



Sneak Peek at Ownership Based Authorization in Ed-Fi

Ed-Fi Alliance

Hello!



Sayee Srinivasan
Solutions Architect
Ed-Fi Alliance



-  sayee.srinivasan@ed-fi.org
-  +1 512 600 3618
-  Schedule time with me.
-  Get started with Ed-Fi today!







SAVE CONTACT



Vinaya Mayya
Software Development Lead
Ed-Fi Alliance



-  vinaya.mayya@ed-fi.org
-  +1 512 600 3621
-  Schedule time with me.
-  Get started with Ed-Fi today!



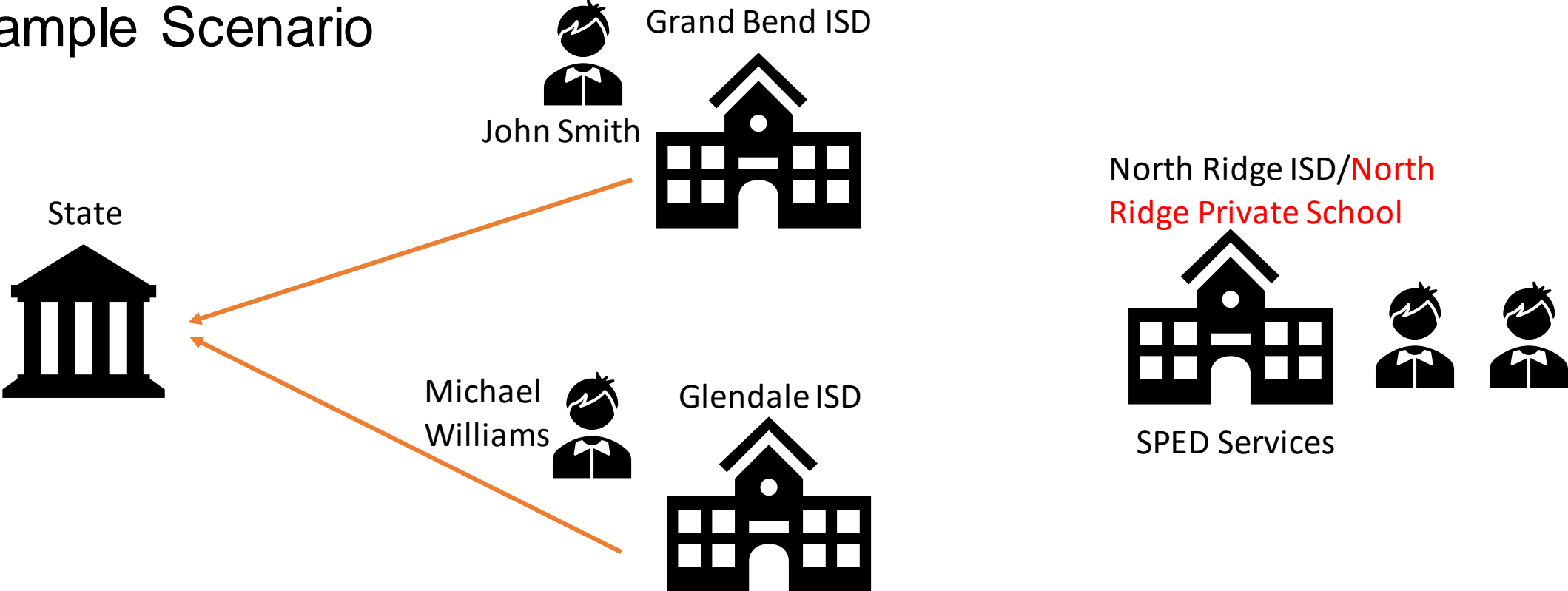
SAVE CONTACT

Use Case – Resident District Submitting Data for Private Schools

- In a state level implementation, LEAs submit data to the State for students attending their OWN district as well as for students attending any PRIVATE day schools.
 - Private day schools offer special education program services that are sometimes not offered by LEA's own schools
 - Multiple LEAs send students to the **same** private day schools.

