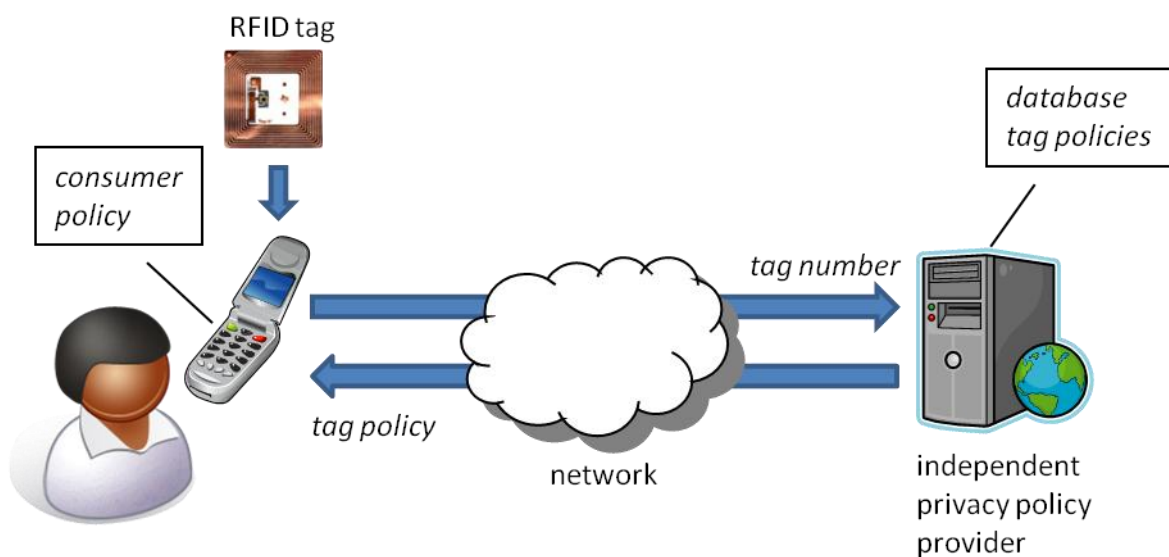


DIFR Privacy Coach

System Design

De implementatie van de Privacy Coach bestaat uit 2 delen:

- De client – een applicatie die op de mobiele telefoon van de eindgebruiker draait.
- De server – centrale applicatie waar middels XML berichten privacy policies voor RFID tags uitgelezen kunnen worden.



De Client

De Client applicatie is een Java toepassing die op een telefoon gedraaid kan worden waar een RFID lezer op aanwezig is. Door de applicatie te starten en de telefoon vervolgens bij een RFID tag te houden wordt de Privacy Policy die bij deze tag hoort van de server opgehaald. De policy wordt vervolgens gematched tegen een door de eindgebruiker ingesteld profiel wat opgeslagen is op de telefoon.

Subsystemen

De client bestaat uit de volgende subsystemen:

1. User Interface

De eindgebruiker bedient de applicatie middels dit onderdeel. Hier worden tevens de andere subsystemen aan elkaar geknoopt.

2. Tag Reader

Hier wordt wanneer de gebruiker zijn telefoon bij een RFID tag houdt de unieke ID uitgelezen.

3. Web Service Connector

De connector verzorgt de communicatie met de Web Service. De uitgelezen tag ID wordt in het juiste formaat naar de server gestuurd en het bericht wat terug komt wordt naar een Java object omgezet zodat andere onderdelen van de applicatie hier makkelijk mee overweg kunnen.

