Privacy-preserving Resource Sharing using Permissioned Blockchains (The Case of Smart Neighbourhood)

1 A case study for proof-of-concept implementation.

In this section, we present an example of a digital object sharing using CP-ABE to describe the application of our blockchain based resource sharing scheme. Suppose, A_o owns a movie *"Tom's Trip to Moon"* that he wants to share. We assume that the attribute universe of each user is {*Age*, *Preference*, *Club membership*}, where $Age \in [5, 80]$ is an integer value, $Preference \in \{local, international\}$, and *club membership* is realized by a (possibly empty) subset of three clubs, $club1, club2$, and $club3$ corresponding to *Fan-club of cartoon movies*, *Fan-club of adventure movies* and *Fan-club of horror movies*, respectively. Objects (shareable data) are associated with a *title* and a set of properties from the $\{Type, Quality, Size\}$ universe, where $Type \in \{Movie, e\text{-}book, image\}$, $quality \in \{SD, HD, UHD\}$[1], and $1MB \leq size \leq 10GB$.
Based on this description, we have the following setup for our use case scenario: *(i)* attributes of user A_o, $attr_A = \{$*31, local, club2*$\}$ and user B_r, $attr_B = \{$*20, international*, $\{$*club1, club2*$\}\}$, *(ii)* movie properties, $prop_O = \{$*Movie, HD, 16 MB*$\}$, *(iii)* metatdata, M_{c_O} = "*Tom's Trip to Moon is a story of a child who dreams to travel to moon someday.*", *256-bit symmetric key*, "*https://onedrive.com*", and *(iv)* access policy, $acc_O = \{$"Age" $> 6 \wedge$ "Preference" $= (local \vee international)$ $\wedge$ "club membership" $= club2\}$.

[1] corresponding to standard definition(SD), high definition (HD) and ultra high definition (UHD) qualities

2 Advertising an object

Please see Figure 1 for the sequence diagram of advertising an object by a resource owner.

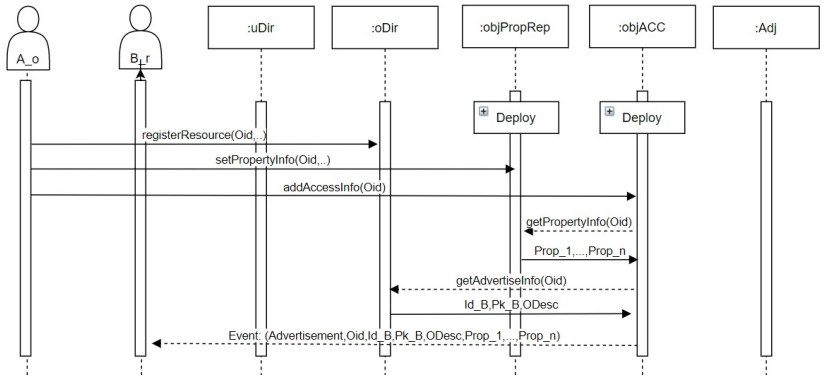

Figure 1: Sequence diagram of advertising an object by resource owner

3 Requesting an access.

Resource requester B_r searches its local database that contain the list of advertised resources and finds the identifier of the resource they want to get access to. Then user A retrieves the address and ABI of `objACC` and `objPropRep` contracts. If resource is available user A retrieves the properties and certificates of the resource from `objPropRep` contract. Then, they send a request to `objACC` contract to gets policies and CP-ABE metadata. BA perform the authentication and replies to the requests of user accordingly. When user gets CP-ABE metadata, he decrypts it using his private key. If the decrypted link does not provide the resource that user wants, he make a complain to `Adj` contract for further checks.

$B_r \rightarrow$ `oDir`: *Oid*

`oDir` $\rightarrow B_r$: pId_{A_o},pk_{A_o}, *ODesc,* ***`objPropRep`*** *address,* ***`objPropRep`*** *ABI,* ***`objACC`*** *address,* ***`objACC`*** *ABI*

$B_r \rightarrow$ `objPropRep`: *Oid*

`objPropRep` $\rightarrow B_r$: $Prop_o$, $Cert^o_{CA}$

$B_r \rightarrow$ `objACC`: *Oid*

`objACC` $\rightarrow B_r$: $c^{CP-ABE}(M(c_O))$, acc_o