twocanoes

Platform SSO

Timothy Perfitt
Twocanoes Software
tperfitt@twocanoes.com

Intro

- Timothy Perfitt, founder of Twocanoes Software in 2012

- Apple Engineer, 2001-2012

- Maker of Winclone, Boot Runner, Bluetooth Smart Card Reader, XCreds, Bluetooth Beacons, and many smaller utilities (DFU Blaster :))

- Working with Apple to provide additional tutorials and documentation for PSSO

What is the purpose of Platform SSO?

- Platform Single Sign On (PSSO) is a native way to get single sign-on tokens at the login to allow an Enterprise Single Sign-On Extension (eSSO)

- eSSO is a system extension to share tokens between Apps and Web Pages.

Purpose

- Understand what PSSO is for, how it is configured, and how it works
- No crypto, no config files, no message flow diagrams. Concepts. Lots of Concepts. and a Demo.
- No Kerberos. No WS-Trust.

What PSSO Isn't and Isn't Supposed to Be

- MFA Prompts At Login Window
- User creation for One-To-One deployments
- Compatible with a predefined SSO protocol

Enterprise Single Sign On

- System extension deployed in an app that extends macOS in the user session
- Requires URLs registered via MDM that will be redirected to the single sign-on extension
- The host of the redirect URLs must contain an associated domain JSON file that contains the team ID and bundle identifier of the extension.
- Host must be accessible by Apple's CDN
- Host must have a Apple provided certificate trusted by the System Root, and cannot use other root certificates

Say That A Different Way

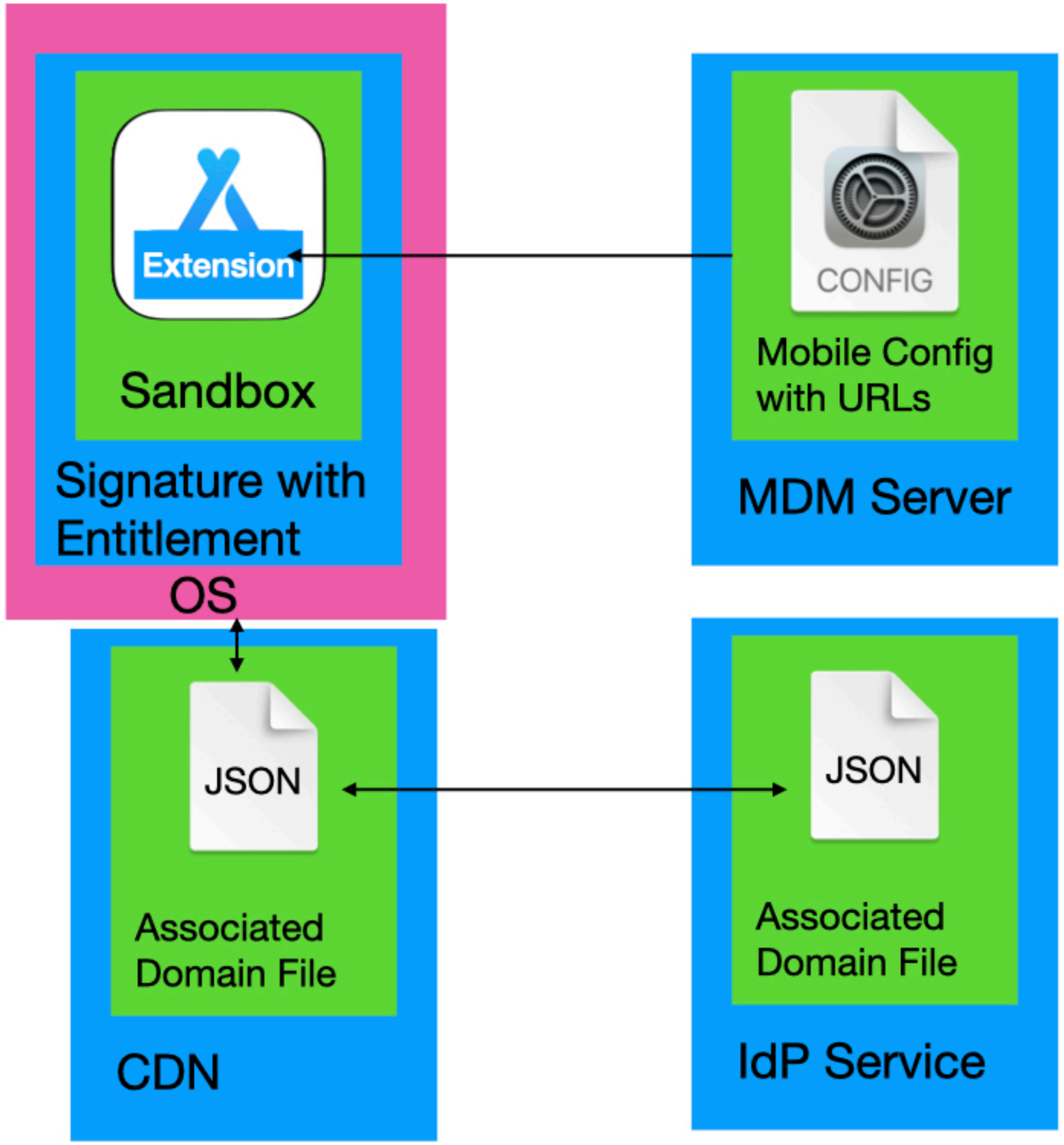
- Device must trust the configuration (MDM enrollment)