Problem - Vendor SIS data sync from one LEA to ADE implementation of Ed-Fi ODS API (AzEDS) inadvertently deletes data submitted by another LEA SIS. This issue happens with students enrolled in private day care schools that takes in students from surrounding LEA for special education programs.

Example Scenario



Problem

	GET	POST	PUT	DELETE	Comment
Grand Bend ISD	Y	Y	Y	Y	Both Grand Bend and Glendale can read/write students data in North Ridge Private School
Glendale ISD	Y	Y	Y	Y	Both Grand Bend and Glendale can read/write students data in North Ridge Private School

Resident District Submitting Data – Authorization

- Submitting district or the resident district will have a key and secret for all schools in their district.
- The same key and secret will be associated to the private school also.
- The enrollment record will have the attending school id as the school id.
- StudentSpecialEducationProgramAssociation has the attending school id.

Enrollment Record and SPED Record

Enrollment
Record

Student	School	EntryDate	EntryGradeLevel	EntryType
John Smith (100)	North Ridge Private School (1000)	08/25/2021	9	New year school
Student	School	EntryDate	EntryGradeLevel	EntryType
Michael Williams (200)	North Ridge Private School (1000)	08/25/2021	9	New year school

SPED
Record

Student	Ed.Org	Program	BeginDate	ParticipationStatus
John Smith	North Ridge Private School	SPED	08/25/2021	Active In Program
Student	Ed.Org	Program	BeginDate	ParticipationStatus
Michael Williams	North Ridge Private School	SPED	08/25/2021	Active In Program

Scenario 2 - Vendor's Concern

- SIS receives Ed-Fi resources from the ODS that are owned by different systems/vendors when the GET is not restricted by who can read the data.
- If there are errors with the data owned by others, then the problems are:
 - It remains in the incorrect state in the ODS if it is not corrected.
 - Lots of hits to the API that are unnecessary.
 - Filling error logs with frivolous information
 - Creating confusion with the districts because they feel they send the correct data, but the data is not getting submitted.

Concern & Questions

- Data created by one LEA (or App key) can be read, updated or deleted by another LEA (or App key).
- Questions:
- How can this be prevented?

Ownership-based Authorization

- Ed-Fi ODS / API primarily uses a relationship-based authorization strategy based on education organizations.
- Additional level of authorization may be needed for some specific resources that could be shared across multiple source systems. e.g., Students/Staff/Parents.

