NewEra Multi-Factor Edit (MFE)

- An example of a practical ZTA implementation step
- ZTA says access rules must be as granular as possible
- Traditional PERMITs at dataset level
  - No member-level granularity in RACF
  - PARMLIBs and PROCLIBs – all or nothing access
- MFE provides member and UNIX file “categories”
- Restricts categories of a configuration to specific USERIDs
- Enhanced access control by category
  - MFA, one-time-use tokens, etc.

Integrity Controls Environment (ICE)

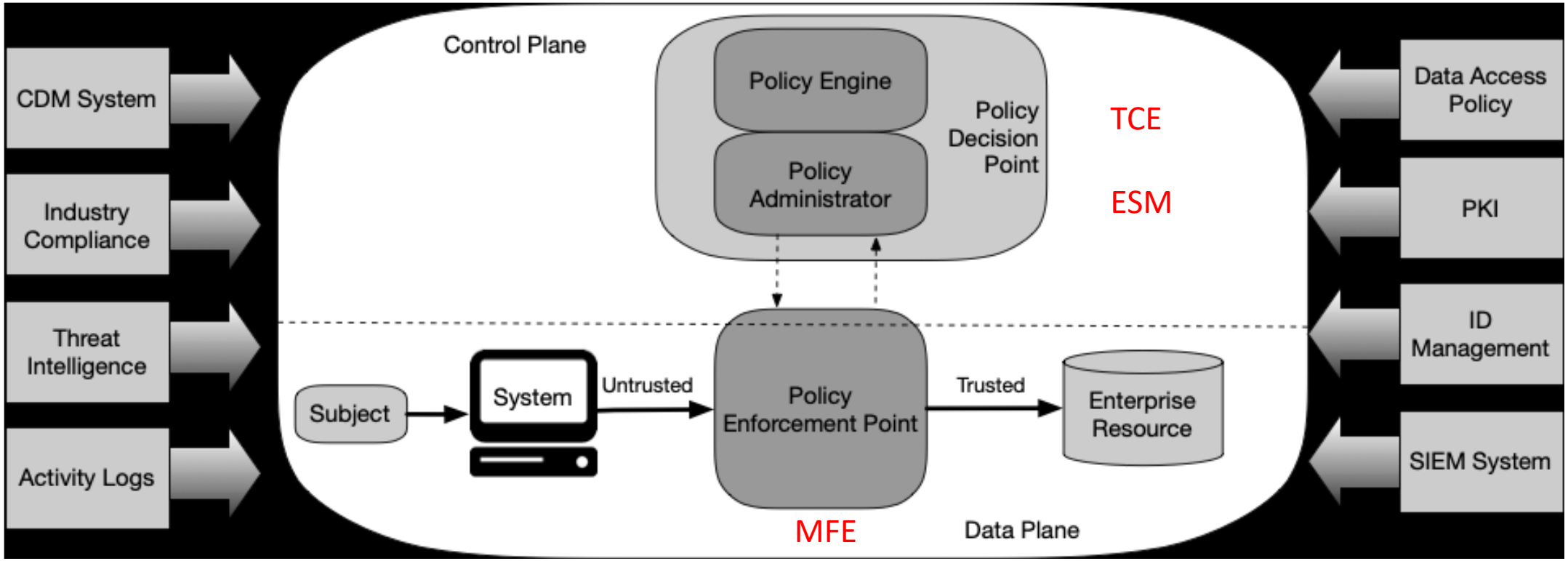
A New Tool to Enhance z/OS Configuration Security by helping you create a ZTA!

Multi-Factor Edit (MFE) is an extension of the available ICE control structures that surround a TCE Category. In practice it requires that a category be defined as an MFE Controlled Profile. Once a Profile is defined all access to its Datasets, Files and/or Load Libraries will be Denied/Warned unless/until users are specifically permitted access to the Profile.

Permitted users attempting access will receive, or their designate will receive, a One-Time Pass Ticket by Email/SMS. This event specific OTP must be entered by the requesting user in order to continue along the access/update path. All actions taken by the user while in a TCE Controlled TSO/ISPF Edit Space immediately invoke TCE Descriptor and Journaling.