- The identity Provider must approve the extension by providing the JSON file at its endpoint.

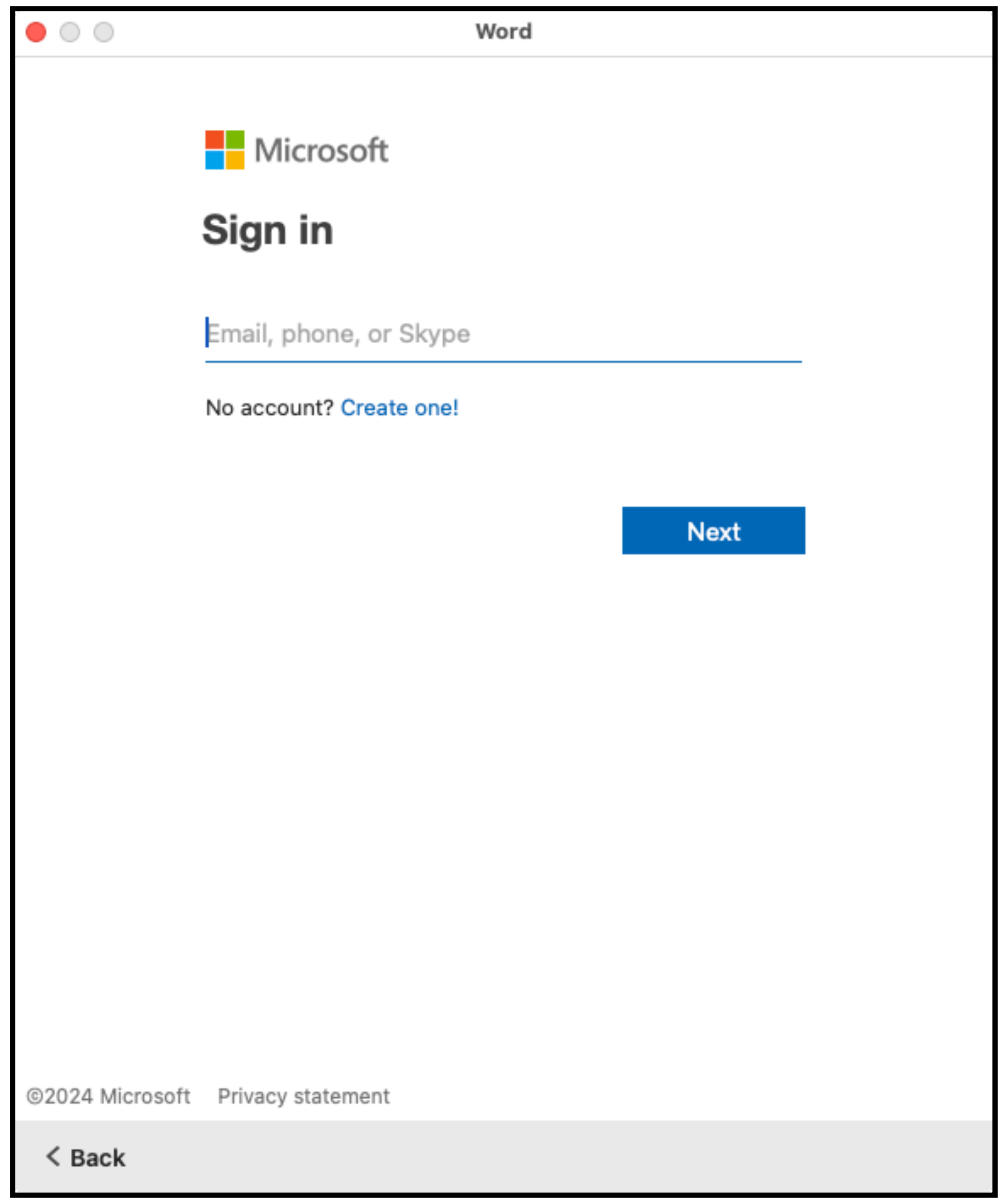
- TLS sniffing using 3rd party tools that require installed roots will not work

