Architecture

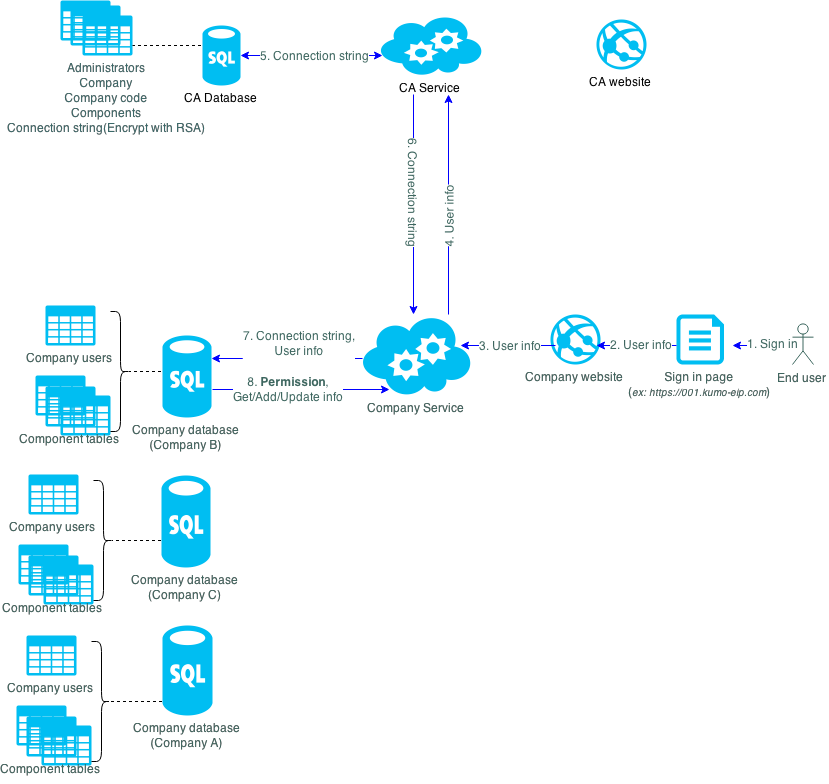
[KUMO]

Version [2.0]

Prepared by

[Alice Huynh]

1 Architecture Diagram

****

Red line: when administrator sign in

Blue line: when end user sign in

EIP system has 2 main application. Central Administration website (CA) and company website with separate database for each company. It mean all company will use the same company website. Each company has their own separate database.

Company information are managed by KUMO administrator directly from CA. Based on end user sign-in information (in this case, we use **sub-domain approach** for authentication), the corresponding company information (database connection string, components) will be send to company website to retrieve data showing to the end user.

RSA algorithm will be use in CA and company website to encrypt and decrypt company’s information. Company service will call CA service on CA to query information. CA service will return data which matches with the client code in encrypted data. Company website has to use a provided public key to decrypt that data to get database connection information. The public key will be generated automatically for each company.

CA website is a MVC website. It’s like the template. The page that administrator see on their screen is the template + data from CA database.

Company website is a MVC website too. It’s like the template. The page that end-user see on their screen is the template + data from company database.

# Sub-domain approach

Company users will be saved in their own database.

To make **Sub-domain approach** work, when end-user sign in, they have to input correct sign-in URL to identity which company they are belong to, and system will using that information to resolve their database. (*Ex: user Alice in company A will sign in at https://001. kumo-eip.com, user Bob in company B will sign in at* [*https://002.kumo-eip.com*](https://002.kumo-eip.com)*)*.

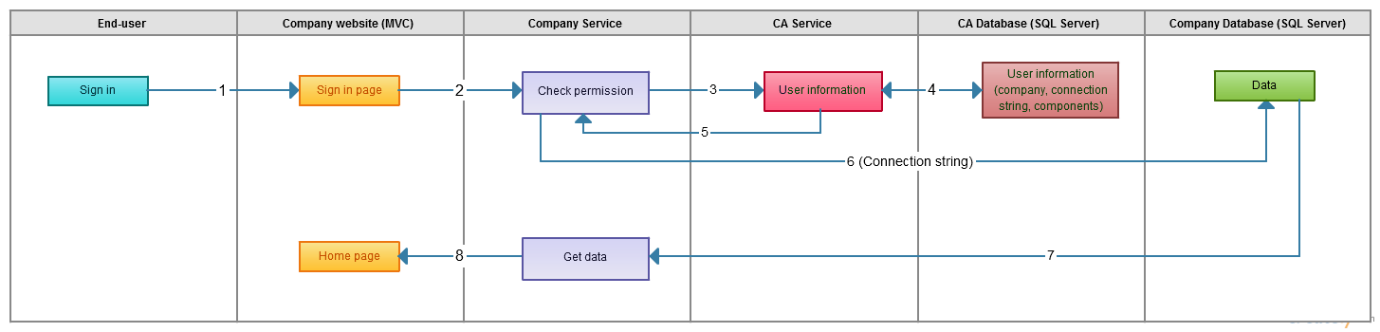
1. **Advantage**

* Company information was managed on CA website
* Can using 1 domain for Company website
* Database for companies is separate and they are only work on their database.
* Don’t need to store company user information on CA website
* Better performance because database separate
* Easy to maintain/backup/restore company database
* Less development effort because don’t need to add additional code to connect to 2 database.

1. **Disadvantage**

* Users must log in correct URL of their company, example [https://**001.**kumo-eip.com](https://001.kumo-eip.com)

# End-user sign in



* 1. End user sign in to Company website (ex: user Alice of company A will sign in at [https://**001.**kumo-eip.com](https://001.kumo-eip.com))
  2. Company website send input information to the Company Service.
  3. Company Service will send input information (include the sign in URL information) to CA Service
  4. Based on the sign in URL ([https://**001.**kumo-eip.com](https://001.kumo-eip.com)), CA Service connect to Central Admin database (CA database), getting connection string to company database and return it to CA Service.
  5. Service get connection string and user information from CA Service.
  6. Using those information, Service connect to corresponding company database, check the account is valid or not.
  7. If it’s valid (username and password is correct), Service will get data from corresponding company database and return it to the Company website.
  8. Company website show data returning from Service.