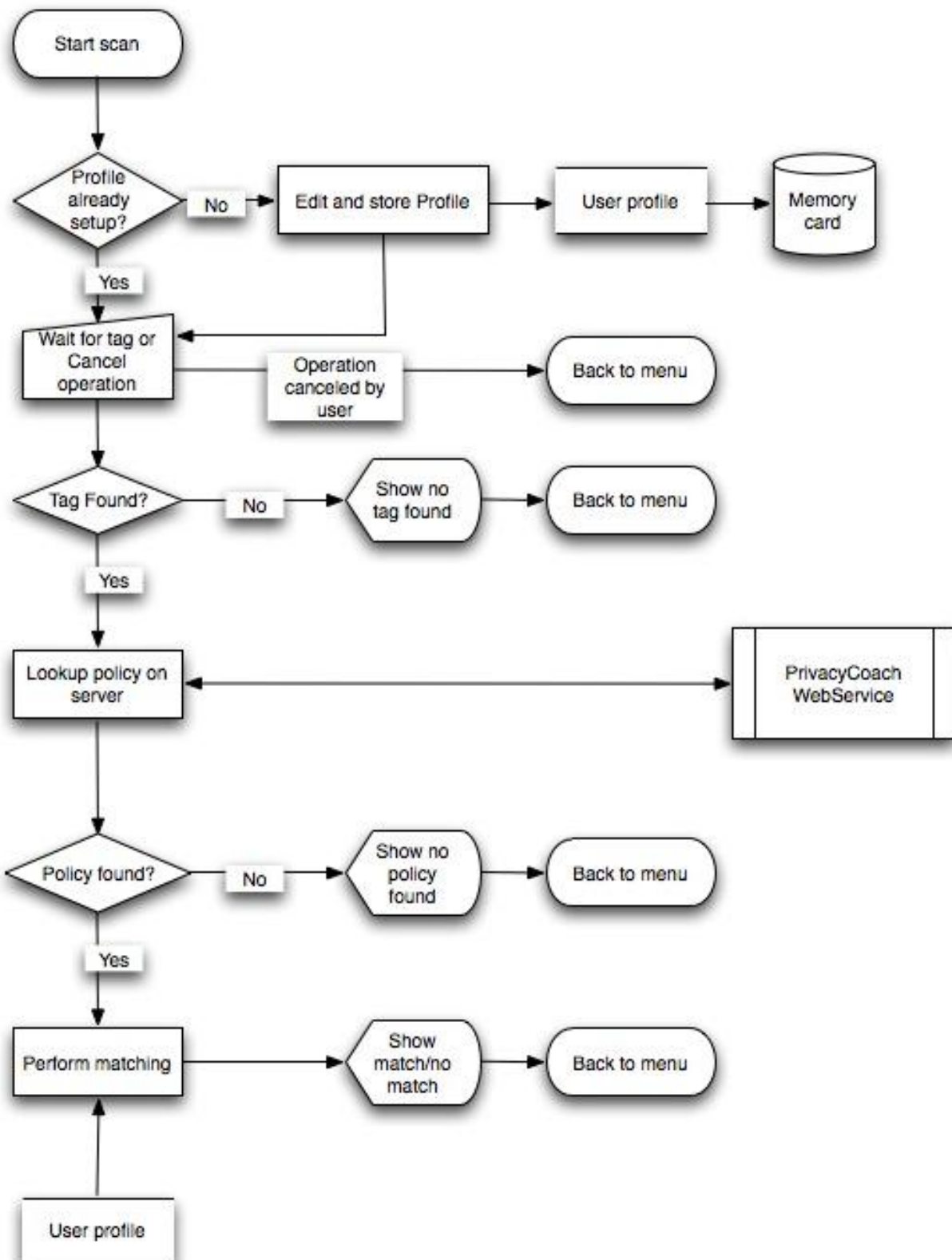
4. Matcher

De policy die geretourneerd wordt door de server wordt hier gematched tegen het door de eindgebruiker ingestelde privacy profiel. Hier wordt bepaald of een bepaalde policy al dan niet toelaatbaar is voor de eindgebruiker.

5. User Profile Reader/Writer

Verzorgt het inlezen en wegschrijven van het door de eindgebruiker ingestelde profiel. Het profiel wordt weggeschreven op de geheugenkaart van de telefoon.

Flow overzicht



De Server

Het server gedeelte van de applicatie is een webservice waarin die aan de hand van een tag ID in de URL een XML document retourneert met daarin de bijbehorende Privacy Policy, of een foutmelding als er geen policy is gevonden voor de ID. De verschillende policies worden in een MySQL database opgeslagen. Tevens beschikt de applicatie over een simpel Web interface waarin policies voor tags aangemaakt en verwijderd kunnen worden.

Model

In het datamodel op de server worden de volgende entiteiten gebruikt:

Tag:

Dit is een referentie naar een fysieke RFID tag met een uniek ID.

PrivacyPolicy:

Deze entiteit bevat precies 1 privacy policy. Voor elke ja/nee vraag zal er 1 PrivacyPolicy object zijn.

TagPolicy:

Deze entiteit koppelt 1 of meerdere tags aan een lijst de lijst van beschikbare Privacy Policies. Voor elke policy zal er aangegeven worden of hier een waarde ja of nee van toepassing is voor de gerelateerde tags.

Input/Output

De webservice zal aangeroepen worden door in de URL van de service de Tag ID mee te geven. De server bevraagt de database over de policies die gelden voor deze tag. Mocht de tag gevonden worden dan wordt de volgende XML geretourneerd:

```
<?xml version=1.0?>
<privacy-policies tagid=[de ingevoerde tag]>
  <privacy-policy policy-id=[unieke id van de policy]
value=[true/false]>
  ...
  ...
</privacy-policies>
```

Wanneer de tag ID niet gevonden wordt in de database wordt het volgende document geretourneerd:

```
<?xml verion="1.0"?>
<privacy-policies>
  <error tagid="[de ingevoerde tag]">
    Geen policy gevonden voor tag
  </error>
</privacy-policies>
```