- You can't run it internally (Associated Domain / CDN Requirement)

Trust


Extension
Sandbox
Signature with Entitlement
OS
CONFIG
Mobile Config with URLs
MDM Server
JSON
Associated Domain File
CDN
JSON
Associated Domain File
IdP Service

App with SSO



Word

Microsoft

Sign in

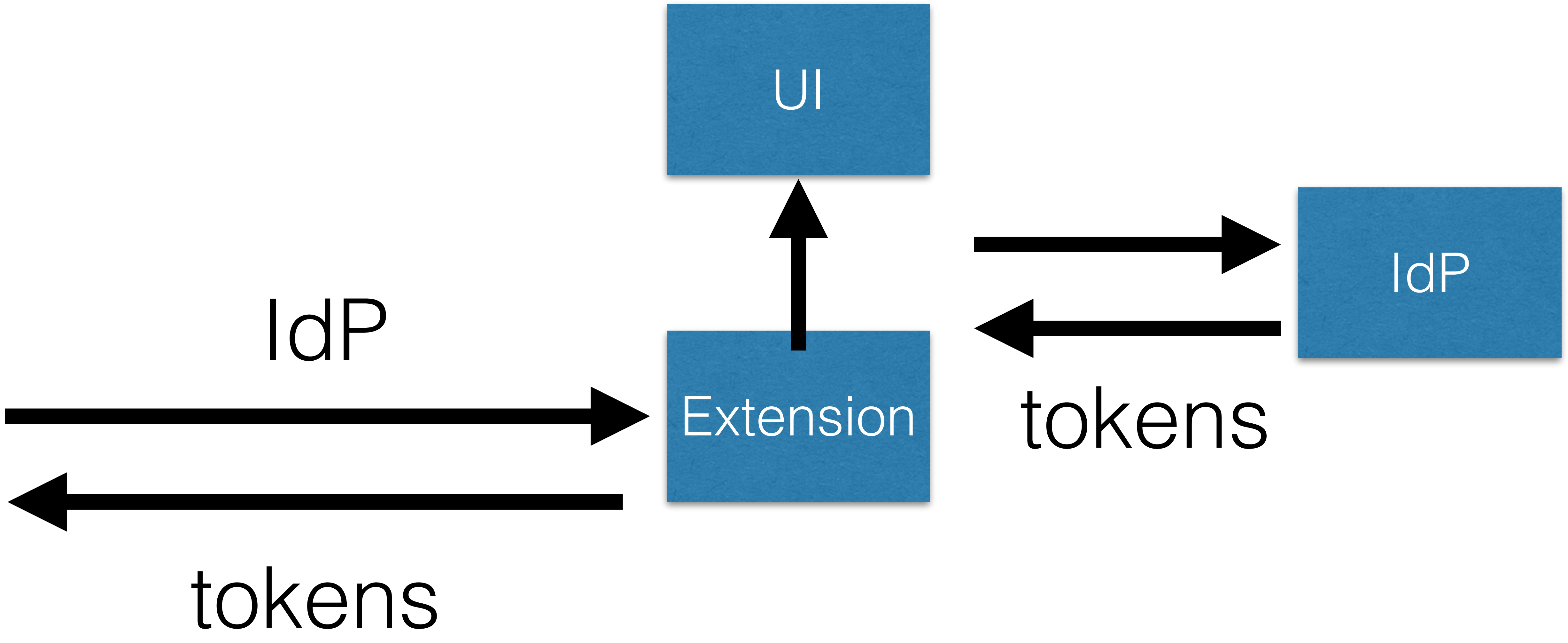
Email, phone, or Skype

No account? Create one!

Next

©2024 Microsoft Privacy statement

< Back



I thought this was about PSSO!

What is the purpose of Platform SSO?

- Platform Single Sign On (PSSO) is a native way to get single sign-on tokens at the login to allow an Enterprise Single Sign-On Extension (eSSO)

- eSSO is a system extension to share tokens between Apps and Web Pages.

