DESIGN DOCUMENTATION

e-Qualification

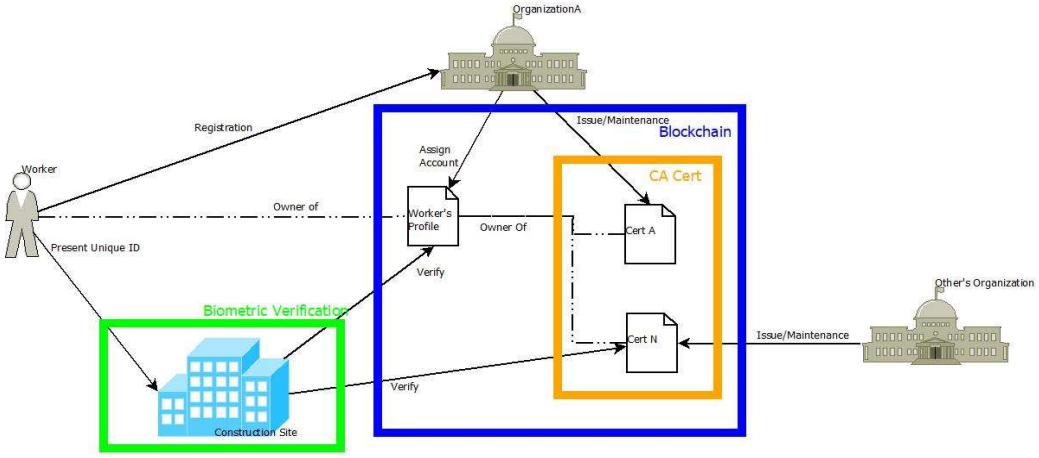
V1.1

Dick Chan

dick@assetonchain.com

TABLE OF CONTENTS

0. OVERVIEW



From the high-level overview diagram, the proposed solution can be separated into 2 main components:

1. Digitalization of qualification:

   All qualification issued by organization will be transformed to a digital certificate format using traditional CA technology.

2. Blockchain:
   Private Ethereum network for secure information access and interaction in the form of smart contract.

The following table summarized each sub-component that build up the solution.

Sub-component	Description	Implementation	Main component
Individual/Worker	Individuals obtain qualifications and owner of worker profile	Blockchain wallet	Blockchain
Qualifications	Physical certificates issued and maintenance by Organizations to individual on recognition of skill's level obtained.	No	No
Digital Certificate	Digital representation of Qualifications, based on CA cert Technology	• CA • Smart Contract • ERC721	• Digitalization of qualification • Blockchain
Organization	Entity that responsible for issue and administration of qualification Each organization has their own qualification	Blockchain wallet	Blockchain
Organization staff	Work in organization on digital cert maintenance and assignment, permission is controlled by organization	Blockchain wallet	Blockchain
Organization Directory	A directory service for each organization for resource lookup	ENS	Blockchain
Public Directory	A directory service which service for organization lookup and their related role	ENS	Blockchain
Role base access control	It is used to maintain permission for organization staff on which function can be perform.	Smart Contract	Blockchain
Profile of individual	A storage which contains individual's personal information and qualification obtained.	Smart Contract + ERC721 Token	Blockchain

1. INDIVIDUAL/WORKER

Individual/worker is an ordinary account that issue from the blockchain with a pair of public and private key which used for identification purpose as usual.

2. QUALIFICATIONS AND DIGITAL CERTIFICATE

Traditional qualifications are issued in physical card format with related information printed, here is a sample of the field which may find on the card:

a. Name (Eng and Chi)
b. Photo
c. Types of qualification
d. Issue date and expiry date
e. Issuing Authority
f. Teams and conditions

Those information describe above serve for 2 purposes:

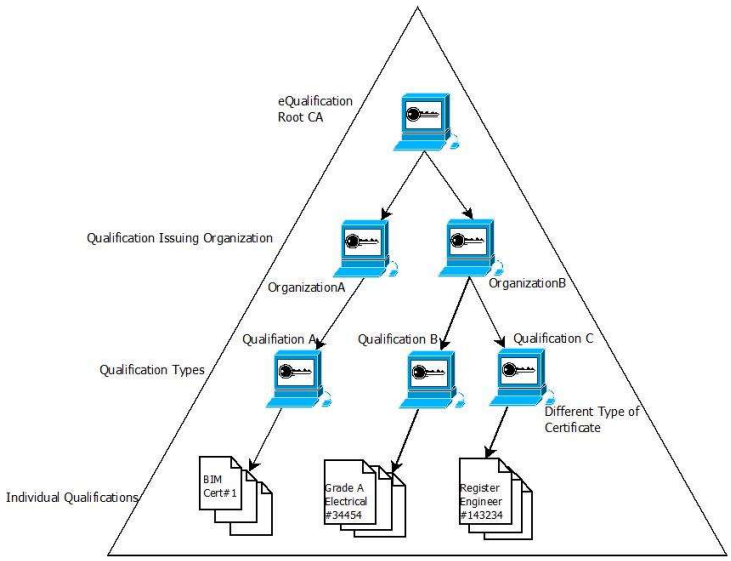
a. Identify the owner
b. The legitimacy of the qualification
    i. Is it valid?
    ii. Is issued by the right Authority?

Intuitively, with these two requirements and the need of digital transformation, it is easy to think of a ready to use and well proven technology which full fill the needs above – Certificate Authority (CA).

Each issued qualification to individual by organization can be represented by a signed digital certificate as the usual one. While it is easy to show how legitimacy purpose is achieved, the identity purpose will need helps from blockchain which will cover later.

Each qualification issuing organization can have their own CA or it can use CA service provider outside. In this solution, it is assumed to use the second scenario which all organization will use a single CA and each of them will act as an intermediate CA located in the second level.

Here is a simple illustration on the structure.



The CA tree structure will have at least 4 levels. The second level is representing each issuing organization (Organization Digital Certificate) while the third level act for different types of qualification (Digital Cert Cabinet) that is provided by organization. Those qualifications issue to individual will be at the leaf node.

