# API Security Work Done

Below are the API security work which i co-ordinated,

* OAuth for internal customers
* OpenAM Rest STS for external customers

Just write down the work which you have done in your previous project.

* OAuth based security for internal customers
* OpenAM Rest STS based security for external customers

SAML Assertion was used. Public / Private key pair is used for encryption.

OpenAM worked as Identity Provider.

So what is the sequence of events that happens :-

1. Node API calls restful STS endpoint of OpenAM. While calling Node API passes Customer email.
2. OpenAM returns digitally signed SAML assertion.
3. Node API sends digitally signed SAML assertion to Spring Boot Api via Mule Gateway.
4. .SAML Assertion reaches to the Spring Boot API.
5. Spring boot api decrypts digitally signed SAML assertion, with the help of public key
6. Once SAML assertion payload is decrypted, Spring boot api extracts customer email from the payload
7. Spring boot api calls OpeaAM api to validate if customer exists, or else customer registration flow gets executed. Thats a separate flow.

Q. What is a SAML ?  
Ans - SAML (Security Assertion Markup Language) is a XML based framework for authentication and authorization, between two entities. These two entities are popularly known as,

* Identity Provider
* Service Provider

SAML is a standard single sign on (SSO) format.