AUTOMATA

Technology Services

Setup and Restore - macOS

macOS Recovery and Safe Mode
Erase Assistant and Disk Utility
Migration Assistant
Keychain Access & Passwords App

Introduction to macOS Recovery

Practical Exercise

macOS Recovery

- Pre-boot environment when the Mac cannot boot using the hard disk's system folder or to make changes before the system loads.

Using Safe Mode

Practical Exercise

Startup Security for Mac

Practical Exercise

Using Erase Assistant

Practical Exercise

Using Disk Utility to Erase a Mac

Practical Exercise

Revive or Restore a Mac Using Apple Configurator

Practical Exercise

Revive & Restore

- While it doesn't happen often, a Mac's firmware can be corrupted due to a failed OS install/upgrade or for other reasons.
- In this case you have to use Apple Configurator to 'revive' the Mac, which updates/re-installs the firmware and a copy of macOS Recovery.
- When you revive a Mac, the users's data volume is not touched so data may be recoverable.
- Note: this is only applicable on Apple Silicon based Macs, this does not apply to older Intel based Macs.

Revive & Restore

Using Migration Assistant with a new Mac

Practical Exercise

Managing Login Passwords

Practical Exercise

Hiding a User Account on Mac

Practical Exercise

Keychain Access Utility

Practical Exercise

iCloud Keychain

Practical Exercise

Passwords App

Practical Exercise

Digital Certificates

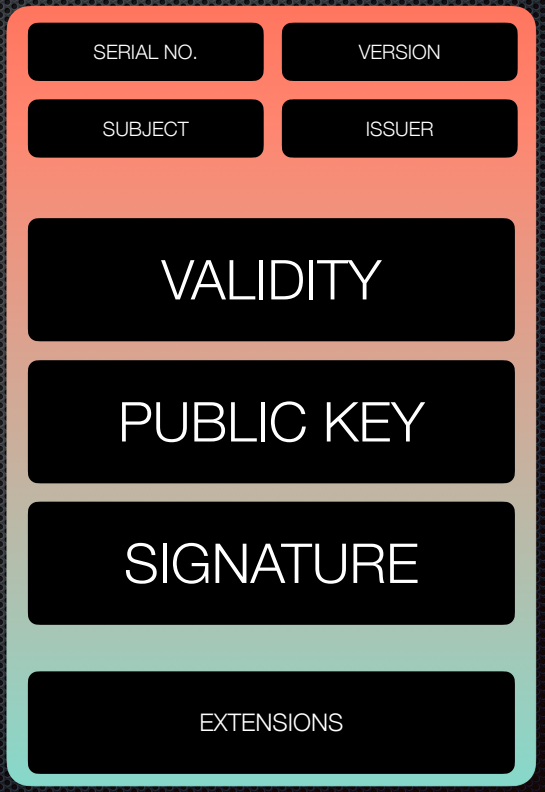
Lecture

Purpose

- Purpose
- Used to establish trust between two sources for the secure exchange of data.
- Encrypt network communications.
- Authenticate users to networks and services without the need for usernames/passwords.

Structure

- Structure
  - Public Key
  - User Information
  - Certificate Authority Information



Anatomy of a Certificate

Certificate and Identity Formats

- A certificate and it's associated private key are known as an identity.
- Certificates can be freely distributed but private keys need to be kept secure. The public key must have a matching private key to decrypt.
- The private key is stored as a PKCS #12 - .p12 file.
- Apple supports .cer, .crt, .der, X.509 with RSA keys for certificate formats. They support .pfx and .p12 as identity formats.

Trusting & Verifying Certificates

- A certificate is usually signed (verified) by a Certificate Authority.
- To evaluate a certificate's chain of trust, a device verifies the signature of the certificate and the root authority (anchor).
- Apple devices include a number of pre-installed root certificates called Trust Stores.

Trust Stores

- Categories
  - Trusted certificates
  - Always Ask certificates
  - Blocked certificates
- MDMs provide the ability for organizations to distribute certificates and establish the cert as a root that it trusts.
- MDMs also allow for a payload to automatically not accept untrusted certificates.

Considerations for Managed Macs

Lecture

Managed Setup Assistant

- Similar to iOS, Managed Macs that use Automated Device Enrollment can be configured to skip some steps and have profiles deployed to manage settings like Location Services or Software Update.
- Like iOS, Macs can also be made to update to a minimum macOS version via MDM during Setup Assistant.
- Managed Macs can have a hidden local Administrator account created automatically during Setup Assistant.
  - Can also be configured for the user to create a Standard account via Setup Assistant.