PSSO

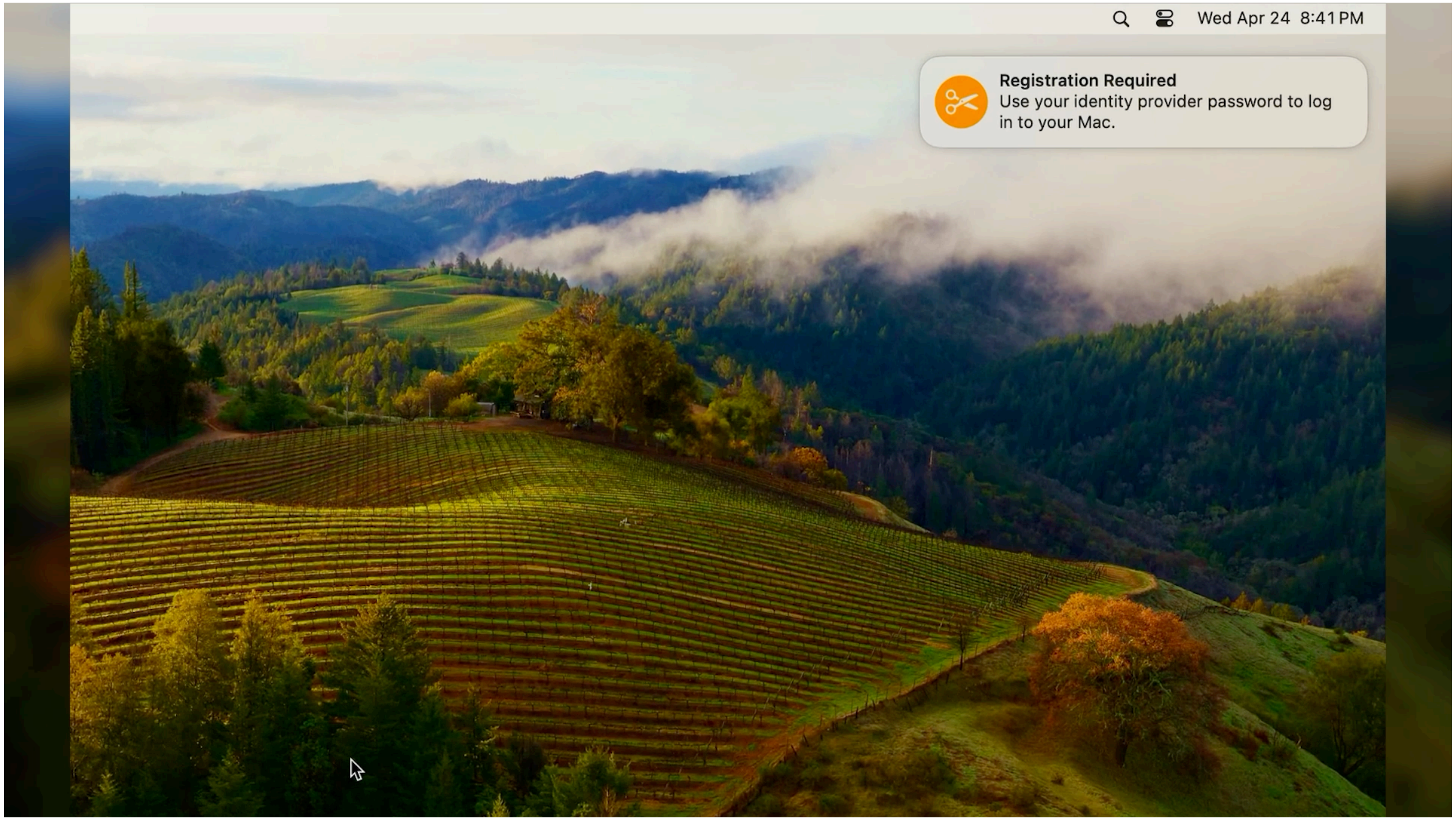
Login Window Username and Password

Shared Key / Users Session

Login Window Smart Card

Also: WS-Trust

Registration / Device Trust

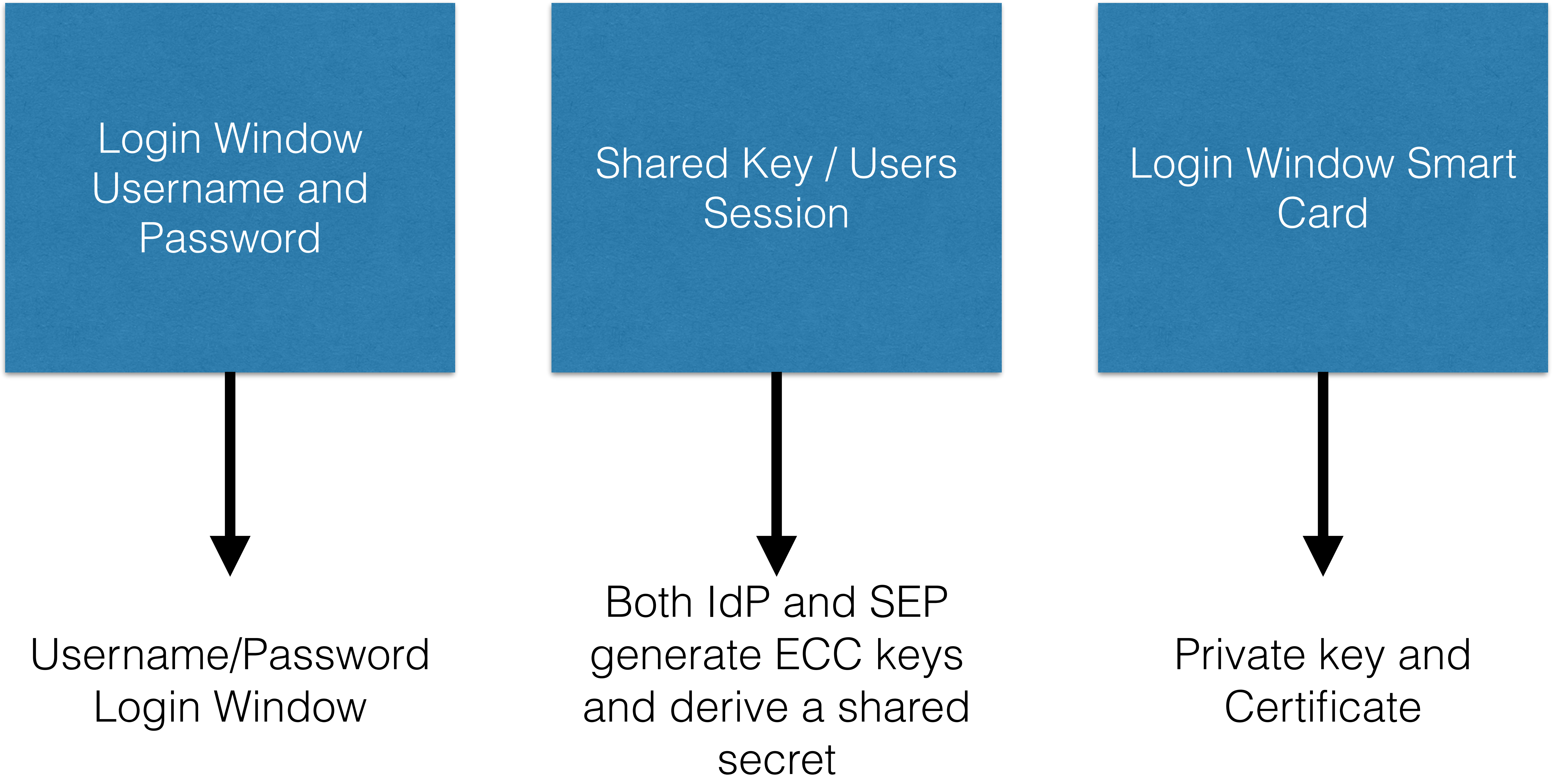


Registration Required
Use your identity provider password to log in to your Mac.

Device Trust

- ECC keys created in the secure enclave, public key shared with IdP during registration
- IdP advertises its public key at endpoint on IdP
- keys used to sign and encrypt tokens between Mac and Identity Provider

