The Control Editor (TCE)

allows you to meet these standards for Zero Trust on the Mainframe

NIST SP 800-207 August 2020 AC AU CM IR

To understand how TCE can help you meet the standards established by the National Institute of Standards and Technology (NIST) SP 800, we need to fully understand how NIST 800 applies to the mainframe environment.

What are Zero Trust and a Zero Trust Architecture as Defined by NIST? Formal Definitions (from NIST SP 800-207)

Zero Trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

It is very important that one of the major tenants of ZT is that these standards are to be applied when a network has been in some way compromised. Access by a person or network acting in a non-expected manner or accessing resources not necessary for that person in their job performance. Assuming it is someone who gains access who does not own the credentials or someone attempting to expand access beyond their authority.

Two Weaknesses

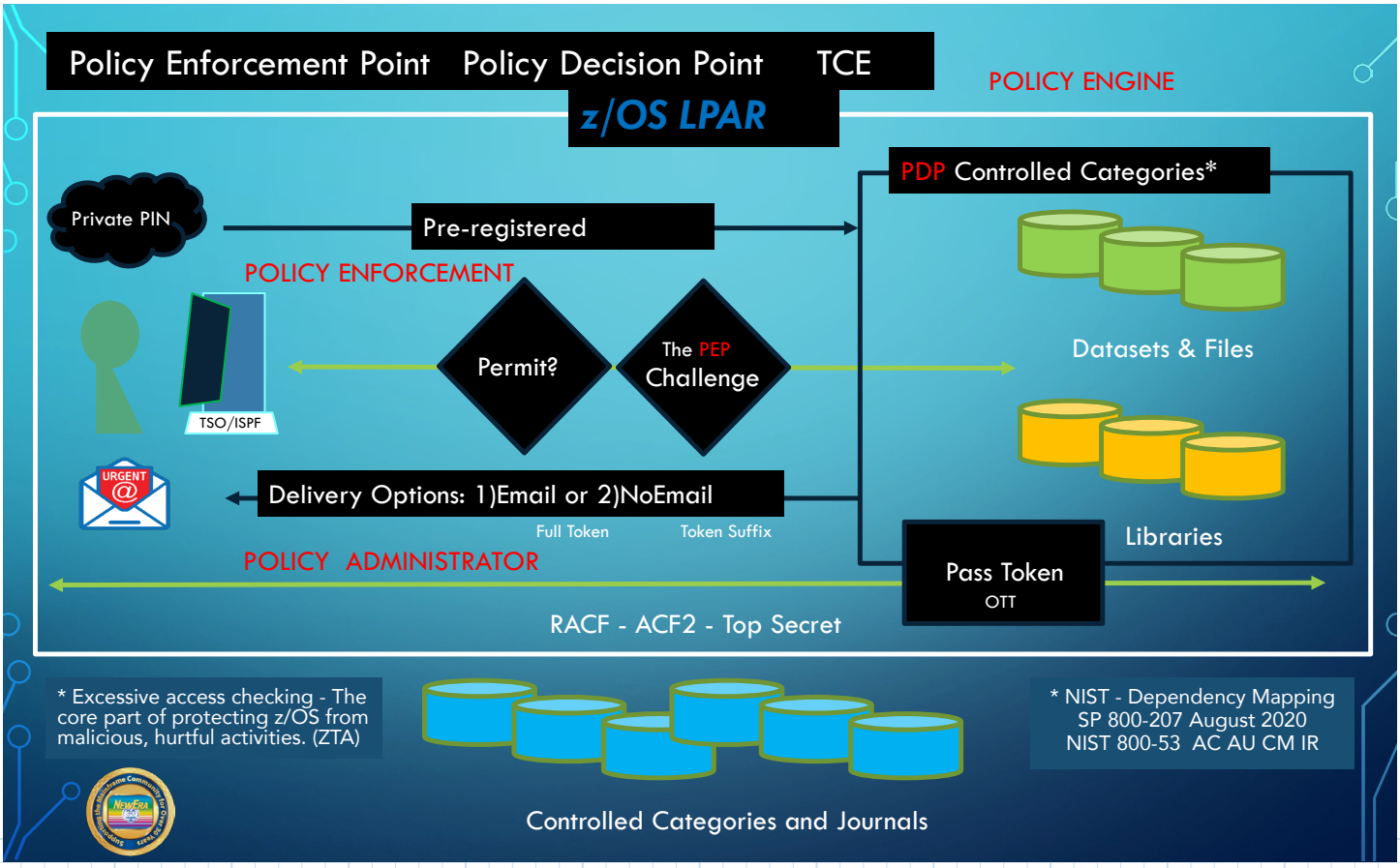
The GOAL for creating a ZTA for the mainframe is to resolve two weaknesses with the existing mainframe security environment.

