

# Detect Suspicious Access to Private Key Files and Export Attempts Across Platforms, Detection Strategy DET0549

Archived: 2026-04-05 16:45:32 UTC

## AN1516

A process (non-system or user-initiated) accesses private key files in user profile paths or system certificate stores followed by potential network connections or compression activity.

### Log Sources

### Mutable Elements

| Field             | Description   |
|-------------------|---|
| FilePathRegex     | Regex for matching key file extensions (.pem, .pfx, .ppk, etc.) or known certificate directories like C:\Users\*\ssh\ |
| ParentProcessName | Set of known benign certificate management tools to exclude (e.g., certutil.exe, ssh.exe)                             |

## AN1517

User or script-based access to ~/.ssh or other directories containing private keys followed by unusual shell activity or network connections.

### Log Sources

### Mutable Elements

| Field            | Description  |
|------------------|--|
| FilePathRegex    | Directory/file path regex for ~/.ssh, *.pem, *.key, *.p12                        |
| CommandLineMatch | Script or user agent seen accessing keys (e.g., cat ~/.ssh/id_rsa, tar ~/.gnupg) |

## AN1518

Access to user private key directories (e.g., /Users/\*/.ssh) via Terminal, scripting engines, or non-default processes.

### Log Sources

| Data Component                            | Name             | Channel  |
|---|------------------|--|
| <a href="#">File Access (DC0055)</a>      | macos:unifiedlog | open/read access to private key files (id_rsa, *.pem, *.p12)     |
| <a href="#">Process Creation (DC0032)</a> | macos:unifiedlog | launch of bash/zsh/python/osascript targeting key file locations |

**Mutable Elements**

| Field          | Description  |
|----------------|--|
| ProcessName    | Processes reading key files (osascript, python, bash, etc.)              |
| FileAccessPath | Private key and certificate paths like /Users/*/ssh, /Library/Keychains/ |

**AN1519**

CLI-based export of private key material (e.g., 'crypto pki export') with anomalous user session or AAA role escalation.

**Log Sources**

**Mutable Elements**

| Field           | Description   |
|-----------------|---|
| CLICommandMatch | Regex for export commands (e.g., crypto pki export, export ssh-key)   |
| AAAUserContext  | Source username or role performing export — may tune for known admins |

---

Source: <https://attack.mitre.org/detectionstrategies/DET0549#AN1519>