PSSO User Authentication



Login Window Username and Password

Username/Password Login Window

Shared Key / Users Session

Both IdP and SEP generate ECC keys and derive a shared secret

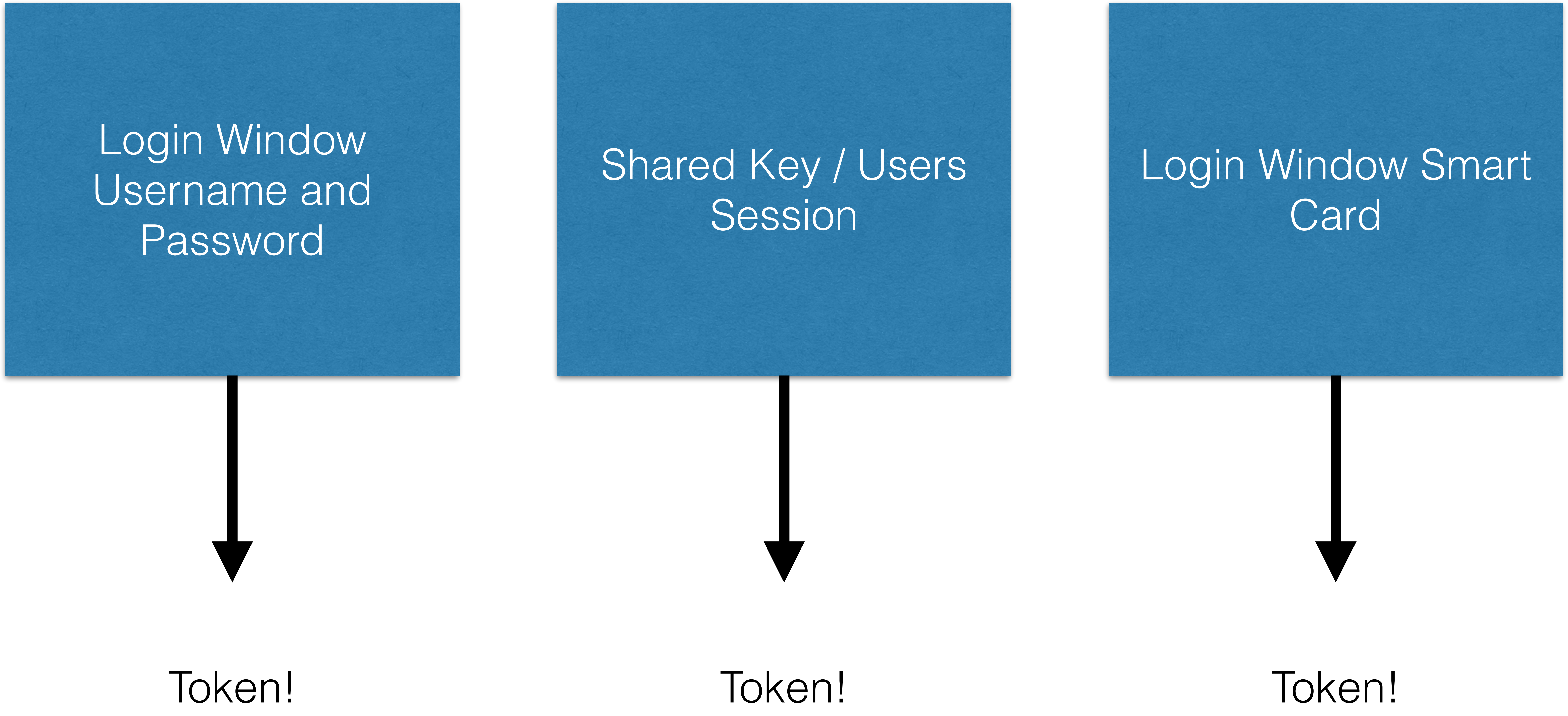
Login Window Smart Card

Private key and Certificate

Token!

- End result of all flows is a token assertion from IdP inside a refresh token
- assertion can be any info that IdP provides that is presented later for authentication
- refresh token available to SSOE to be used in when authenticating
- PSSO uses refresh token to get another refresh token about every 4 hours

PSSO User Authentication



Login Window Username and Password

Shared Key / Users Session

Login Window Smart Card

Token!

Token!

Token!

OIDC Tokens? SAML Token?

- PSSO and eSSO is IdP agnostic, but requires IdP opt-in

- SSOE is 3rd party developer code that decides how to authenticate and what UI to show

- PSSO is apple code that requires a specific interface and cryptography on the IdP endpoints. Tokens are defined by Apple but refresh token contains opaque data that is passed to the SSOE

PSSO Username and Password Login

- User creation at the login window
- Password, Keychain and FileVault Synchronization
- Groups and Authorization

Requirements

- User must set up PSSO (no automated enrollment) after login
- IdP cannot require MFA UI at Login Window
- IdP must know about extension (and probably developed it)
- IdP must extend their endpoints to support PSSO
- IdP must be able to authenticate user with refresh token to provide application tokens for eSSO.
- User is prompted for prior password if not provided during login
- All users are prompted to register

Finder
File
Edit
View
Go
Window
Help
Wed Apr 24 8:40 PM
APR
24
tv

New At WWDC 2024

- Unlock FileVault
- Login policies can now require IdP authentication across FileVault, login window, and lock screen
  - AttemptAuthentication
  - RequireAuthentication
- HPKE

More Info

- SSO Page:
  https://twocanoes.com/sso

- Try it out!
  https://github.com/twocanoes/sso

- Build Your Own:
  https://github.com/twocanoes/psso-server-go

Questions?