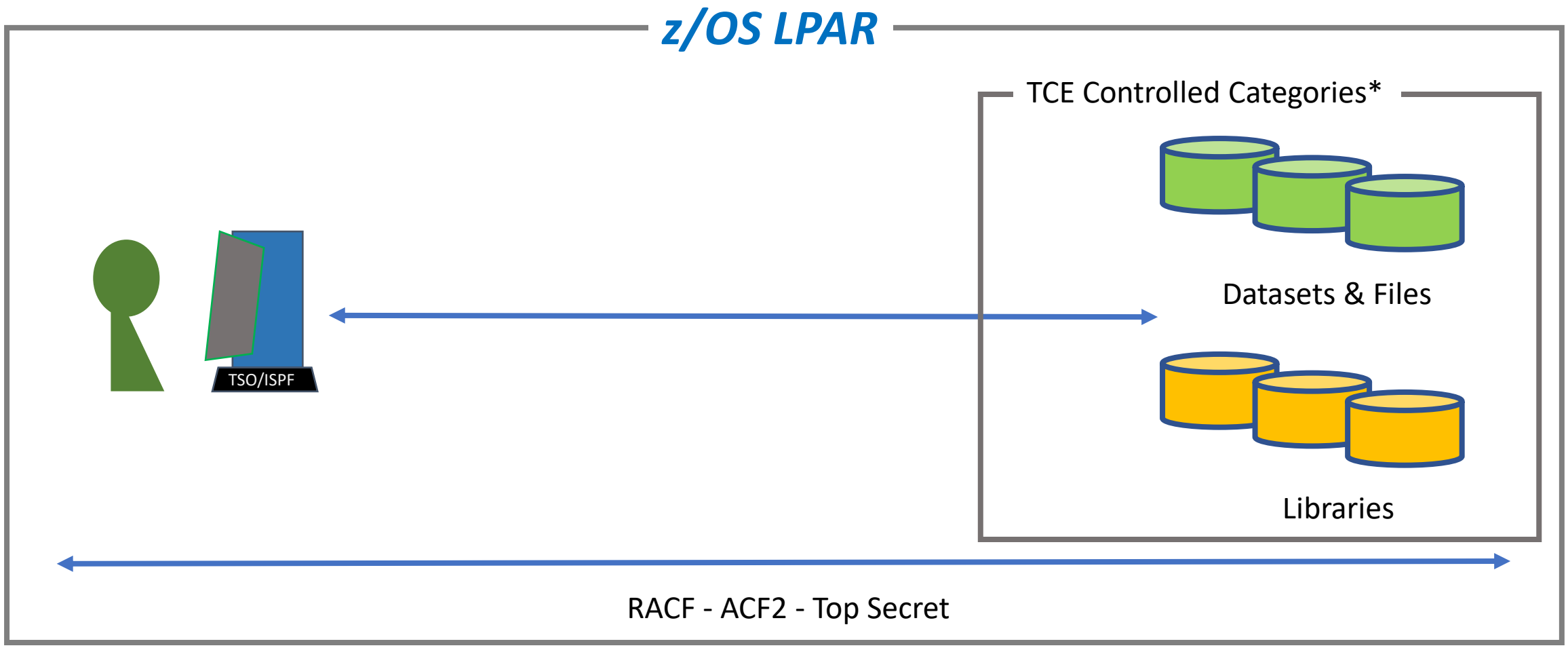
In this introductory webcast, we will describe how MFE uniquely ensures full transparency and full disclosure of resource access/update to events and, in doing so, enhances/supplements the security boundaries you already have in place as provided by either or all of the External Security Managers. No changes to existing, in place security controls are required as MFE is an enhancement to and not a replacement that fully supports the security provided by RACF, ACF2 or Top Secret.