When generating a digital certificate, it is required to have a public/private key as input, for the solution, there are three places which will need it:

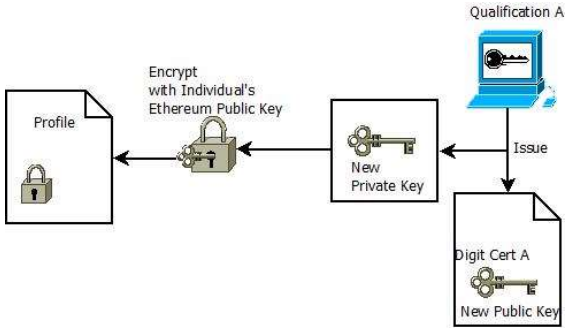
1. Organization Digital Certificate (second level)

   The Ethereum public/private key of organization can be used for generating organization digital certificate.

2. Digital Certificate Cabinet (third level)

   Any ECC public/private key is ok, either on-chain or off-chain.

3. Individual Digital Certificate (leaf node)
   It is suggested to use a new pair of public/private key for generating digital certificate for individual instead of using individual Ethereum pair of keys. Once the digital certificate for individual is issued, the private key of the cert can encrypt with the individual's Ethereum public key and associated with the individual's profile. This action can enforce the identity verification purpose. Below is a simple diagram to illustrate the process:



2.1 INTEGRATION BETWEEN DIGITAL CERTIFICATE WITH ETHEREUM

The above section has introduced how to transform qualification into digital certificate based on CA with only limited association with Ethereum. In the following section it will cover how is digit cert interact with blockchain.

2.1.1 REPRESENTATION OF INDIVDUAL DIGITAL CERTIFICATE ON ETHEREUM

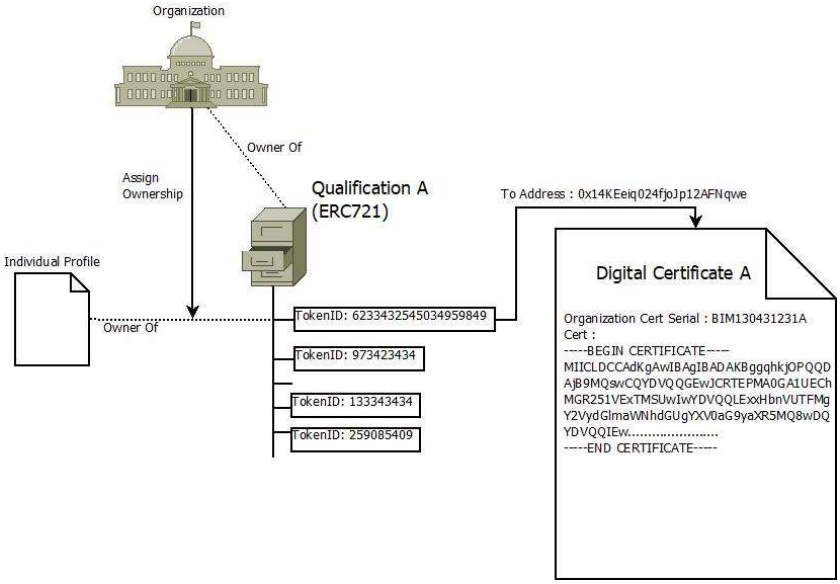
Each issued individual digital certificate is represented by a smart contract on Ethereum which it uses to contain the cert in PEM format(~4KB) with other's additional information require.

2.1.2 LOGICAL ORGANIZATION OF INDIVIDUAL DIGITAL CERTIFICATE ON ETHEREUM

In order to manage those qualification smart contract efficiently, it is suggested to adopt tokenization for those qualification smart contract. In the solution, it will use non-transferable ERC721 standard to represent different types of qualification issued by organization.

ERC721 will be act as a logical cabinet (Qualification Cabinet in this solution) on Ethereum which it logically contains a collection of qualification smart contract under the same category, each of the qualification smart contract is represented by a unique token ID and is assigned to a specific owner (individual's profile in this solution). The owner of the cabinet will be the qualification issuing organization.

Furthermore, other than a collection of tokens ID, the cabinet will also contain the Digital Cert Cabinet of its own (third level) for ease of verification.



2.1.3 ACCESS OF QUALIFICATION SMART CONTRACT AND QUALIFICATION CABIENT

On Ethereum, smart contract is reference by a unique contract address in byte format which is hard to manage, furthermore as there may be many types of qualification and individual qualifications, it needs a way to reference the desire qualification smart contract as easy as possible. In this solution, Ethereum Name Service is introduced to enhance the manageability and efficient on access for contract.

ENS is an address lookup service in Ethereum which it translates a human readable URI into Ethereum address. The whole picture of ENS will be covered later in Organization Directory section, here, only Qualification Cabinet and Qualification smart contract is concerned.