Relationship-based



Ownership-based

Ownership-based Authorization

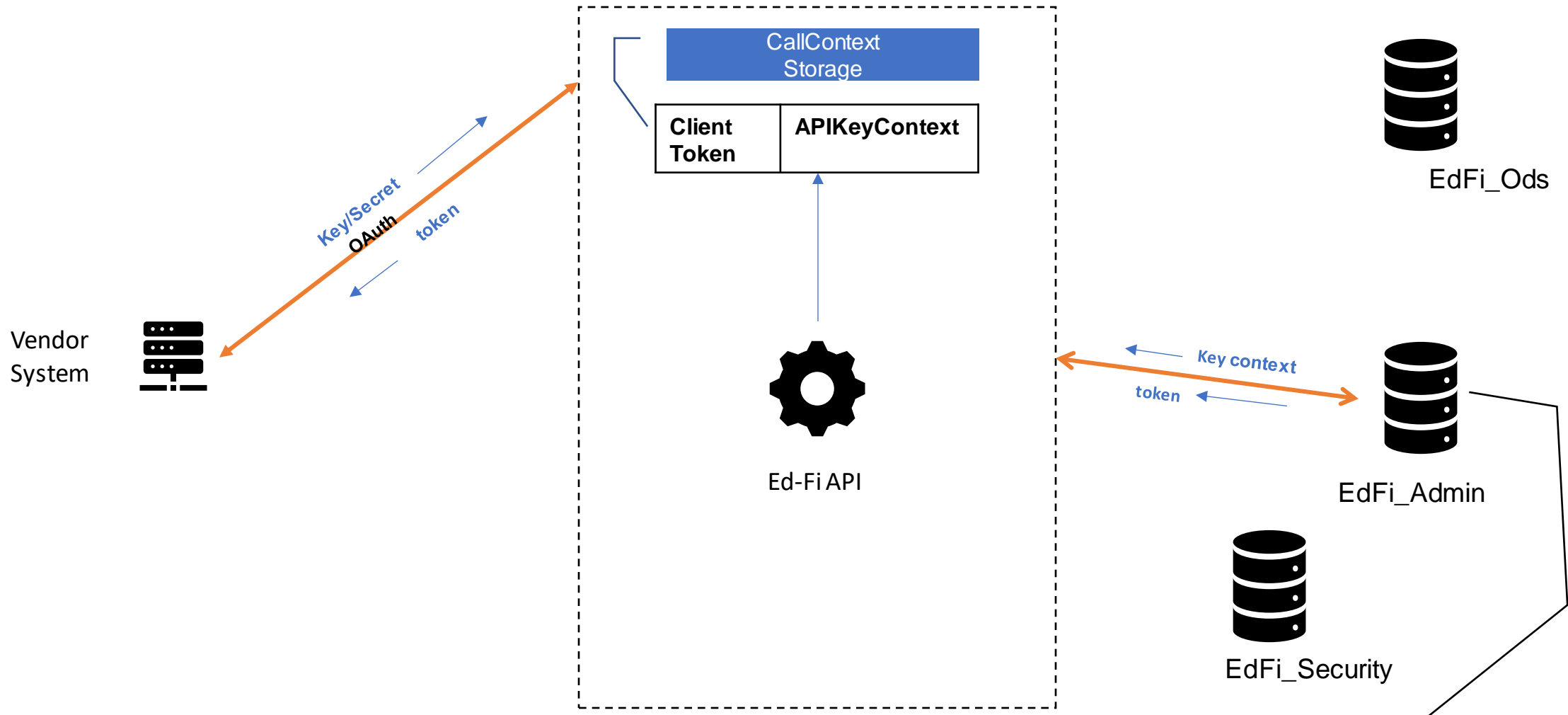
- Ownership-based authorization is a **configurable optional feature**:

```
"ApiSettings": {  
  ...  
  "Features": [  
    {  
      "Name": "OwnershipBasedAuthorization",  
      "IsEnabled": true  
    },  
    ...  
  ]  
}
```

