ORK4 IAM Policy Design

Glossary

- **Endpoint Service:** an endpoint providing access to view, modify, append, remove, or calculate objects stored in the ORK. A service might be the Attendance or Award service.

- **Service Object:** a specific instance representing a single object produced by an Endpoint Service. Each Service Object has a single Service Object Security Requirement, which may be encoded as an ORN (below).

- **Composite Object:** an object, which may be returned by a service, which is a composition of service objects from one or more services. Examples are lists of attendance objects, or simplified output objects, such as a kingdom object and its associated list of park objects. Each object carries its own Service Requirement. *A composite object does not have a Service Requirement*. Security concerns are always at the specific Service Object level.

- **Security Requirement:** An object with a 1 to 1 relationship with a single Service Object, composed of a set of provisos that define the security context for interacting with the Service Object. The provisos of a Security Requirement are called Conditions.

- **Policy:** A set of Claims. Policies are associated with Roles. A policy determines the actions that a Role may take in the ORK.

- **Claim:** An object composed of a set of provisos that define a set of grants for the claim. A Policy is composed of one or more claims.

- **Resource:** a specific subset of a service and optionally, a specific procedure on that service. A resource might be Event/Edit on the Attendance service, or View on the Mundane service.

- **OrkResourceName (or ORN):** a formatted string that encodes a single claim for an ORK4 policy or a service requirement for an ORK4 endpoint service object. An ORN is a format, The order of the provisos is defined by **Service Object Security Requirement**. A proviso is recorded without its associated Service, since the service is identified by the Security Requirement ordering.

- **JWT:** The format of the access token returned by the ORK authorization server. The **JWT** contains the user's **policy**. Users who are not authorized have a default implicit view-only policy applied to their session. *An ORN or a policy is not self-enforcing*. Only a policy signed by a trusted **IDP** should be considered valid for granting claims by the policy.

Example:

```
Attendance:1:1:1:1:1:1:ORK/SetAttendance
```

This ORN is composed of 3 sections:

1. Endpoint service (Attendance)
2. Provisos (1:1:1:1)
3. Resource (Record/Update). May also be a glob (particularly for Security Requirements)

- **Proviso:** A pair of data composed of a Proviso Service and an identifier. The identifier may be one specific value, null (represented by the empty string) or a glob (*), which indicates "all identifiers for the service".
- **Condition:** A proviso for a Security Requirement. Must be either null or a specific identifier.
- **Grant:** A proviso for a Claim. If a grant is specified as a glob, then it matches any condition identifier during comparison.
- **Satisfaction:** A role may perform a resource action if any claim associated with the role's policy satisfies the Security Requirement of the underlying Service Object. A policy is satisfied if any Claim satisfies the Security Requirement. A claim is satisfied if any grant satisfies the Security Requirement. A grant is satisfied if any grant proviso satisfies any condition proviso. A grant/condition proviso is matched if the service of both provisos is the same and their identifiers match, or either identifier is a glob (example below).

Operation

Every Service Object has a related Security Requirement. The provisos of the Security Requirement are defined by the Service Object definition. A Security Requirement does not have an explicit set of resources defined, and the resource is expressed as a glob.

All access to the ORK occurs via Roles. Roles may be implicit. Each role has one or more policies attached to it. A policy is a list of claims, expressed as ORNs. If any of the claims satisfies a Security Requirement for a given Service Object, then that role may call the related resource and resource procedures associated with it.

Examples

Inserting an attendance record for the park Dagobah in the Principality of the Golden City is gated by the implicit security requirement:

```
Attendance::1:34:577:::ORK/AddAttendance
```

Where conditions are:

- Configuration: not set
- Game: 1 (Amtgard)
- Kingdom: 34 (The Golden City)
- Park: 577 (Dagobah)
- Event: not set
- EventInstance: not set

If a user account is the Park PM of Dagobah, they user might have the following Claim in their user policy:

`Attendance::::577:::ORK/*`

Which would **allow** on the **claim(577)** == **grant(577**) for the resource **claim(ORK/*)** >= **grant(ORK/AddAttendance)**

So in this case, because the role's Park claim is 577 and that satisfies the Park grant in the security requirement, it is allowed. A Kingdom PM might have an Attendance claim of `Attendance:::34:*:::ORK/`. Which would allow attendance resource activity on any park in the Golden City (although, technically, the * glob operator is not necessary). Similarly, you could construct a "park only" admin that could modify any park but no kingdom-level attendance as follows: `Attendance::::*:::ORK/*.` Or an admin who could enter attendance at any event instance: `Attendance:::::*:ORK/AddAttendance`

The format of of the ORN for each service endpoint is detailed in the `*Format.php` files in `src/Domain/IAM/ORN/`.

A typical local PM Policy might look like the following:

```
[
	"Attendance::::577::ORK/*",
	"Park::::577:ORK/*",
	"Mundane::::577::ORK/*",
	"Awards::::577::ORK/*",
	"Event::::577:ORK/*",
	"Officer::::577:ORK/*",
	"Unit::::577::ORK/*",
]
```

Design

Classes

Proviso

Holds a service and identifier pair.

Grant extends Proviso

A proviso for a policy claim

Condition extends Proviso

A proviso for a security requirement

Resource

The specific component or procedure of a service that is claimed in a claim

ProvisoList

An ordered list of provisos

Requirement

A gate against which claims are satisfied

Claim

A collection of grants against a specific service endpoint and resource

Policy

A collection of claims

Enums

OrkService