A policy service perspective on Old and New Payroll Clerks

The authorization system is a Policy Administration Point (PAP) which recognizes the department chair in chemistry as an authority of chemistry department administration (probably by querying the Policy Information Point (PIP)). The Policy Administration Point is used to remove Gina from the role Payroll Clerk and add Marcus to that role via its interactions with the Policy Information Point (a registry of some sort). Marcus's is also given an attribute Payroll_SCOPE which indicates the set of organizations over which this role applies. Previously an access management administrator had set up policies in the Policy Enforcement Point which associated the role Payroll Clerk with the privileges READ_NON_EXEMPT and WRITE_NON_EXEMPT scoped to an attribute Payroll_SCOPE (stored in a PIP) . Because some the financial application resources associated with the payroll clerk role have embedded Policy Decision Points, the Policy Administration Point also initiates the provisioning to resource specific PDPs. These may be completely embedded in an ERP system or their maybe localized PIPs and PDPs that serve a subset of resources. For example a directory with a group indicating those in the payroll clerk role with each subject in that group having specific attributes which indicate the scope of their responsibility .

When Marcus or Gina attempts to access a payroll resource, the local policy decision point will determine the appropriate policy and grant or deny access.

See Also

XACML Terminology and Data Flow Diagram