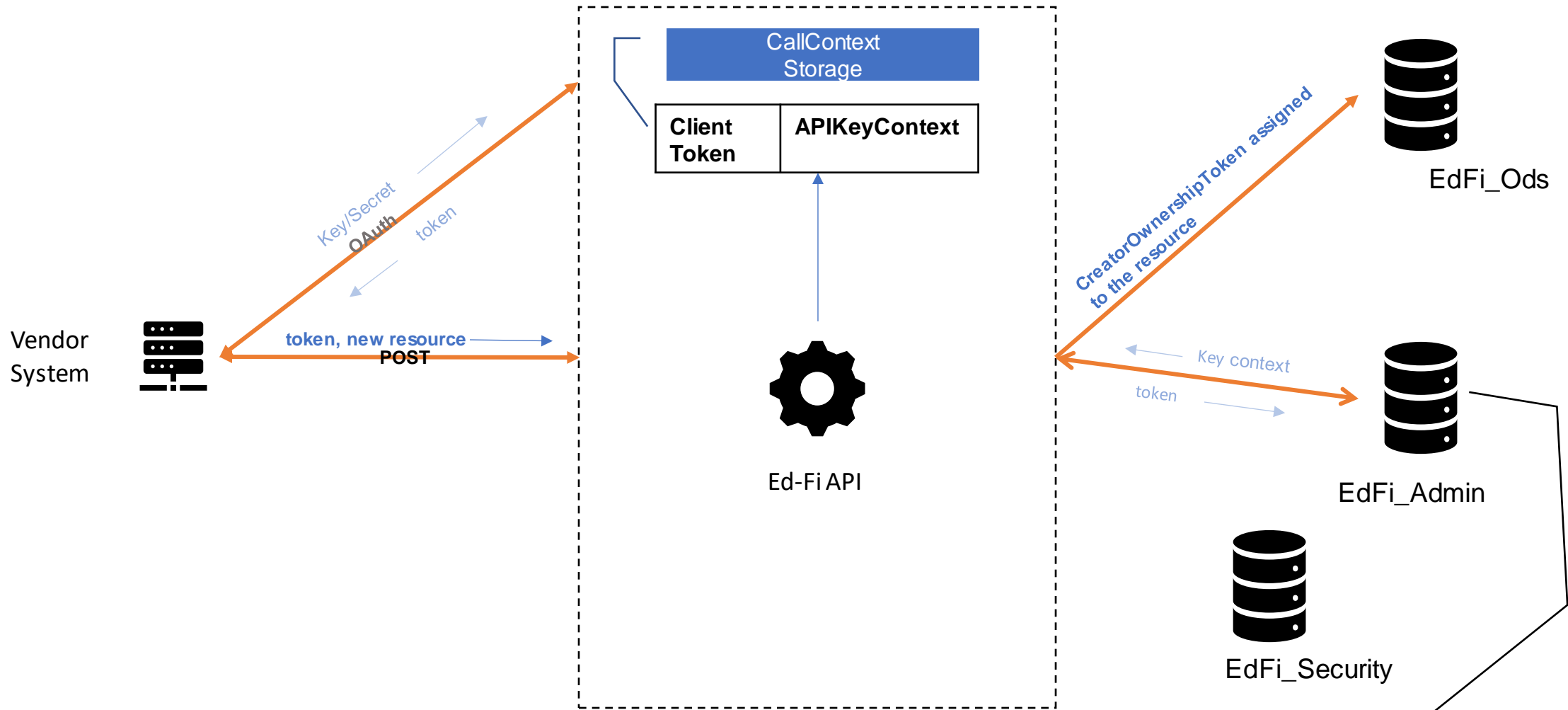
- Adds a new “Ownership-Based” Authorization Strategy to Security setup.
- Allows API hosts to configure “Ownership-Based” Authorization Strategy for any resource/action.
- API authorizes access to individual resources based on the concept of “ownership”, when configured.