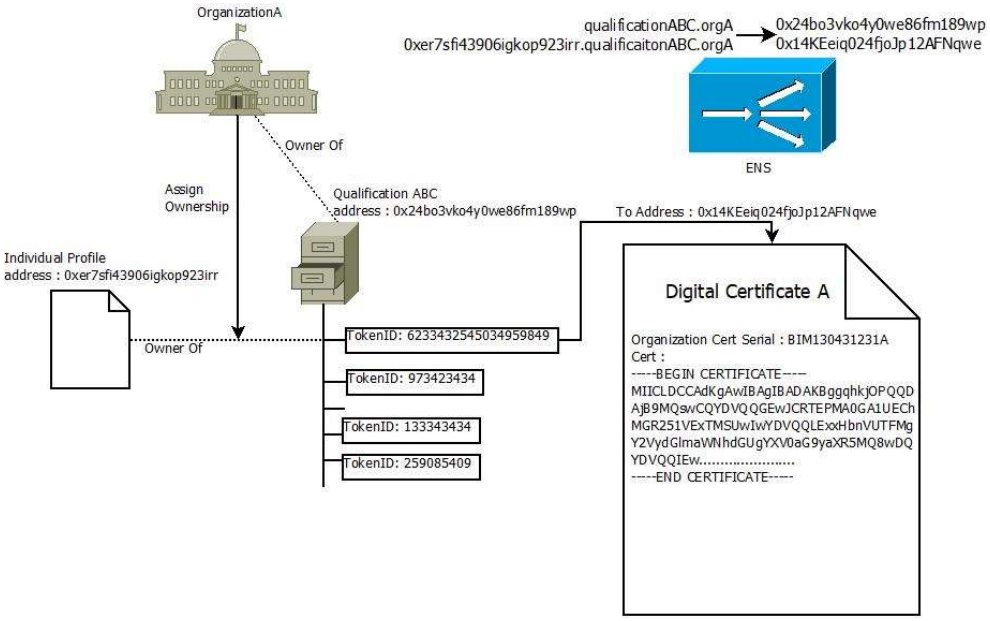
Each Qualification cabinet will have a name associated with it, and this name will be concatenated with the issuing organization name to form a URI, for example:

qualificationABC . orgA

and for those individual qualification smart contract, it will have the following format URI :

<owner's profile contract address> . qualificationABC . orgA

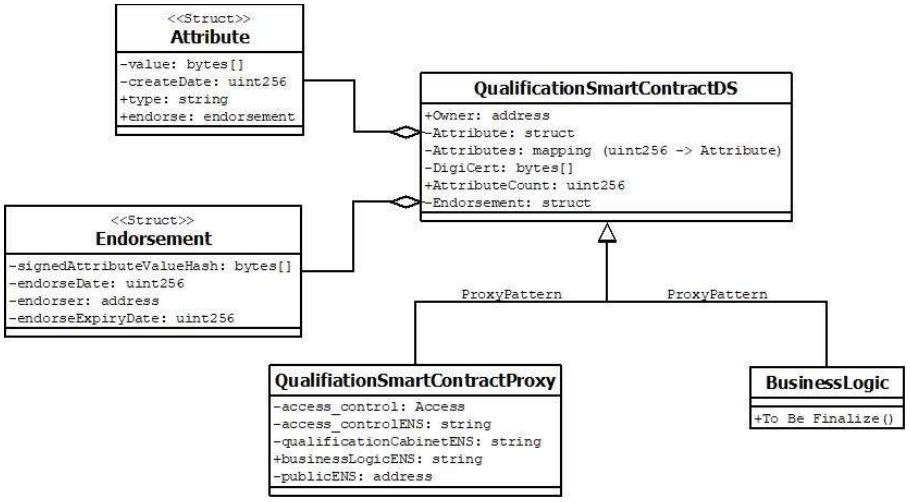
Those URI will then register in the ENS with its own smart contract address.



2.2 IMPLEMENTATION OF QUALIFICATION CABINET AND QUALIFICATION SMART CONTRACT

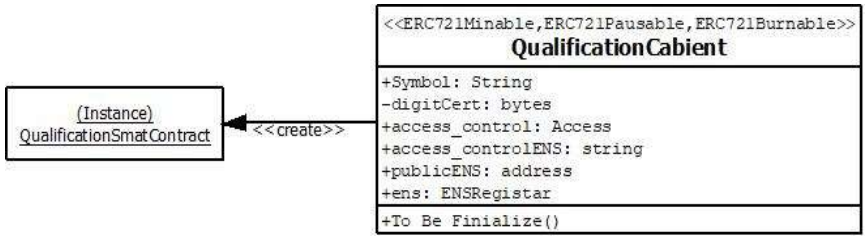
2.2.1 QUALIFICATION SMART CONTRACT

Qualification Smart Contract Class Diagram (Not Finalized)



2.2.2 QUALIFICATION CABINET

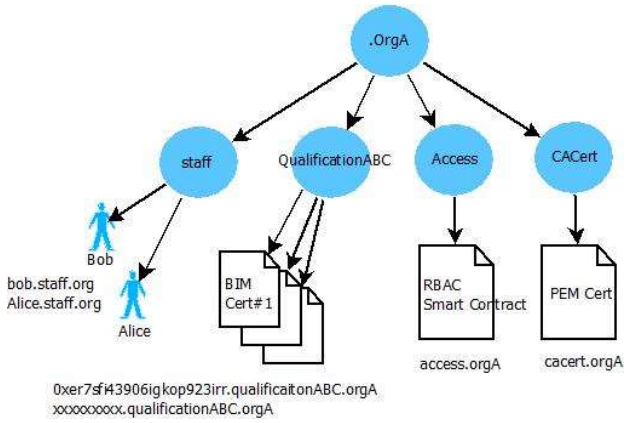
Qualification Cabinet Class Diagram (ERC721)



3. ORGANIZATION , ORGANIZATION STAFF AND ORGAINZATION DIRECTORY

Organization serves two roles in this solution; the main purpose is as a qualification issuing authority and the second is to endorse information. As from pervious section, organization may have many resources such as: different types of qualification, issued qualifications to individual, access control and staff, so it is why a directory service is need for handling and managing those resources. In this solution, each organization will have their own directory service instead of a consolidate one in order to provide flexibility on rather they will have their own blockchain or not.

