

Delegation

Under the proposed procedure for delegation, a PDP MAY substitute a policy (P2) for an existing policy (P1) under the following circumstances:

1. The issuer of P2 (the delegator) qualifies as the access-subject of P1¹.
2. With the exception of their “access-subject” elements², P1 and P2 are identical.

This procedure allows one entity to grant privileges that it possesses to another entity. It doesn't address Frank's famous “airline pilot” use-case, which is to be treated as an “administrative” use-case, rather than a “delegation” use-case.

Notes

1. If P2 is supplied in the request, then the substitution MUST apply only for the evaluation of that particular request.
2. Equivalently, the PDP MAY substitute only the “access-subject” element from P2 into P1.
3. Naturally, by the standard rules for policy evaluation, the access-subject of the request (the delegate) must qualify as the access-subject of P2.

Question

How does the issuer of P2 know P1, so that he/she can satisfy condition 2, above?

Variant

Substitution should also be permissible if P2 is no more general than P1, in the sense that there are no requests that would be granted under P2, but that would be denied under P1.

This provision is useful when the delegator cannot discover P1, so cannot be certain to satisfy condition 2, above.

It is probably not practical to take two arbitrary policies (P1 and P2) and test whether P2 is no more general than P1. However, in certain special (and potentially useful) circumstances it may be practical.

Example 1

¹ An entity is said to qualify as the access-subject of a policy if it satisfies all the <SubjectMatch> criteria contained in the <Subject> element whose SubjectCategory attribute has the value urn:oasis:names:tc:xacml:1.0:subject-category:access-subject.

² The “access-subject” element is the <Subject> element whose SubjectCategory attribute has the value urn:oasis:names:tc:xacml:1.0:subject-category:access-subject.

If P2 contains `x-match(attribute-x, match-string-a)` and P1 contains `x-match(attribute-x, match-string-b)` and `x-match(match-string-a, match-string-b)` is “True”, then P2 is no more general than P1.

Note: in this example, a and b are match strings, whereas the standard requires that the first argument of a match function be an attribute value.

Example 2

If P2 contains conjunctive conditions that don’t appear in P1, then P2 is no more general than P1.

Conclusion

Tentatively, we might conclude that, under very constrained circumstances, it will be possible to verify that P2 is identical to, or no more general than P1 (with the exception of the access-subject element). This may prove useful when the delegator cannot discover P1.