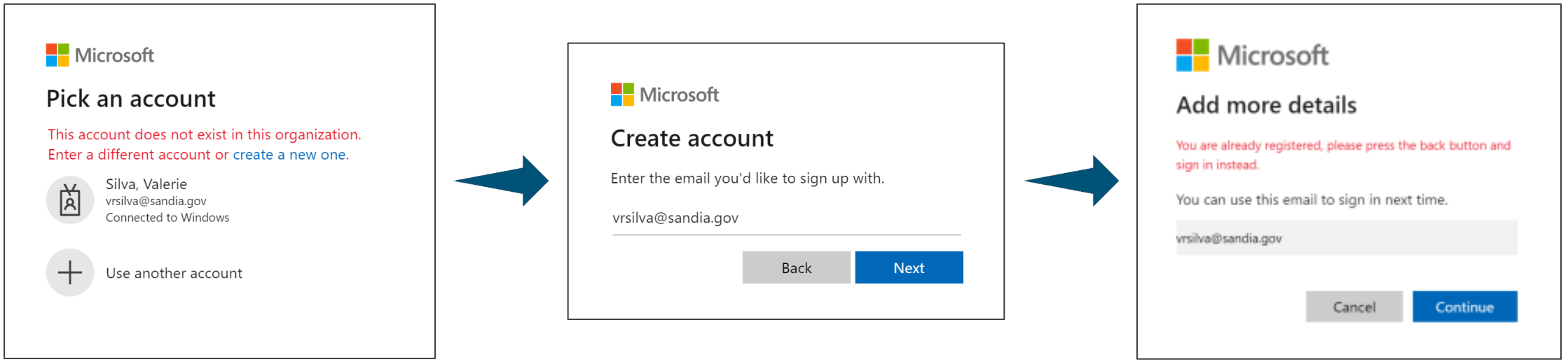
Certificate field	User attribute
1 RFC822Name	certificateUserIds
2 PrincipalName	certificateUserIds
3 SubjectKeyIdentifier	certificateUserIds
4 SHA1PublicKey	certificateUserIds



Challenges

User Flow and Exchange Contacts

Email addresses that are associated with Exchange contacts can’t onboard during user flow



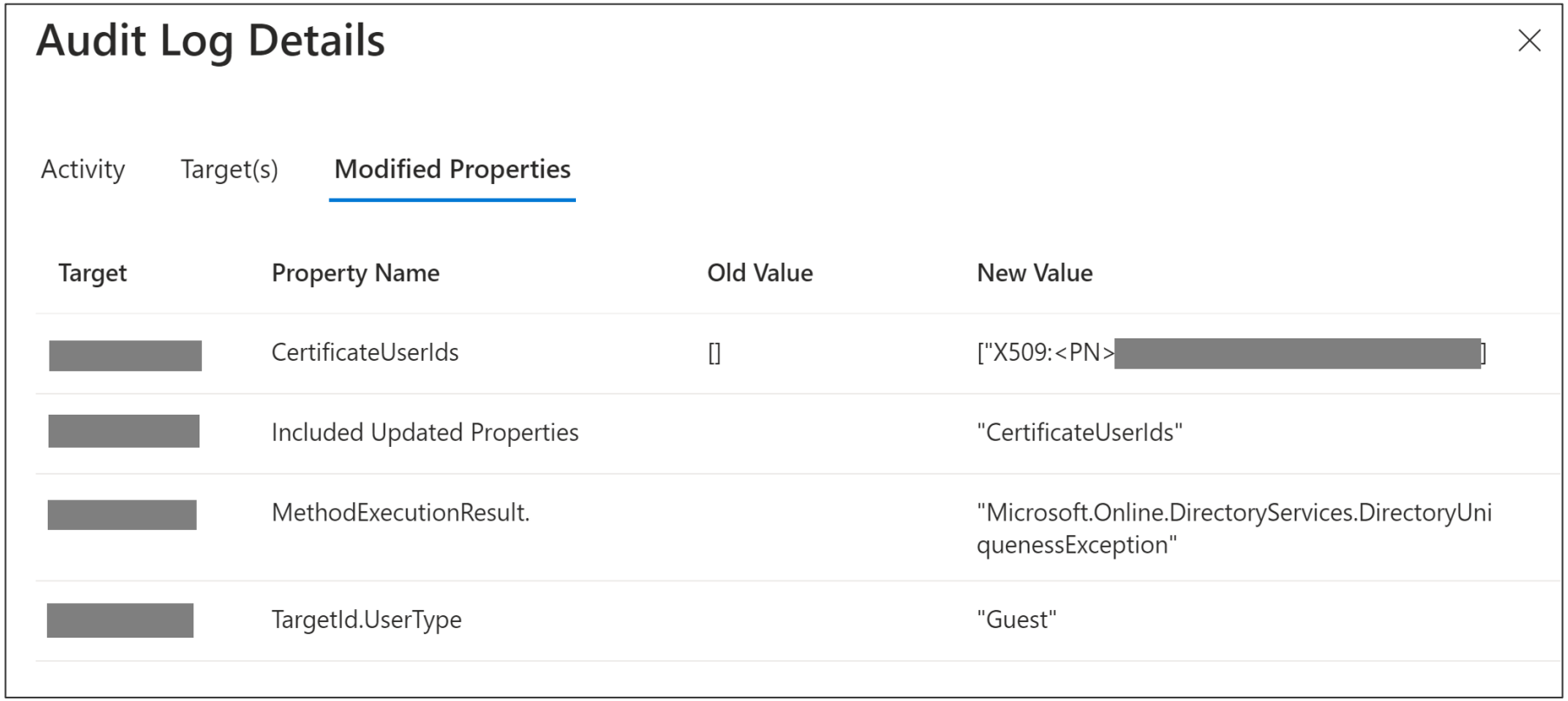
1. User attempts sign in and is prompted to create account