The directory service will be fulfilled by ENS. Each organization will assign a unique naming for the root node of the directory tree, and they are freely to register URI under it except some per-defined keywords. Here is a simple diagram to demonstrate the ideas:

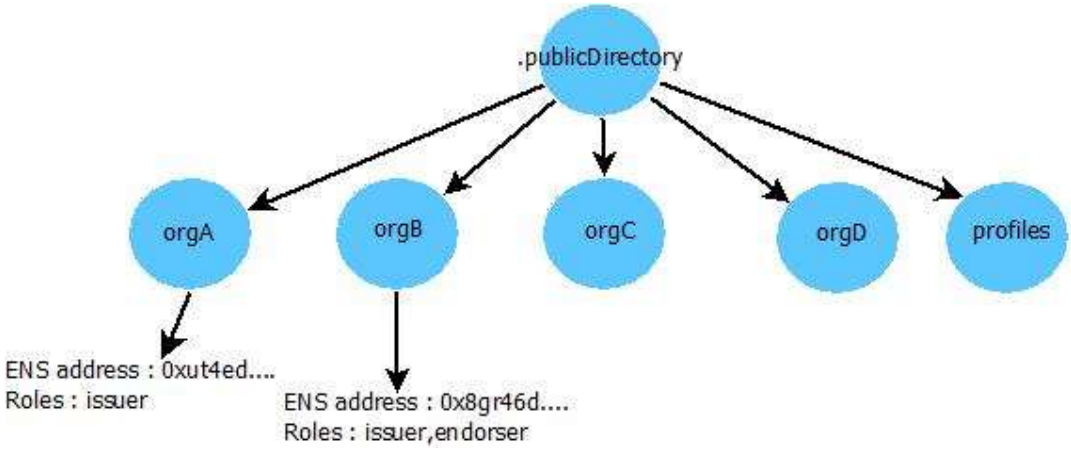


4. PUBLIC DIRECTORY

The public directory service is nothing more but a directory which contains public information for access, there are 2 kinds of information which needed:

1. each organization's ENS endpoint and their duty
2. Individual Profile

It is used to bridge up those separated organization directory service and Individual profile



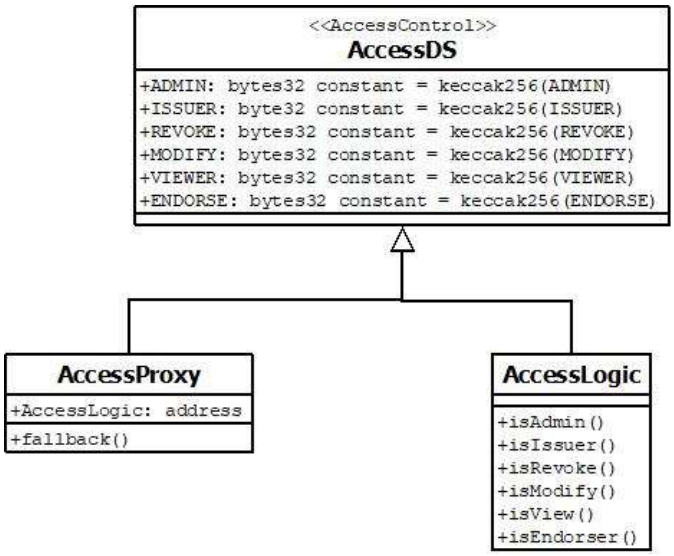
5. ROLE BASE ACCESS CONTROL

Access control is applied on the action to qualification cabinet, qualification smart contract and individual/worker's profile base on pre-defined roles. Organization will have own access control setting to their staff on permitting who can perform what action. Those predefine roles is summarized in the following table:

Role Name	Description
ADMIN	Super admin
ISSUER	Can issue qualification smart contract to individual
REVOKE	Can revoke issued qualification smart contract from individual
MODIFY	Can change information
VIEWER	Can view information
ENDORSE	Can endorse information

5.1 IMPLEMENTATION OF ROLE BASE ACCESS CONTROL

Role base access control class diagram

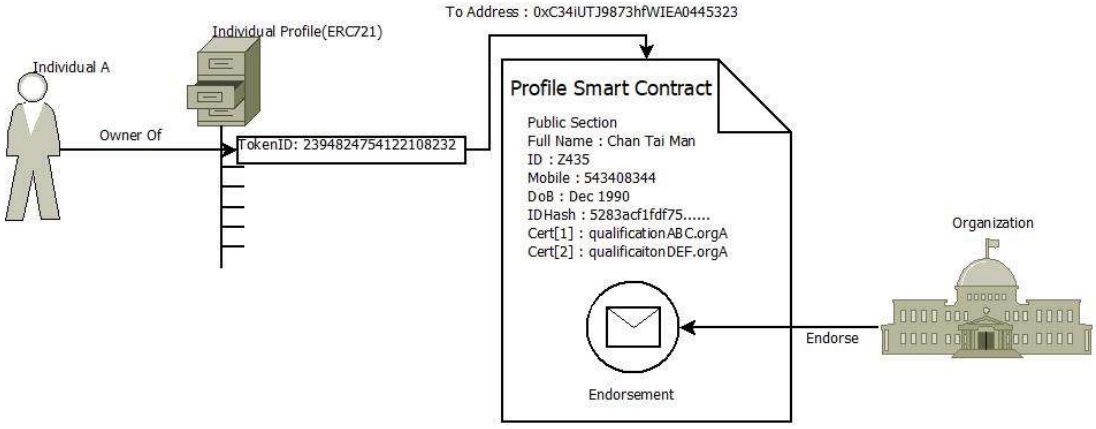


6. PROFILE OF INDIVIDUAL

Individual's profile is used to store related personal information which has register in the solution together with those qualification cabinet URI that they have obtained. The profile can be generated by anyone who wish to use the service and maintain that personal information by themselves, below is a high-level visualization of the profile smart contract.

