DESIGN SPECIFICATION

Oracle Consulting Services

IGS.Provisioning Service Model

Author:	Dieter Steding
Creation: Date:	06/29/2023
Latest Update:	07/13/2023
Control Number:	<Document Control Number>
Version:	1.0.0.0

Approval:

Document Control

Change Record

Date	Author	Version	Change Reference
06/29/23	Dieter Steding	1.0.0.0	No previous document

Reviewer

Name	Position

Distribution

Copy No.	Name	Location
1	Library Master	Project Library
2		Project Manager
3		
4		

Table of Content

Accountability

Participants accountability includes:

The participants are able to implement the dependencies of multiple IT systems necessary for account provisioning in order to obtain the extensive use of a specialist procedure. This requires the participant is familiar with the infrastructure components involved.

Ensuring that the data provided by the F-IAM are integrated in their timely correctness.

Any violation of the consistency and integrity of the data provided will inevitably result in the rejection of the user accounts affected, regardless of the interface used for delivery.

The participants are obliged to rectify errors themselves. Full support from the operational staff of the Federal Criminal Police Office is not provided.

For a participant who decides to independently control the provisioning of the user accounts through his IAM system, any rights to a further manual assignment of rights, roles or user accounts in the central F-IAM are withdrawn (view only principle; responsibility principle).

Provisioning Service Model

The Provisioning Service provides the API to trigger provisioning accounts to the target system. Therefore it is a facade on top of the core functionality Identity Manager already offers for this purpose.

The need to implement such a service arises from the distribution of the services across the participants that supply data for provisioning and the consistency and integrity of such data at the time of its delivery.

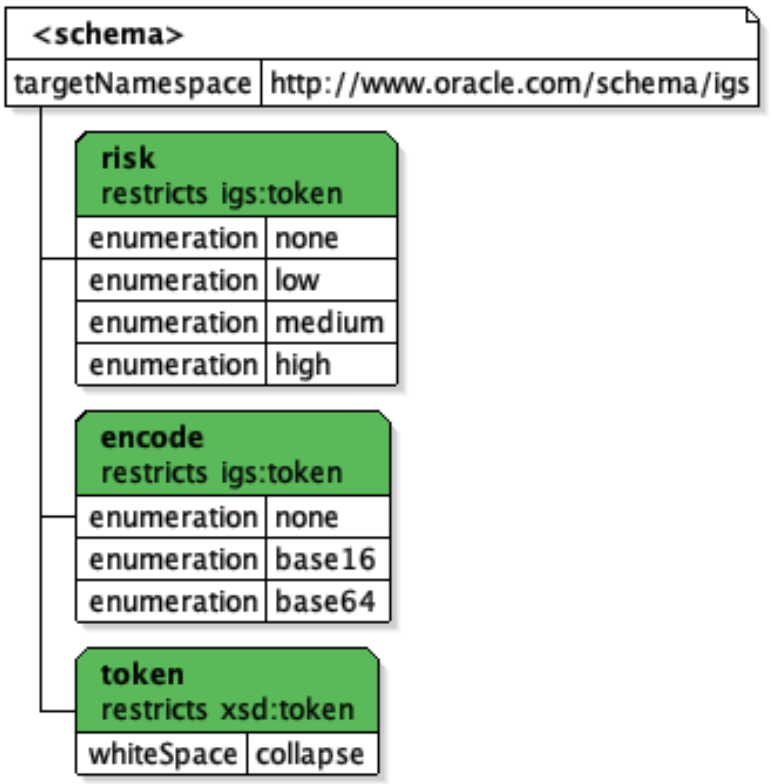
The main task of this service is therefore to protect the internal provisioning processes in Identity Manager from inconsistencies within the data delivery and to ensure the security requirements of the Federal Criminal Police Office with regard to the sensitivity of the data. At the same time, this service is responsible for communicating to the data sources provisioning orders that cannot be carried out for any reason.

Data Types

The entities declared within the schema underlying the Provisioning Service Model are based on a shared core schema.