2. User starts account creation process

3. User is informed their account is already created

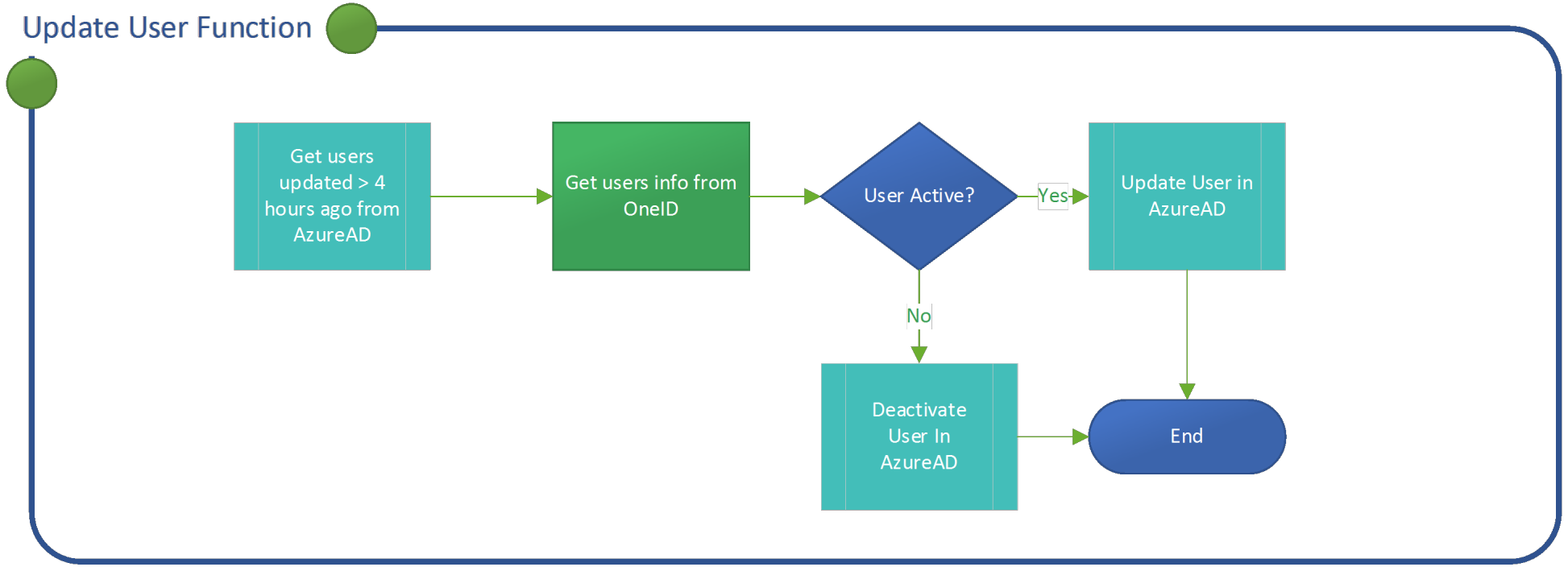
Certificate Based Authentication

- Certificate can only be tied to one account
- There are many people across DOE Complex with two or more accounts