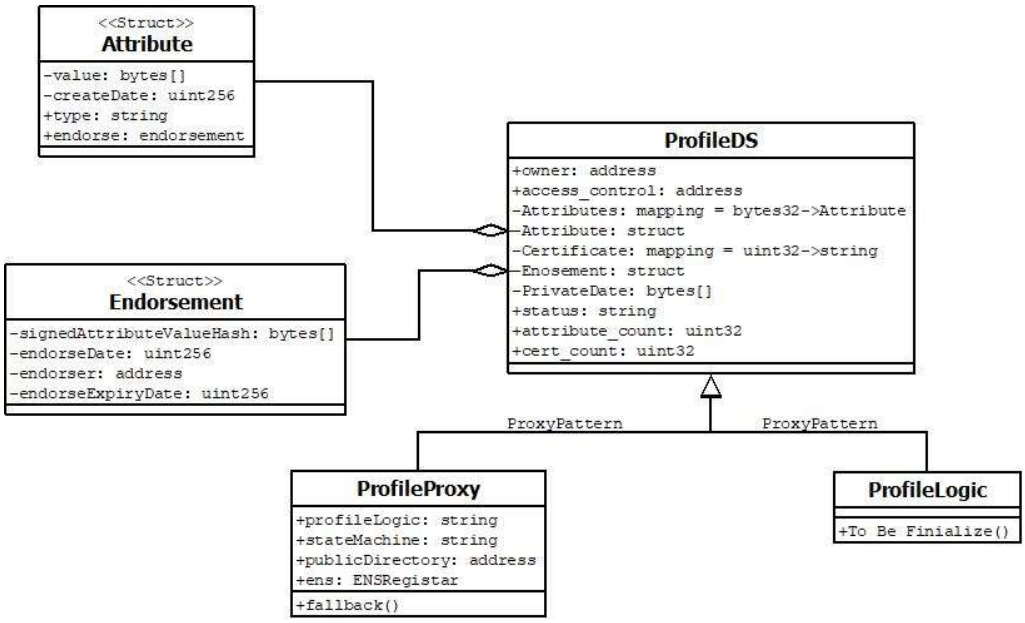
After the profile smart contract is established, it can ask for endorsement on the personal information from organization. As the personal information is provided by individuals, state restriction is enforced to qualification issuance on profile which it require the profile must be in endorsed state to receive qualification, the transition will be shows in the next section.

As before, in order to manage huge number of profiles for individual, those profiles will be logically group into a collection under the ERC721 standard, just like for those qualification smart contract.

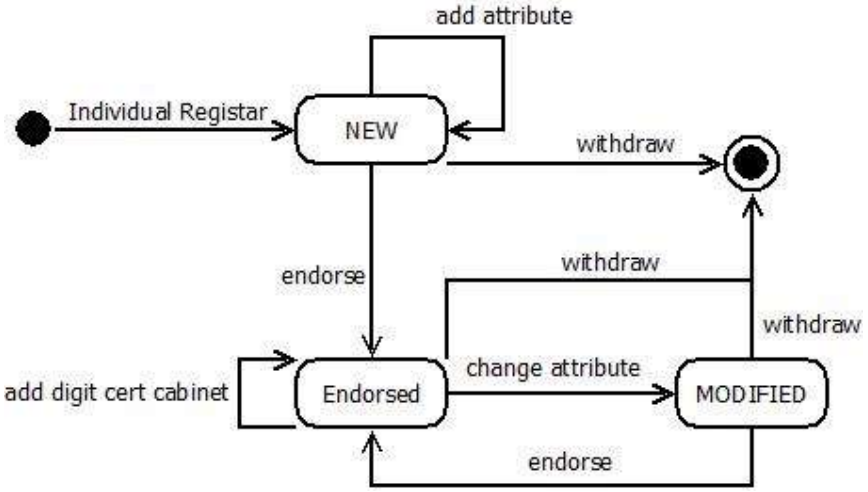


6.1 IMPLEMENTATION OF INDIVIDUAL PROFILE ON ETHEREUM

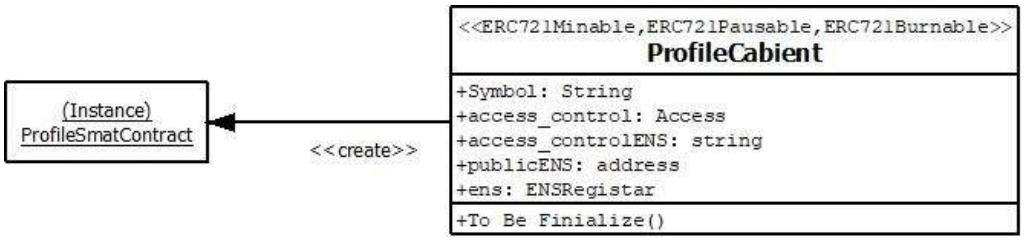
The profile will be implemented as a smart contract just like the qualification smart contract.
Class diagram of individual profile.



State diagram for Individual profile:

