COMPLETE ES

TSNZ4.3 Project Glinda

Va avea urmatorul continut:

Project Glinda: Overview

Version Control

Version	Date	Changes
0.1	05/01/2017	Initial draft
0.2	06/01/2017	Added details for monitoring and auditing
0.3	11/01/2017	Details of logging on and device locking to account have been added.

Overview

Obviously, dating apps are nothing new, with Tinder being the current market leader, however there is seen rather a dark side to Tinder. It's too easy to get an account, and you're never sure if the person you'll meet aligns to the photograph.

This level of unease is greatest within the gay and lesbian community, for whom 2016 has seen increasing aggressive behaviour towards this community. We want to create a dating experience where people can feel more comfortable that the person they meet will be the person in the photograph.

We also are very mindful that we don't want to become another organisation which relies of heavy data mining, and requires official documents. But for the safety of our users, we want to be sure the person with the account is someone we know about.

We started work in earnest to create a Gay and Lesbian Tinder, or Glinda, with the mission of providing as safe a dating experience for the gay and lesbian community as possible.

A key part is to have a validated account, you need to register an account with a valid credit card. One of our admins will then video phone you to speak with you – this conversation will be recorded, if you match the profile picture you've provided, you become a registered user – that's all there is to it, no paperwork.

To achieve all this we are using some services which already exist such as Skype for communications and dcPay as our payment gateway to minimise what we need to build from scratch.

Scope

Mobile Support

Glinda will be an application which will work on iOS and Android phones. The application will require a relatively modern phone – we'll only support iOS 10 and up, and Android KitKat and beyond. Likewise a selfie camera is a must, and when a user tries to install this software on a phone which lacks this, it must result in an error.

Out of scope - phase 1

Currently we're trying to launch Glinda with provision for supporting gay and lesbian users only, we're hoping to expand the base to support bisexual and transgender communities in later releases.

Account Status

A key part of Glinda is knowing you're really dealing with someone who has been verified. It's about making the community feel safer when dating.
Account registration includes several aspects to this – you need both a credit card, and to have been verified by back office staff to match the person who submitted a photograph.
The following outlines the lifecycle of account statuses as an application progresses,

Submitted

Users must enter their details together and then take a photo with the selfie camera. They then need to supply a valid credit card details (which match the name they've given), and are initially charged $1.
At this point, the user account is in a Submitted state. The users personal details are kept in a database, with their separate payment details kept in another, more secure database which only our payment applications will access. There will be a unique key linking user record to payment details.
In addition, a Skype account will be created on their behalf. This will be a unique key "_Glinda_XXXXXX" account. We don't want to build our own communications channel, so are building on top of Skype. Our application will provide some throttling on communications.

Part Verified

Within 48 hours, one of our back office staff will video conference the applicant. They will hold a brief conversation using the selfie camera. Their goal is to confirm the applicant is real, and matches the photograph provided. This video conversation will be recorded, and stored in a video specific database with a unique key. The back office operator will record the unique video key at time of registration.
If the back office operator is satisfied that they have spoken to the person who submitted the application matches the person they spoke to the account is Part-Verified. Otherwise it will be set to either Resubmit if there are issues with the photo or Suspended if fraud is suspected.
The video chat uses a Skype channel to carry the conversation, but the call is launched through our Glinda app.

Fully Verified

Once an account is Part-Verified, a second admin user should review the account and the conversation, and once satisfied can make the account Verified. If they're not satisfied, they can return to either Submitted or Suspended.
A user can choose to also add a new profile photo, which sets the account to New Photo.
This user has to be a different admin to the one who performed the Part-Verified process in line with our four eyes policy.
Only Verified accounts can use the dating applications.

Suspended

If the account is considered fraudulent or it's felt a user has broken the Glinda code of conduct, their account can be suspended by Glinda admin staff. A note will be made against the card details supplied so it cannot be used to create a new account.

Resubmit Required

If the Glinda admin is not satisfied that the user she's video calling relates to the photo submitted, or the photo is of poor quality, they can set the account to Resubmit.
Next time the user log in with the mobile application, they are taken to the selfie page to retake their photo. Once submitted, their account is set back to Submitted.

Payment Overdue

The account is charged an admin fee every 30 days. If this payment fails, the account is moved into Overdue Payment, and they're unable to continue dating services until payment is received.

On Hold

The user can voluntarily put their account on hold. This takes effect the next time payment is due on the account, where instead of being charged, the account is moved from "verified" to "on hold". They can removed this at any time, but will have to be immediately charged an account fee.

Dormant

A Verified user can toggle their account between Verified and Dormant. Dormant simply makes clear they're not interested in dating at the moment.

New Photo Added

If the user wants to submit a new photo, it is taken out of 'Verified' mode and moved into 'New Photo Added'. They are taken to the 'Take My Picture' page, and a new photo taken.
The Glinda admin can review this picture versus the old one, and if satisfied update the photo and revert the account to Verified.
The user can choose to cancel 'New Photo Added' in which case their account will revert to their old profile picture.