Implementation

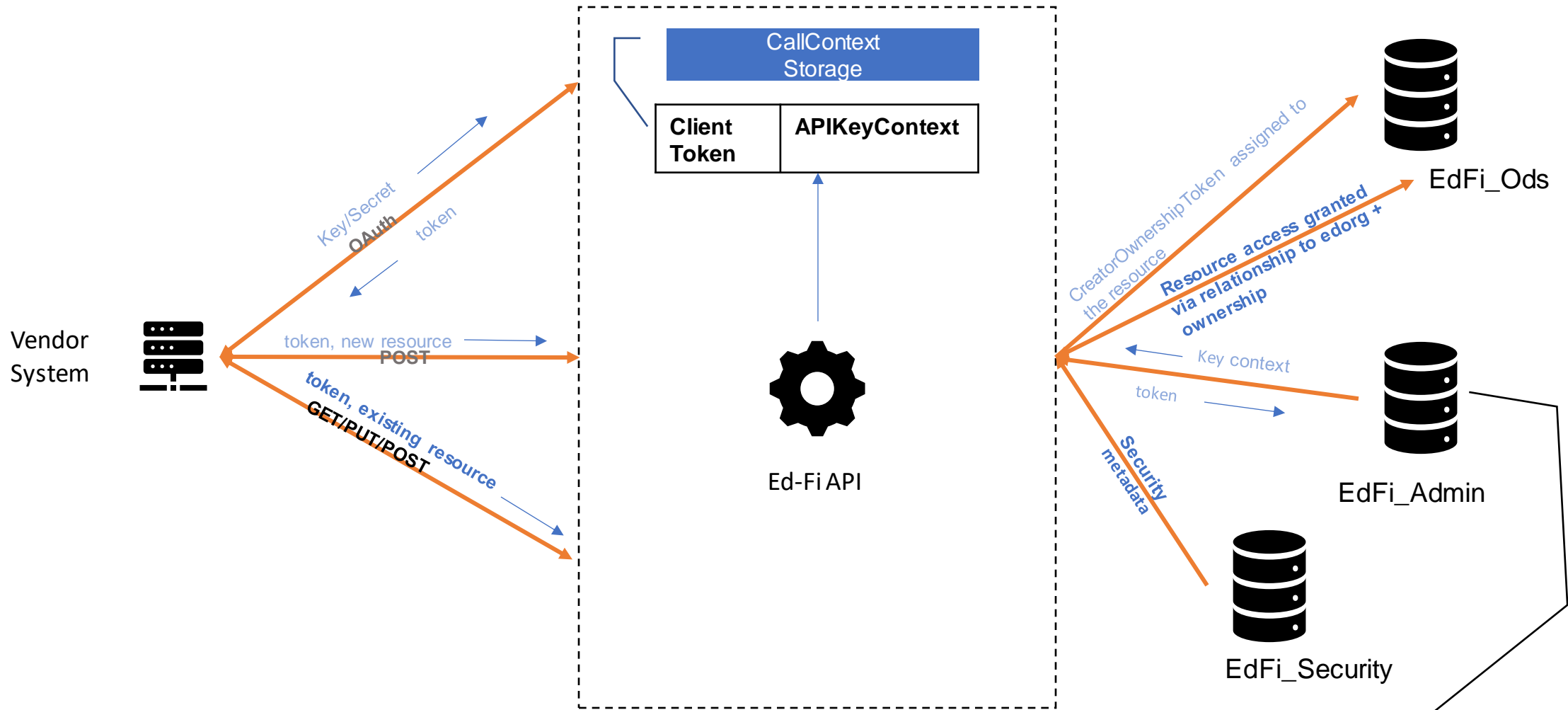
- API Clients are associated with Ownership tokens
- For each record **insert** request
 - Follows the existing authorization strategy
 - Sets the CreatedByOwnershipTokenId property of the root aggregate to the CreatorOwnershipTokenId of the API Client
- For each record **read, update or delete** request, if ownership-based authorization strategy is set for the resource/action
 - Compares the CreatedByOwnershipTokenId from the table record to the ApiClient's OwnershipTokens, If there is a match then allows the request to pass through.
 - If there is no match, then rejects the request and throw an unauthorized error.



API Client:
CreatorOwnershipToken: (for "stamping" newly created resources)
 A set of *OwnershipTokens*: (for authorizing access to existing resources)