META-INF/schema/xsd/core.xsd

This schema only defines the data types used.



Element	Description
token	A token is a simple string with all whitespaces condensed. This means that all control characters are replaced with spaces and the resulting consecutive spaces are reduced to a single space.
encode	

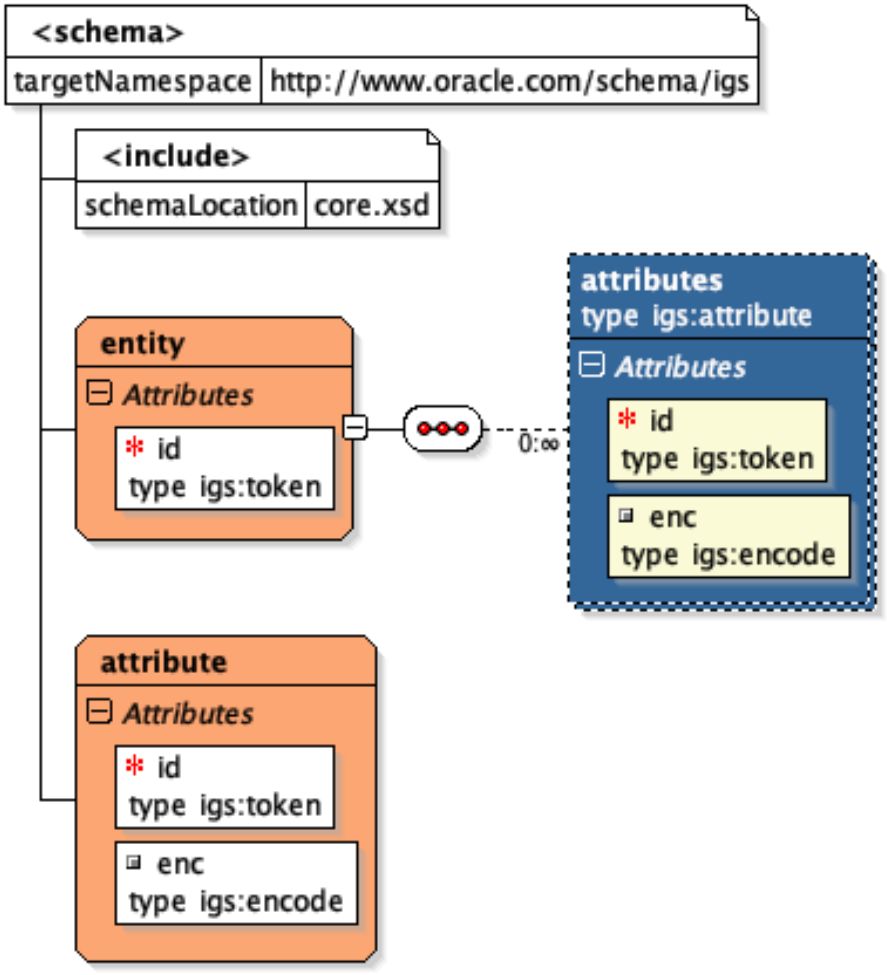
Element	Description
risk	

Core Schema

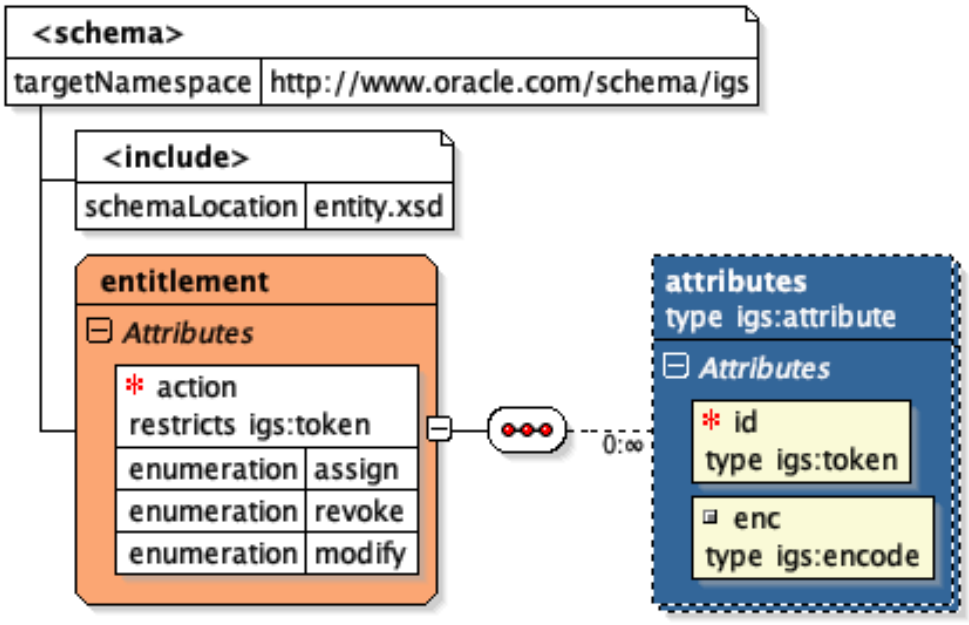
Entity

META-INF/schema/xsd/entity.xsd

This schema only defines the abstract types.



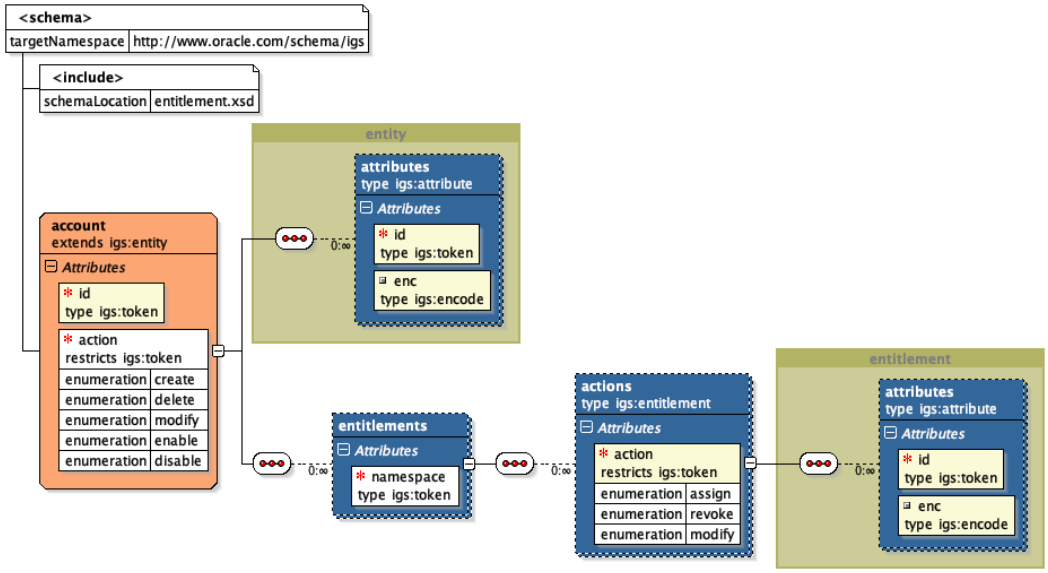
Element	Description
attribute	The complex type *attribute* represents a tagged-value pair. An attribute carries an *id* for naming purpose and encloses the value mapped at that *id*. This complex type is abstract can only exists in an enclosing element.
entity	This complex type *entity* enclose the collection of generic *attribute* definitions. The *id* attribute of this type is the public name derived from the Identity Manager configuration and intended to used for lookup any object deployed in Identity Manager by its name using the *id* as a matching criteria.



Element	Description
entitlement	The complex type *entitlement* declares the attribute *action* and enclose the collection of generic *attribute* definitions. Attribute *action* on its own is an enumeration of the activities *assign* and *revoke*. Therefore it is possible to specify the activity how to handle an *entitlement* at the time of provisioning.

