SC.L2-3.13.10

System & Communications Protection

Key Management

"Establish and manage cryptographic keys for cryptography employed in organizational systems."

Objectives

[a]

Cryptographic keys are established whenever cryptography is employed.

[b]

Cryptographic keys are managed whenever cryptography is employed.

Key Discussion Points

Establish AND Manage:
[a] is key creation and coordination; [b] is lifecycle protection — storage, distribution, rotation, revocation, and destruction. Both must be addressed.

Inventory Required:
Keys must be associated with the systems they protect — a key inventory allows assessors to verify what is protected and whether keys are properly managed.

Lifecycle Coverage:
Key management spans the full lifecycle — from secure generation through storage and use to destruction. Gaps at any lifecycle stage undermine the control.

Manual or Automated:
Small key sets can be managed manually with documented procedures — as the number of keys grows, automated key management systems become necessary.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing cryptographic key establishment and management; system security plan; system design documentation; cryptographic mechanisms; system configuration settings; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel with responsibilities for cryptographic key establishment and management.

TEST

Mechanisms supporting or implementing cryptographic key establishment and management.

SC.L2-3.13.10

SYSTEM & COMMS PROTECTION — Key Management

Plain English

What this control is really saying:

Good encryption with bad key management is still vulnerable. If private keys are stored in plaintext on a shared drive, backed up without protection, or never rotated, the encryption they protect is only as strong as those keys. This control requires a systematic process for how keys are created, stored, protected, distributed, rotated, and destroyed.

How it is used:

- Full-disk encryption keys are generated using the OS built-in encryption tool — each key is associated with a specific device and stored in a restricted inventory accessible only to IT admins.
- VPN and TLS certificates are issued with defined validity periods — expiration is tracked and certificates are renewed before they expire.
- Private keys are protected with a passphrase and stored in a key management system — never in plaintext on shared drives or emailed to users.
- A key management policy documents generation, storage, access, rotation, and destruction procedures — the policy is reviewed annually and referenced in the SSP.

Real World Example

The Scenario

Acme Defense uses full-disk encryption on all CUI laptops. The recovery keys were generated during setup and saved in a spreadsheet on the file server. The spreadsheet is accessible to all company employees with no access restriction.

What the assessor finds

An assessor reviews the spreadsheet and finds it contains recovery keys for all 23 laptops, unprotected. Any employee can access or copy any recovery key. Two former employees' accounts still have access to the file server — and therefore to all laptop recovery keys.

SPRS Score Impact

3.13.10 carries a point value of 1. Weak key management undermines the entire cryptographic posture — encryption is only as strong as the protection of the keys it depends on.

What Good Looks Like

Key management policy documented, keys generated using approved methods, private keys protected with passphrase and stored securely, key inventory maintained, certificates tracked and renewed before expiration, key destruction documented at system decommission.

Common Gaps

What assessors actually find in the field:

✗ **No key management process**

Encryption is in use but there is no documented process for how keys are generated, stored, or rotated — key management is ad hoc.

✗ **Private keys stored insecurely**

Private keys are stored as plaintext files on shared network drives — any user with file access can copy or use the key.

✗ **Keys never rotated or expired**

Certificates and encryption keys were created years ago with no expiration — there is no lifecycle management process.

✗ **No key inventory**

Keys exist but nobody knows what they protect — there is no inventory mapping keys to the systems and data they secure.

✗ **Key destruction not documented**

When systems are decommissioned, key destruction is not performed — obsolete keys remain accessible and potentially usable.