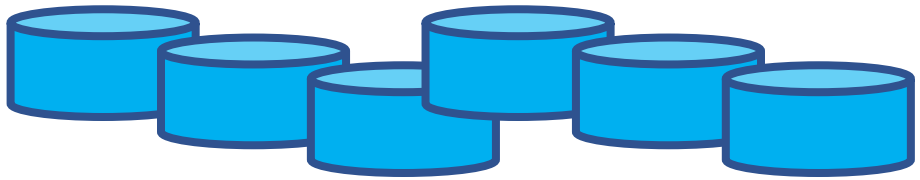
Logical Components of ZTA



Source: NIST SP 800-207

Multi-Factor Edit (MFE) – Edit & Fully Control



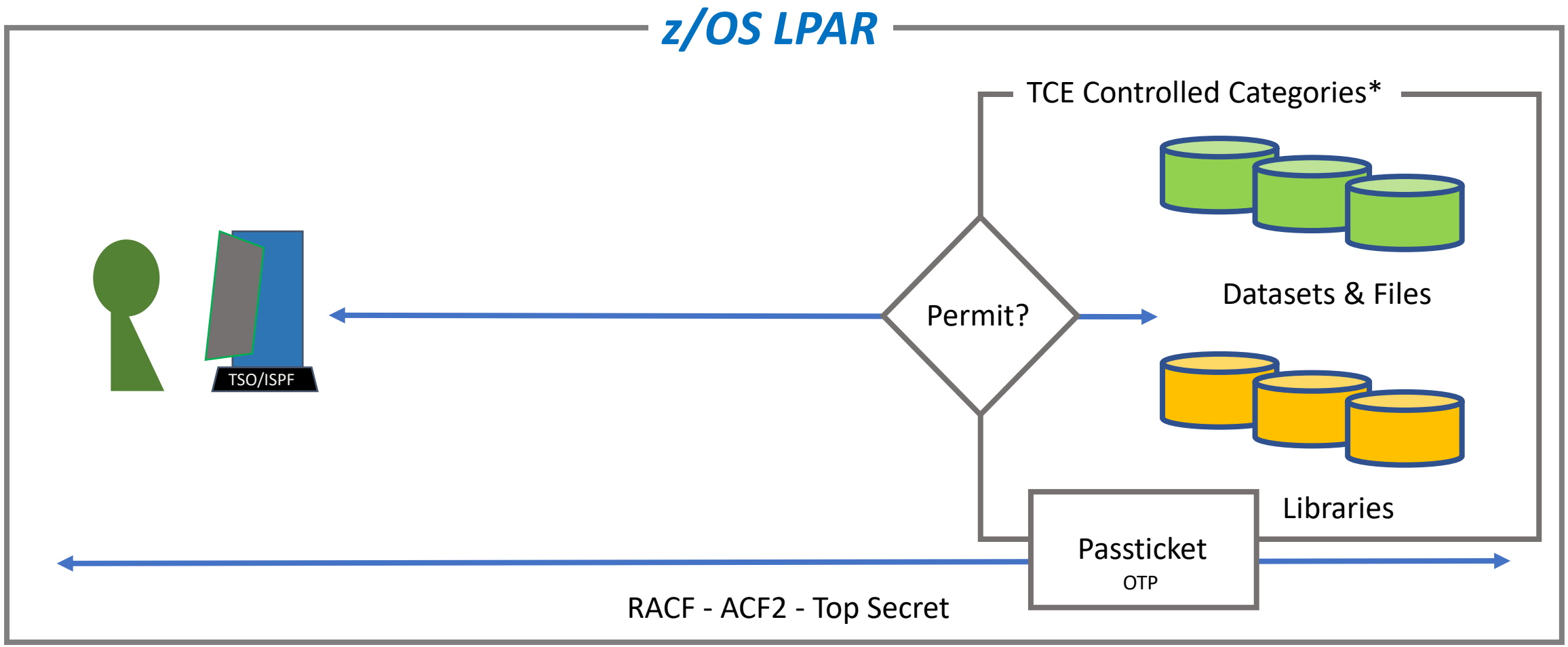


Controlled Categories and Journals

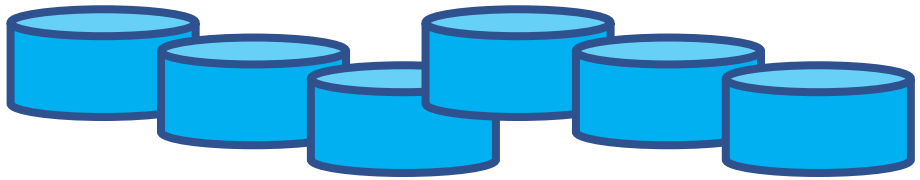
*NIST - Dependency Mapping
SP 800-207 August 2020

NIST 800-53 AC AU CM IR

Multi-Factor Edit (MFE) – Edit & Fully Control



* Excessive access checking - The core part of protecting z/OS from malicious, hurtful activities. (ZTA)