Account

The schema of a user account includes the generic description of the data model of a target system in Identity Manager.

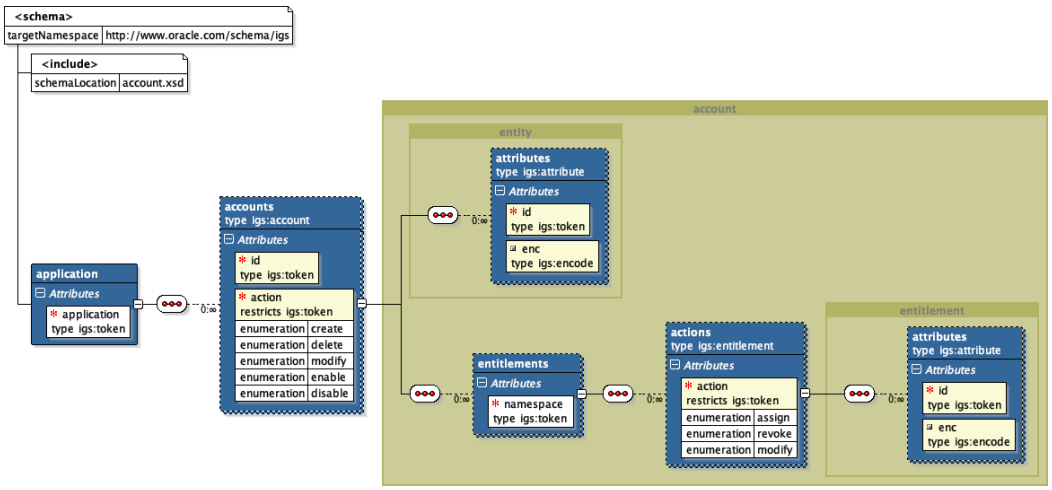


Element	Description
account	An *account* as a complex type inherits all from *entity*. The element entitlements of this type provides the collection of entitlements belonging to the account in the enclosing *application* to provision. The type *account* is extended with the attribute *action*. Attribute *action* on its own is an enumeration of the activities *create*, *delete*, *modify*, *enable* and *disable*. Therefore it is possible to specify the how to handle an *account* at the time of provisioning. An *account* enclose element *attributes* as a complex type that inherits all from *attribute* and therefore enclose the collection of generic *attribute* definitions.
entitlements	The enclosed element *entitlements* of an *account* belongs to a specific *namespace* of entitlements (OIM Child Form). The element *entitlements* is always surrounded by an element *account.*
actions	The enclosed element *actions* inherits all from *entitlement* and is extended with the attribute *action*. Attribute *action* on its own is an enumeration of the activities *assign* and *revoke*. Therefore it is possible to specify the activity how to handle an *entitlement* at the time of provisioning.

Application

The service expects a provisioning request per application systems.

Any provisioning request is base on this schema



Element	Description
application	An *application* as a complex type defines the enclosing element to describe the provisioning actions on an *account*. For that purpose it enclose an element *accounts* based on the complex type *account* that itself inherits from *entity*. The complex type *account* itself enclose the complex type *entitlements*. To be able to specify the activities how to handle the *account* embedded in an application at the time of provisioning the *account* is extended with an attribute *action*. This attribute represents the regular lifecycle activities applicable on an account and enumerates *create*, *delete*, *modify*, *enable* and *disable*. If *action* is unspecified its defaults to *create*. For naming purpose the application provides an attribute *id* that refers to the application instance name which is per definition in Identity Manager a token without any whitespace.
accounts	An *account* as a complex type inherits all from *entity*. The element entitlements of this type provides the collection of entitlements belonging to the account in the application to provision. The type *account* is extended with the attribute *action*. Attribute *action* on its own is an enumeration of the activities *assign*, *revoke*, *enable* and *disable*. Therefore it is possible to specify the activity how to handle an *account* at the time of provisioning. The complex type *entitlements* embedded in *account* inherits all from *entity* and represents the collection of *entitlement*s that belongs to a specific type of entitlement (OIM Child Form).