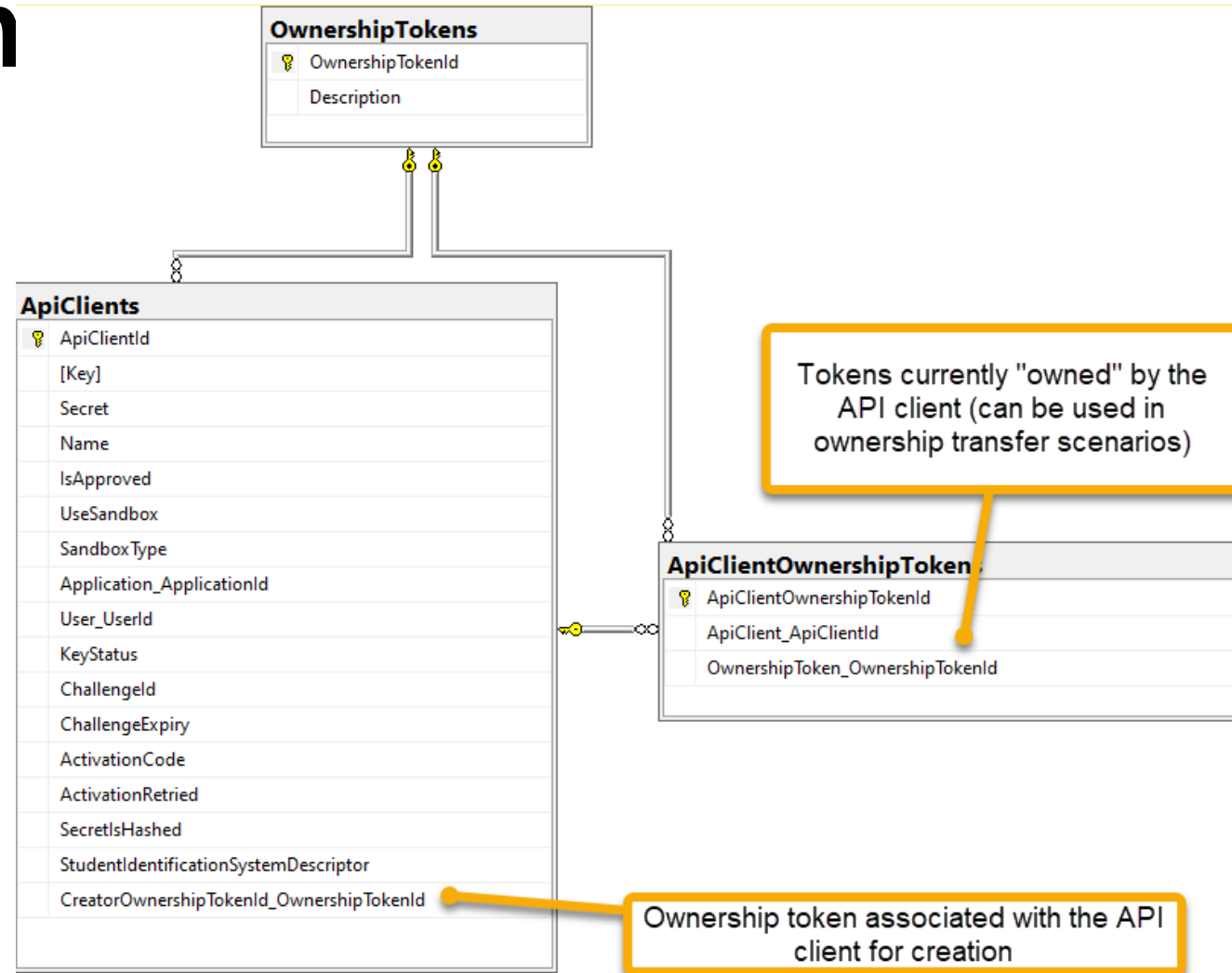


API Client:
CreatorOwnershipToken: (for "stamping" newly created resources)
 A set of *OwnershipTokens*: (for authorizing access to existing resources)



API Client:
CreatorOwnershipToken: (for "stamping" newly created resources)
 A set of *OwnershipTokens*: (for authorizing access to existing resources)

