BEN GOODSTEIN
SENIOR SYSTEMS ADMINISTRATOR, NSMS
IT SERVICES @FUZZYLOGIQ

# SIGNING MACOS INSTALLERS AND APPLICATIONS

# WHAT IS SIGNING?

- All about *trust*
- Used to confirm *developer identity* and *integrity* of software
- Certificate-based
- Encrypted hashes
- Sign with private key, verify with public key

# TYPES OF SIGNING ON MACOS

- Application signing (`codesign`)
  - "seal" - encrypted hash of hashes
  - "requirements" - that must be met
- Installer signing (`productsign`)
  - simple encrypted hash of the pkg

# WHY SIGN?

- Gatekeeper (and other OS systems)
- Manual inspection
  - Command line
  - Suspicious Package
- AutoPkg
  - CodeSignatureVerifier processor

# CODE SIGNING

- `codesign` tool
  - for signing `--sign DEVELOPER_ID (--keychain KEYCHAIN)`
  - for displaying `--display --requirements - --verbose=2`
  - for verifying `--verify --deep --strict --verbose=2`

# CODE SIGNING DEMO

TEXT

## INSTALLER SIGNING

- `productsign` to sign
  - `productsign --sign INPUT_PKG OUTPUT_PKG (--keychain KEYCHAIN)`
- `pkgutil` to verify
  - `pkgutil --check-signature PKG_TO_CHECK`

# INSTALLER SIGNING DEMO

TEXT

# USEFUL LINKS

- Apple's full code signing documentation: https://developer.apple.com/library/content/documentation/Security/Conceptual/CodeSigningGuide/Introduction/Introduction.html
- Marko Jung's talk on certificates at MacSysAdmin 2016: https://github.com/mjung/publications/tree/master/2016-10-06_MacSysadmin_Certificates
- Hannes Juutilainen on code signing: https://speakerdeck.com/hjuutilainen/code-signing-and-macos-security-macaduk-2017