1. Perimeter security is not enough.
If the focus of ZT is focused after the network has been compromised, then the perimeter security has already been bypassed and the resources are already at risk.

2. USERs are Overprivileged.
The current security environment on the mainframe very often grants access rights to users based upon groups of users and resources. There is seldom a level of granularity that can establish a clear relationship between a user and resource. ZT standards require that a relationship with a user is defined with an understanding of workflow and enforced by access policies.

The Control Editor from NewEra Software can overcome both weaknesses in a manner suggested in the standards document by creating and administrating two components of a ZTA as described NIST 800.

Access to TSO/ISPF with ZTA provided by TCE



The Logical Components of ZTA

Policy Decision Point (PDP)
An organizational entity that orders the implementation, continuous review, and the auditing of system controls.

Policy Enforcement Point (PEP)
System entities that make ZTA authorization decisions for themselves or other system entities that request such services; extending the controls of RACF, ACF2 and Top Secret – SAF

The following two components allow for the creation and enforcement of the control that exceeds those provided by the security environment today. These controls provide the functions defined in NIST 800.

Dependency Mapping
Establishing the relationship between the user and resource.

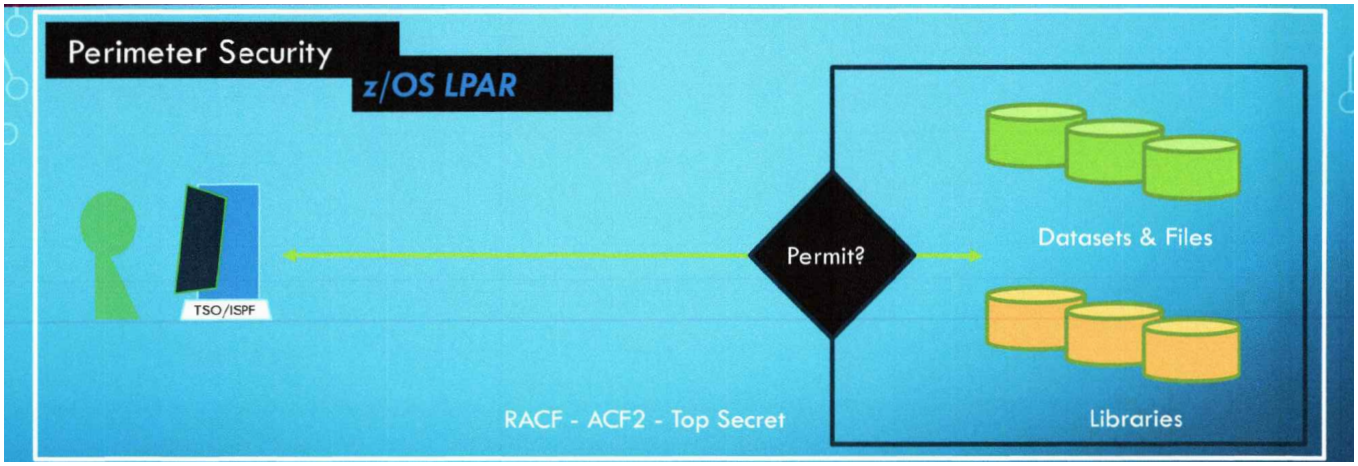
Excessive Access Checking
The core part of protecting z/OS from malicious, hurtful activities (ZTA).

TCE Added Capabilities

The list of additional controls provided by The Control Editor (TCE) that exceed or extend the capabilities of your External Security Manager that can implemented by the ZTA's PDPs and PEPs:

- Backup prior to any change
- Detected Changes
- Documentation of changes
- Notification of change via email or SMS
- BATCH changes must be supported
- Additional PASSWORD required
- Additional PASS TOKEN challenge
- ACCESS granted by type of request
- ACCESS determined at the MEMBER Level

Access to TSO/ISPF without ZTA



Access to TSO/ISPF with ZTA provided by TCE