EdFi_Admin



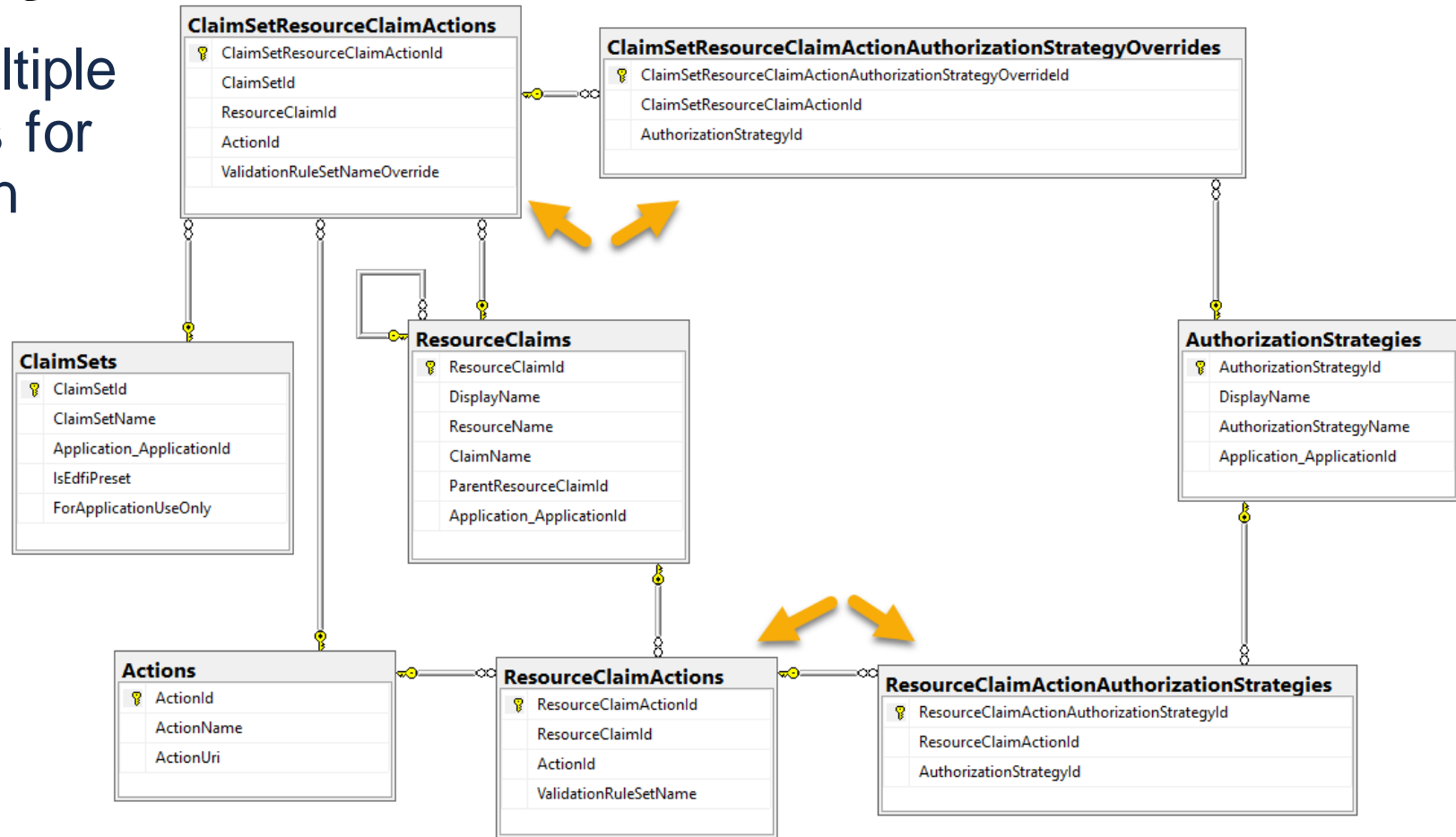
EdFi_Ods

Each aggregate root table in the ODS will have CreatedByOwnershipTokenId column (smallint) added.

Student (edfi)	
BirthInternationalProvince	^
BirthCountryDescriptorId	
DateEnteredUS	
MultipleBirthStatus	
BirthSexDescriptorId	
CitizenshipStatusDescriptorId	
PersonId	
SourceSystemDescriptorId	
StudentUniqueld	
Discriminator	
CreateDate	
LastModifiedDate	
Id	
CreatedByOwnershipTokenId	→
ChangeVersion	▼

EdFi_Security

- Updated to support multiple authorization strategies for a given resource/action combination.



Technical Congress Registration is Open

<https://events.bizzabo.com/TechCongress>



TECH#CONGRESS HOME AGENDA HOTEL COVID-19 SAFETY

TECH
CONGRESS

April 6th - 8th, 2022
The US Grant Hotel | San Diego, CA
In Person & Virtual Options

Register

The screenshot shows a website header with navigation links: TECH#CONGRESS, HOME, AGENDA, HOTEL, and COVID-19 SAFETY. The main content area features a large orange-tinted image of a city building facade. Overlaid on this image is the event logo 'TECH CONGRESS' in white and black text. Below the logo, the dates 'April 6th - 8th, 2022', the location 'The US Grant Hotel | San Diego, CA', and the format 'In Person & Virtual Options' are displayed in white text. A dark grey 'Register' button is positioned at the bottom center of the image area.



ed-fi[®]
ALLIANCE

Wrap up and Q&A