Classification of Authorization Use Cases addressed by XACML

Externalized Authorization Managers: Function

> *"XACML-based EAMs support a range of use cases that aren't supported by embedded authorization logic or by most WAM products:*
>
> • ***Relational authorization** supports policies including dual controls and separation of duties. An example of a relational policy is "Grant access to a medical record only if the requester is the Primary Care Physician for the patient whose record it is." This policy is called relational because the requester will have the required attribute ("Primary Care Physician") only if he (or she) is in a particular relationship with the patient.*
>
> • ***Contextual authorization** supports policies including access based on time of day, physical location, strength of authentication, and characteristics of client platform. An example of a relational policy is "Grant access only if the request origin is within the boundaries of the United States." This policy is called contextual because the requester will have the required attribute ("request origin in USA") in some contexts but not in others.*
>
> • ***Dynamic authorization** supports policies including enforcement of spending and trading limits, rate limitation, and Chinese wall policies. An example of a dynamic policy is "Grant access to file A only if the requester has never accessed file B." This policy is called dynamic because the value of the requester's attribute ("never accessed file B") can change over time.*
>
> • ***Federated authorization** supports policies that rely on partner-provided attributes and that rely on attributes from multiple sources in the same decision. An example of a federated policy is "Grant access only if the requester has been designated a purchasing officer by a registered supply-chain partner organization." This policy is federated because the required attribute ("purchasing officer") is managed by an organization different from the one that manages the policy rule. Federated authorization decisions may also involve rules that require attributes provided by more than one authoritative source; for example, "Grant access only if the requester is a U.S. citizen according to the U.S. State Department and a licensed aeronautical engineer according to the Washington State Department of Licensing."*
>
> • ***Fine-grained authorization**, including control of access to fields in a table or control of access to an operation based on parameter values. An example of a fine-grained policy is "Grant access if the requester is a teller and the transaction amount is less than $1,000, OR if the requester is a manager and the transaction amount is less than $10,000." This policy is fine-grained because it depends not only on the operation and requester attributes but also on the value of an input parameter (transaction amount)."*