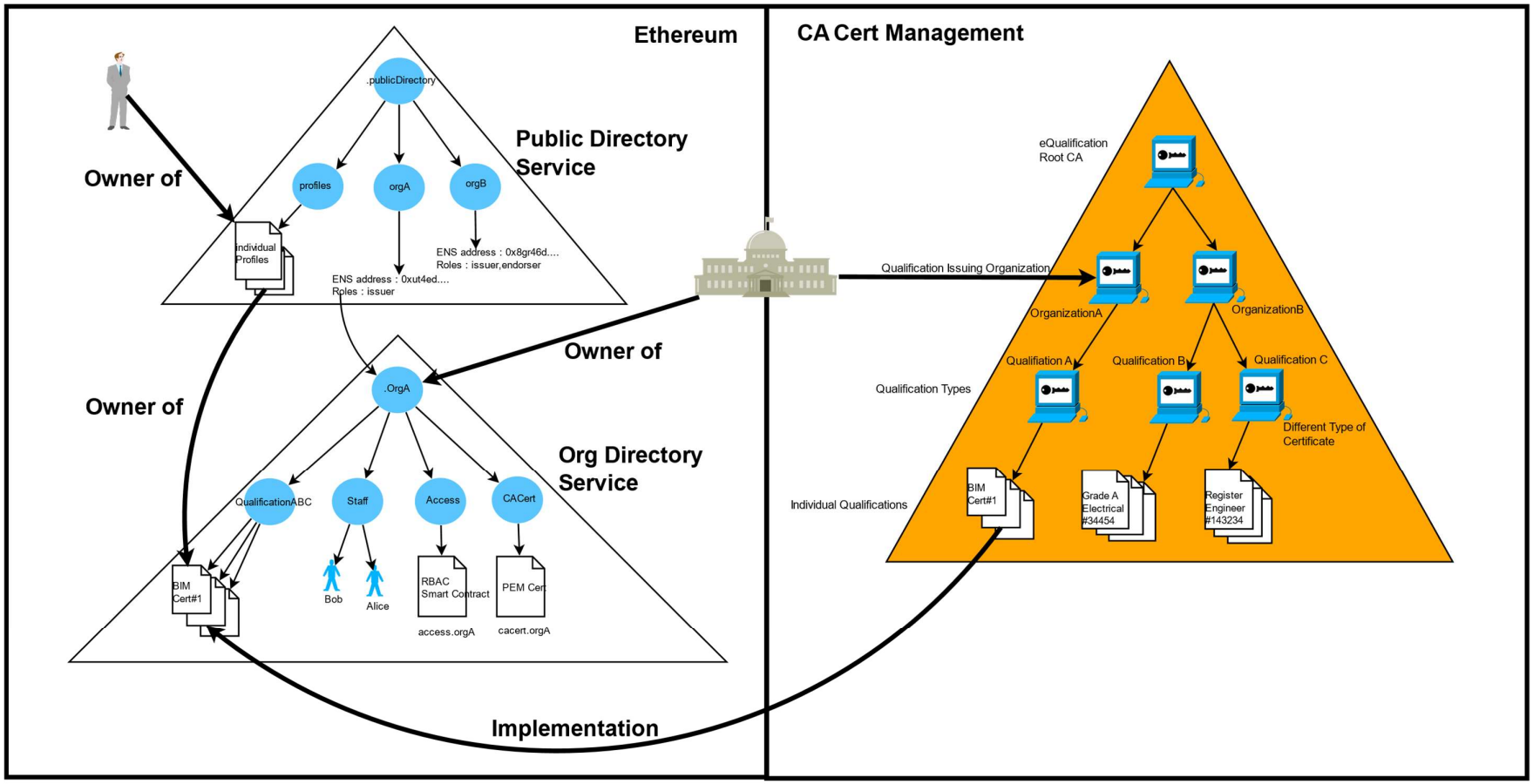


Class diagram for Profile Cabinet



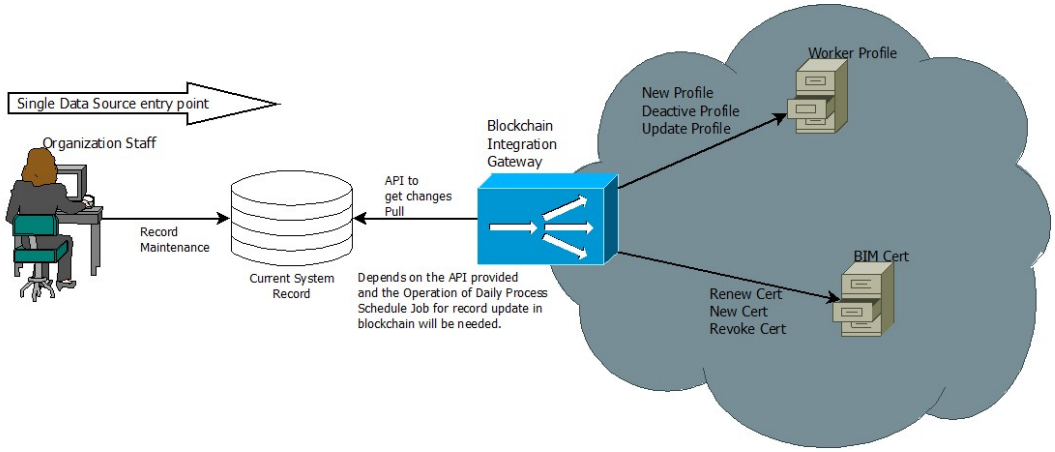
7. OVERVIEW ON INTERGATION OF ALL THOSE COMPONENTS

The following diagram will give an overview structure on how those components described above to be related.



8. INTEGRATION BETWEEN SOLUTION AND CURRENT SYSTEM

The solution is designed to integrate with the current qualification management system in the first phase to automate the process. Those individual's record and qualification data from the current system will be sync to the solution by batch job during pre-agreed time slots.

