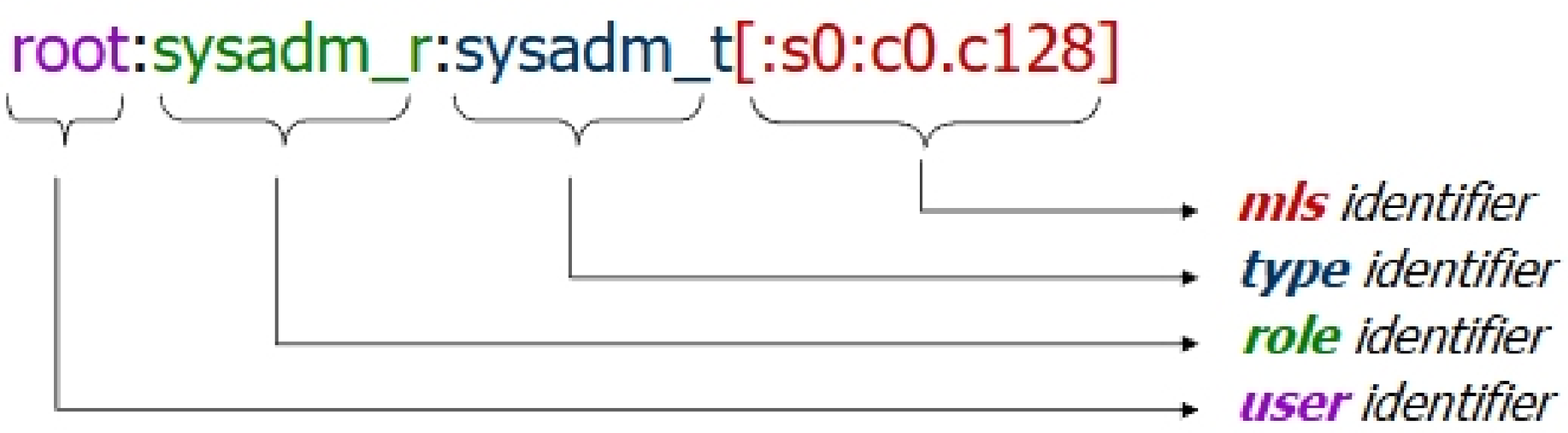
SELinux Policy Concepts and Overview

Security Policy Development Primer for Security Enhanced Linux

(Module 3)

Access Control Attributes

- SELinux assigns subject and objects a security context:



- Security context is only access control attribute in SELinux
- Security Identifier (SID): number represents security context active within the kernel

Standard Linux vs SELinux

- Subject (Process) Access Control Attributes
  - Linux: real and effective user and group IDs
  - SELinux: security context (user:role:type)
  - ➔ Linux UIDs and SELinux UID are independent
- Objects Access Control Attributes
  - Linux: (files) access modes (rwx r-x r-x) and user and group IDs
  - SELinux: security context (user:role:type)