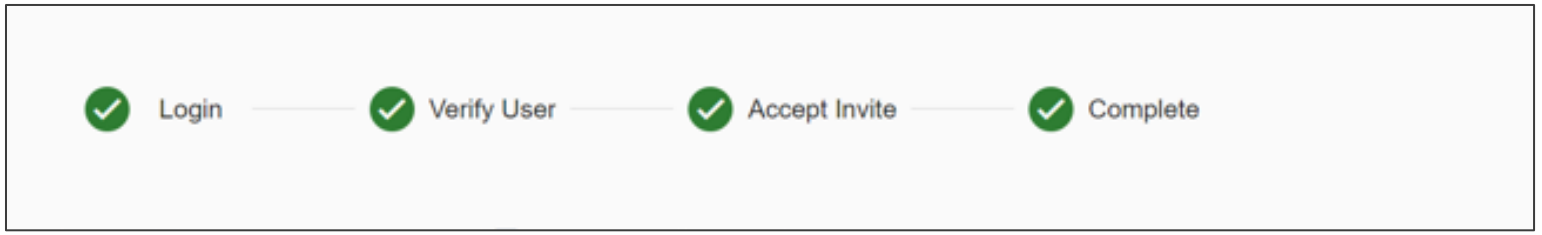
User Lifecycle

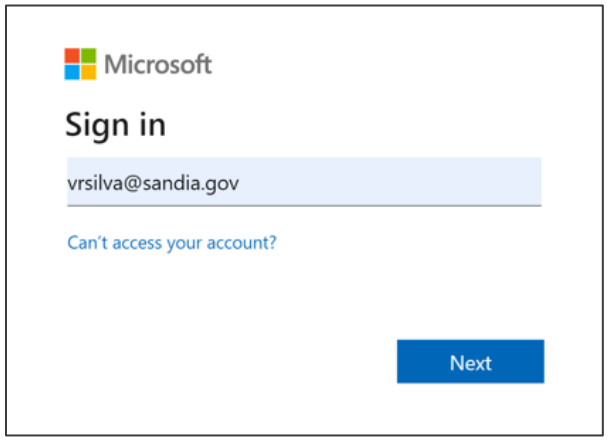
The re-verification process runs every 4 hours to ensure the user is up-to-date in Azure AD

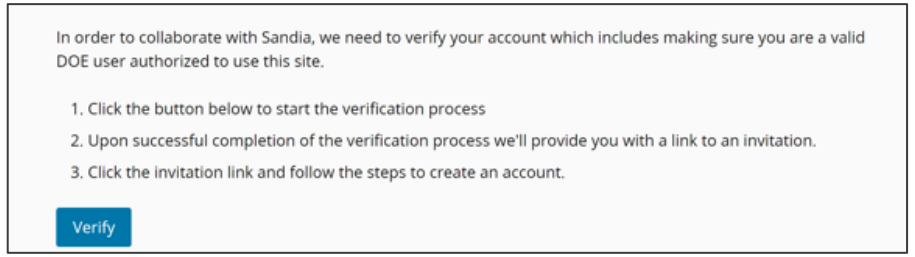


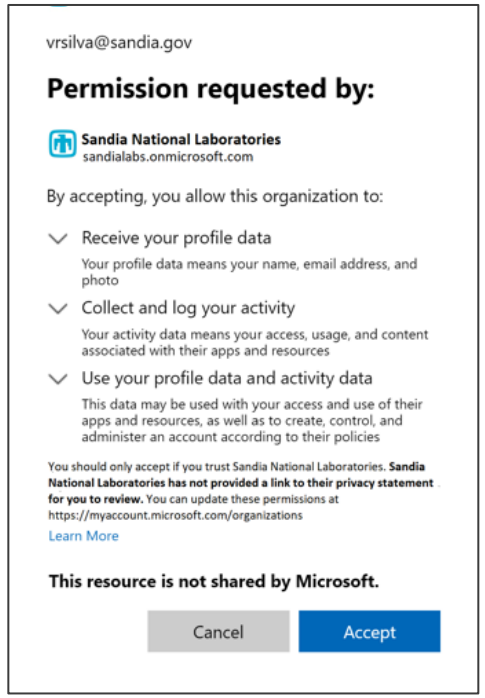
UX Struggles

- Sign In permission page can’t be modified
- Users redirected between our site and Microsoft sign in process
- User might not accept permission
- Timing issues



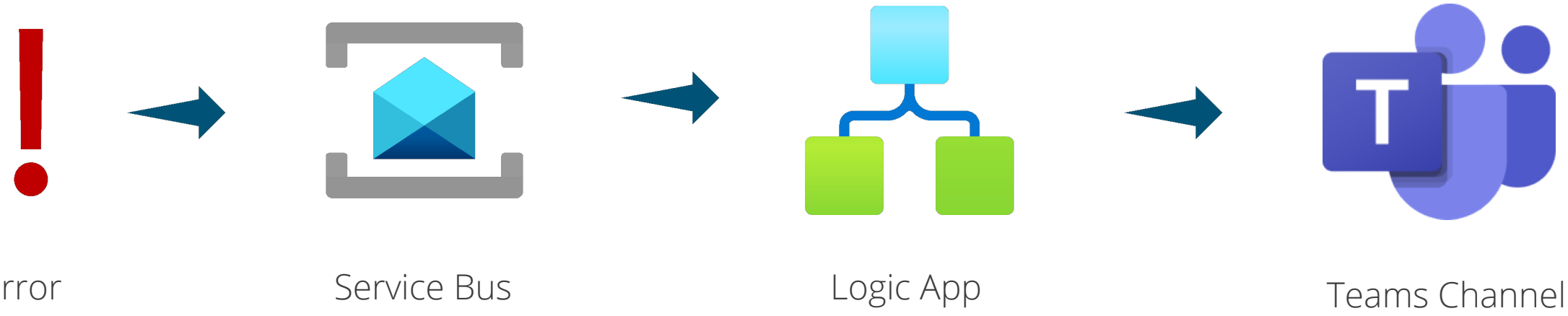






Support for External Audience

- Failure could occur in our application or in home tenant
- Where should people submit service requests?
- Can’t route external users to internal support



Future State

Future State

Access package creation self-service

Expand beyond Office 365 applications

Expand beyond DOE Complex users

Questions