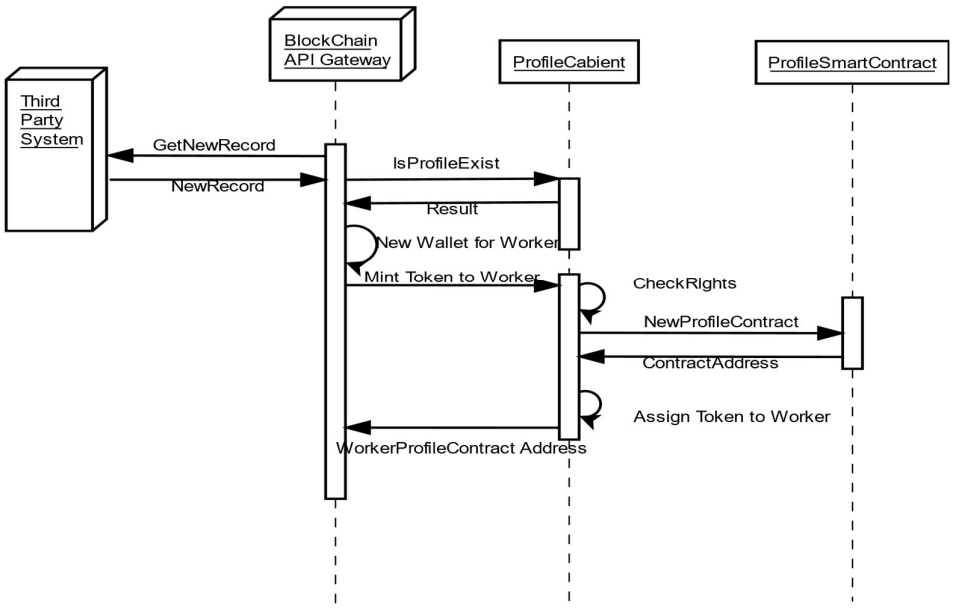


9. INTERACTION BETWEEN COMPONENTS

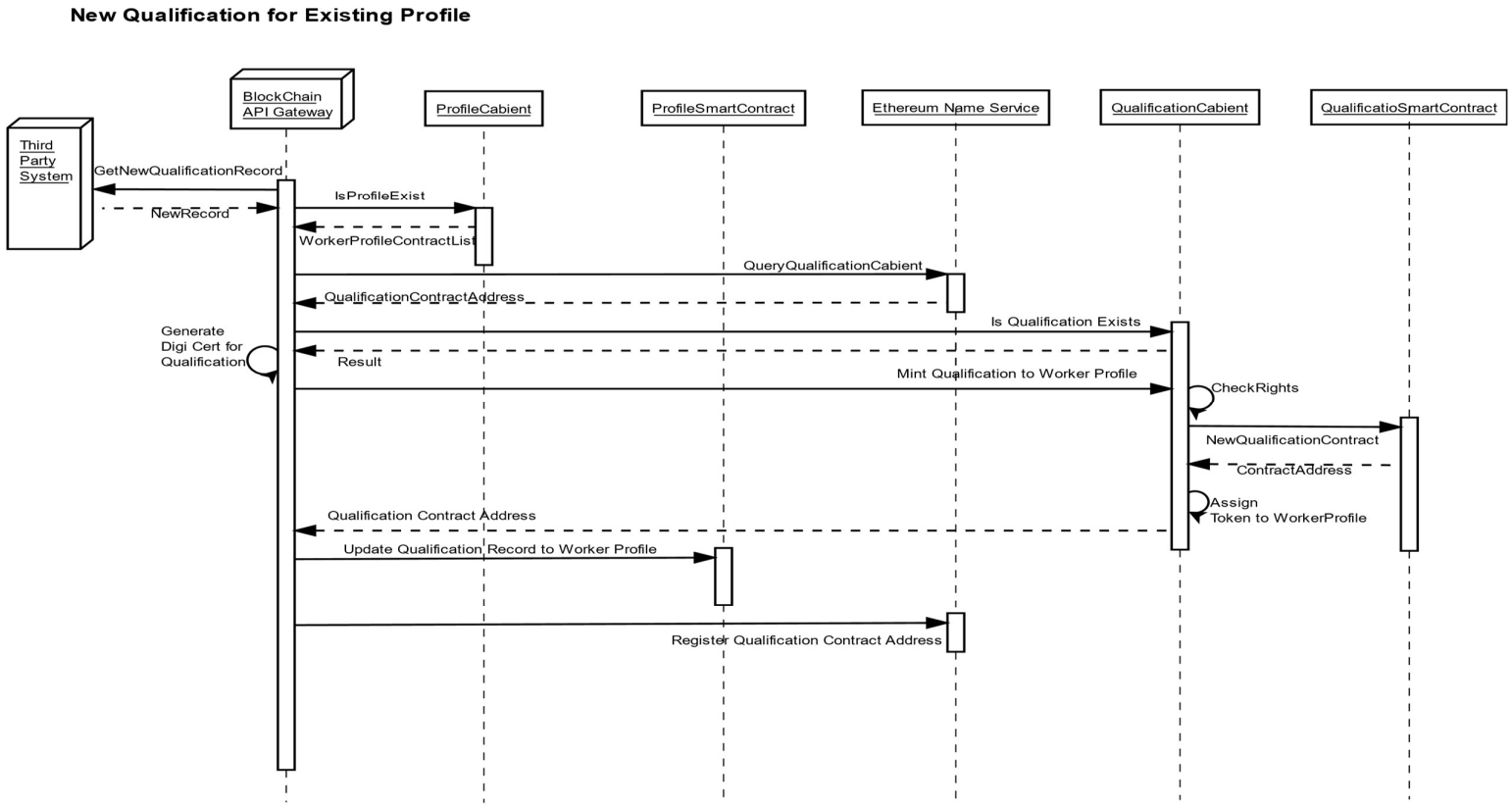
Sequence diagram to illustrate the interaction between components on different action

