MODAPTO [101091996]: Modular Manufacturing and Distributed Control via Interoperable Digital Twins

11.1.2 Managing service permissions and access controls

2025-08-11

Managing service permissions and access controls is a critical aspect of service registration that determines how services are discovered and who can utilize them within the MODAPTO framework.

When registering a service, users can designate whether it should be public or private:

- **Public Services**: These services are visible to all users in the main service grid view without requiring specific access rights or knowledge of service identifiers
- **Private Services**: These services are not visible in the default grid view and can only be accessed by users who know the specific service ID

This public/private distinction provides a simple but effective mechanism for controlling service visibility and access. For more complex access control requirements, the MODAPTO framework leverages additional security mechanisms at the API level.

API-Level Access Controls

Beyond the basic visibility controls in the Service Catalogue, the MODAPTO architecture implements access controls through its API Gateway component, which "controls the access to and from the internal APIs of the physical node it is installed." This component provides several security mechanisms:

1. **Authentication**: Verification of user or system identity before permitting access to services
2. **Authorization**: Determination of what actions authenticated users can perform on specific services
3. **API Rate Limiting**: Controls on how frequently services can be accessed
4. **Request Validation**: Verification that service requests meet required specifications

Managing Service Permissions

To effectively manage service permissions and access controls, service administrators should:

1. **Determine Visibility Requirements**: Assess whether the service should be publicly discoverable or restricted to specific users or systems
2. **Configure Service Visibility**: Set the service as public or private during registration based on the visibility requirements
3. **Document Access Requirements**: For private services, document and securely communicate the service ID to authorized users
4. **Implement API Security**: For services requiring additional security, work with system administrators to configure appropriate authentication and authorization rules in the API Gateway
5. **Regularly Review Access**: Periodically review service visibility settings and access patterns to ensure they remain appropriate

References

1. MODAPTO Consortium. (2023). Service Catalogue User Manual. MODAPTO Project Documentation.
2. MODAPTO Consortium. (2023). API Gateway Security Configuration Guide. MODAPTO Project Documentation.
3. OWASP. (2023). API Security Top 10. https://owasp.org/API-Security/