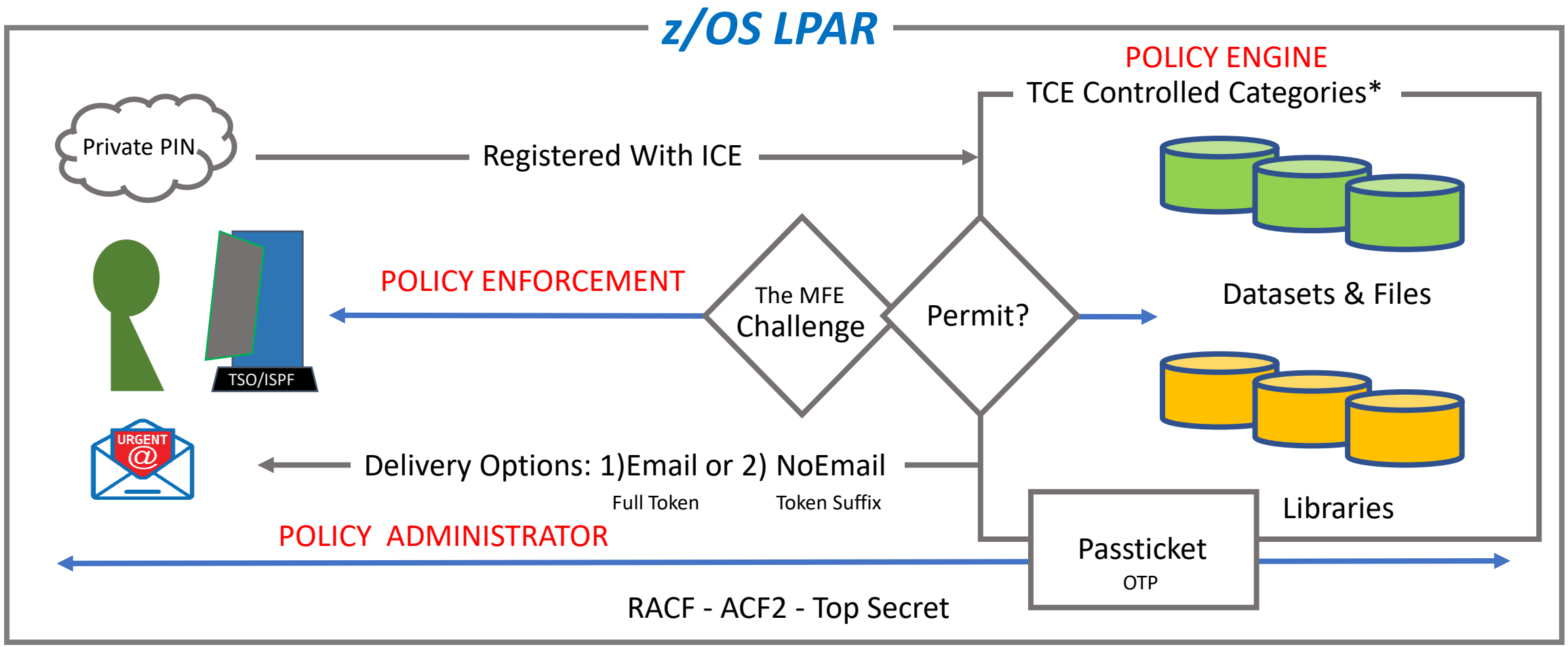


Controlled Categories and Journals

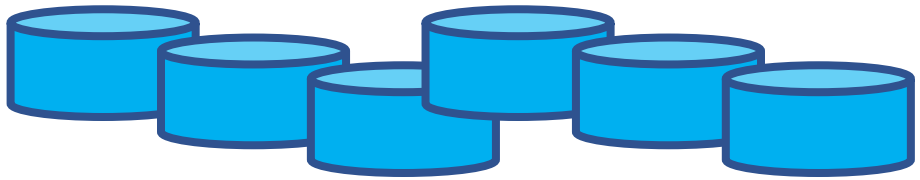
*NIST - Dependency Mapping
SP 800-207 August 2020

NIST 800-53 AC AU CM IR

Multi-Factor Edit (MFE) – Edit & Fully Control



* Excessive access checking - The core part of protecting z/OS from malicious, hurtful activities. (ZTA)



Controlled Categories and Journals

*NIST - Dependency Mapping
SP 800-207 August 2020

NIST 800-53 AC AU CM IR

Are there any questions or comments for

Charles Mills

Or

Glennon Bagsby

Thank You for Attending!

For more information:

Charles Mills
Charles Mills Consulting
charlesm@mcn.org

Glennon Bagsby
NewEra Software, Inc.
ghb@newera.com