9.1 NEW INDIVIDUAL PROFILE

New Profile for Individual

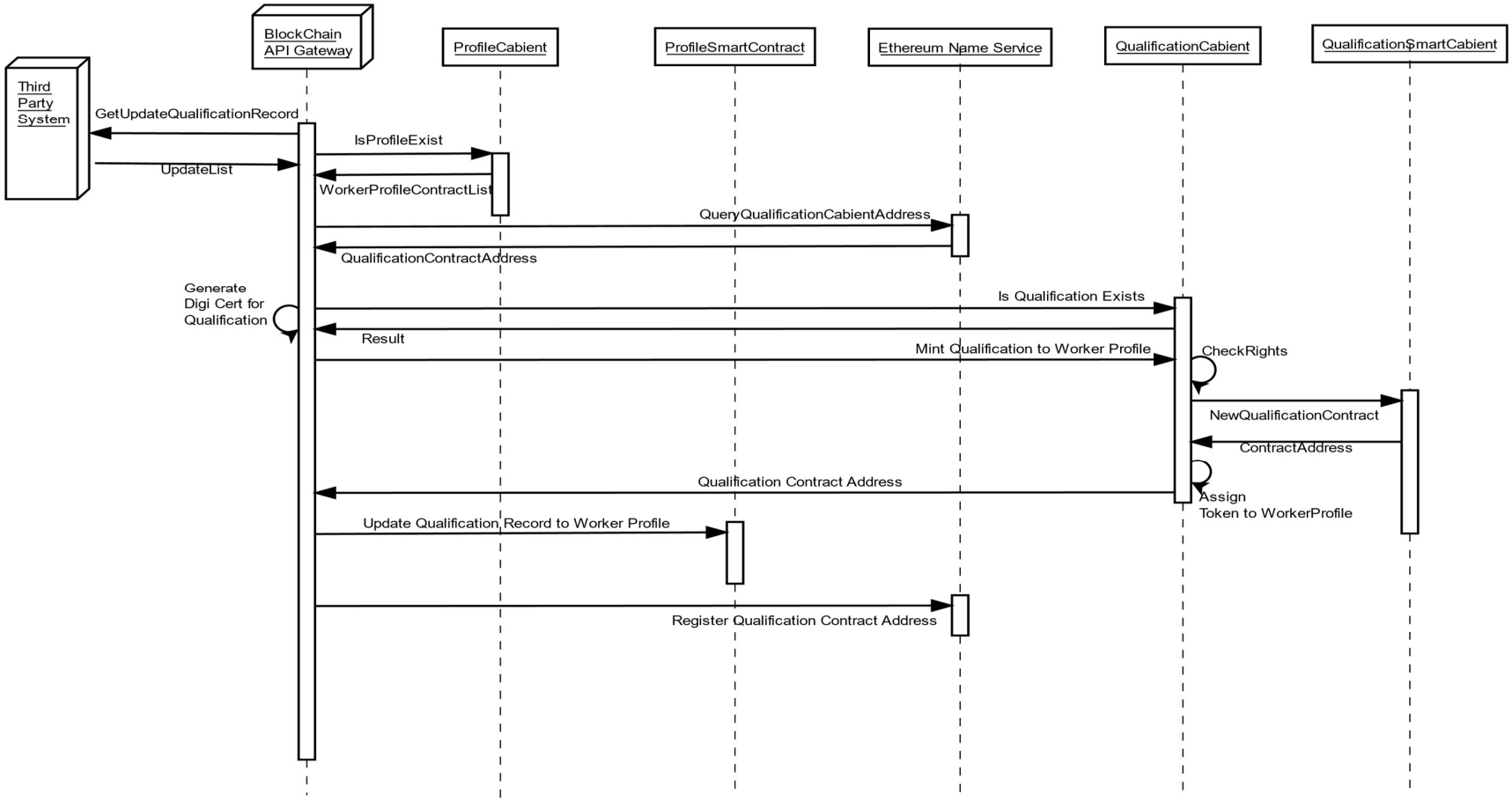


9.2 NEW QUALIFICATION FOR EXISTING PROFILE



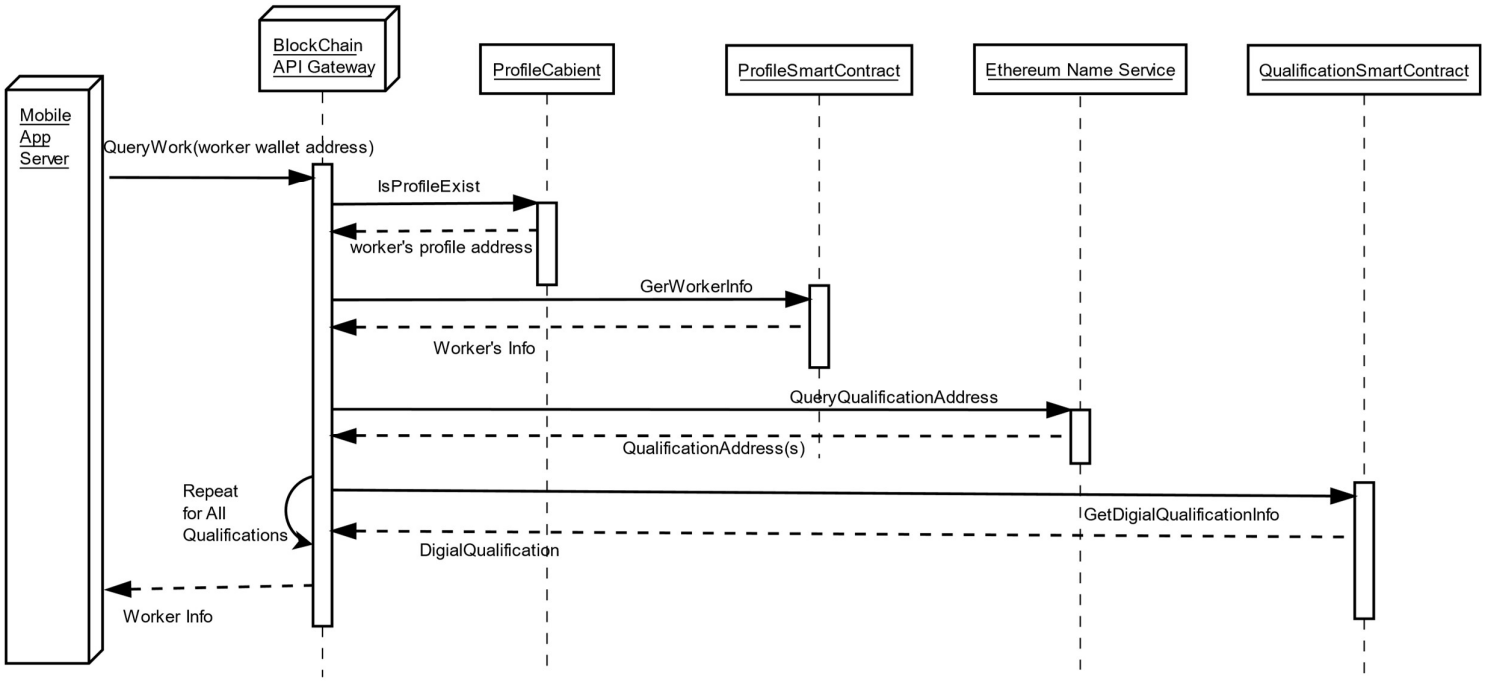
9.3 UPDATE/RENEW QUALIFICAITON FOR PROFILE

Update/Renew of Qualification for Existing Profile



9.4 QUERY OF QUALIFICATION FROM PROFILE

Query Qualificaiton record for Profile



10. INFRASTRUCTURE PROPOSAL

The following infrastructure diagram shows how mobile app and the solution to be implement on hardware level.