Logging On

Registration automatic log on

After a user has successfully submitted their username and password from a phone, they are automatically logged into Glinda with their credentials.
As part of the submission process, details of the mobile phone used are sent as part of the registration process. The phone becomes locked to the account, and a new account cannot be used on this device.
This is to reduce people from using one device for multiple accounts, something which is associated with fraud.
If a user downloads the app on the phone, and tries to go to registration, a check will be performed, and they will receive a warning message 'It looks like this device has been previously registered for an account. Welcome back!'.

Log on to a device registered to another user

If a user attempts to log on to a device which is already registered to another user, an error message will be raised, and they will not be allowed to log on.

Logging out

The user can log out of the app or webpage at any time.

Log on to new device with credentials

If the user logs into an existing account on a new device, that device is also locked to the user account. A user account can have a relationship to multiple devices.

Log on to a web page

When logging into the web page, the functionality available is limited, in this case, no form of device matching occurs.

Customer log on support

If the user has forgotten either their username or password, they can enter the email address they used to register, either their username, or a 1-hour, one-use-only password will be emailed to them.
The login service will only allow 3 incorrect logins to an account within an hour.
Most of this behaviour is considered industry-standard.

Dating services

The Glinda app requires permissions for GPS. We poll devices hourly and record their location – these are kept in a table with location, time, and people's unique key only. We only record current location, no historical record will be kept.
A user can refresh their location at any time.
Using the app, a user perform a search and can select the radius of people they're interested in, the system will then create a list of users who match sexual preference in that radius.
Every user has a list of user IDs for which they're part-matched, matched, mis-matched, blocking.
The user will be shown other users profiles which match criteria (including the rules below).

Part-matched

A user shows an interest in a profile when they swipe left. At this point, they become part-matched.

The profile will then no longer be visible to them when they do a search, however right now they can't make contact.

Matched

If the other party also has swiped left on this users, the couple is matched. They have both shown an interest in each other. It's only at this point that communications can occur between couples on the Glinda app.

Mis-matched

If a user isn't interested in a profile, they swipe right. We call this a mis-match, and record the user ID and date occurred together with a count.
We won't show that profile again to the user for 2 days. If a user swipes right 3 times, we'll but the profile under blocking.

Blocking

If a user has swiped right a profile 3 times, we put it to blocking. The user will not see that profile every again. Likewise, the person with the rejected profile will not be able to see the other users profile from dating searches.
In addition, if a user is uncomfortable with someone they're matched to, they can select to block them. Users will be allowed to report if they feel they've had an interaction which has unsettled them, including a reason.

Use of Skype communications

Two users who are matched to each other can exchange communications. We use anonymised Skype accounts to allow this to occur. We also filter requests in our app service layer to make sure that only communication requests from either admins or matched users are allowed through.
Use of audio/video will only be allowed for admins. They must use video for part-verified confirmation. They can contact users when investigating any reported incidents. These interactions will be recorded.
Matched users are only allowed to interact by text or photo exchange. Each exchange will be recorded in a message table on the database including,

- Datetime
- From user
- To user
- Content

Admins will be able to retrieve conversations only if a user has reported another users actions.
Glinda will not use the Skype application on mobile devices, but will utilise the channel. Each Glinda account will use a secret, anonymous Skype account not normally available on Skype. People on Skype will not be able to make contact as users are only signed in via the Glinda application, and the app layer will not allow chats to get through which are not from admins or are a matched user.

Suggest meetup

We keep a list of nearby public venues which are gay and lesbian friendly and are located nearby.
The database keeps details of their name, location and a website link.
In future we might look to having these places fund for top selection places.

AI filter for photos sent

When a photo is sent between matched users, we will run the photo through the Google Cloud Vision API. If this returns that the picture was obscene (containing genitalia), the photo will not be sent, and the sender warned our obscenity filter.
We expect to bring in a contractor used to working with this sort of material to deal with this aspect of behaviour, and limit exposure of indecent material to staff. We will also respect staffs wishes not to work or view material in this area.
We expect the fine tuning of this to take a while, but marketing expects this to be a key feature to promote safety online.

Channels

Mobile application

The mobile application will be the primary channel for users of Glinda, and available on iOS and Play stores. The application will require the phone to be iOS 10 or Android KitKat and beyond.
It will require permissions to,

- Camera
- Microphone
- GPS location

Public Website

Most interaction on Glinda will be done via the mobile application, however we will maintain a static website to talk about the service we offer and frequently asked questions.
Users will be able to log in, but have a limited set of functions they can perform,

- Manage my account, including changing password
- Toggle account between verified and either ‘on hold’ or 'dormant' modes
- Edit their payment details

Admin site

An admin site will be supported, which will allow selected users to perform admin roles including,

- Trigger Skype call with users
- Change user state to part-verified, verified, suspended
- View users who have been reported
- Review conversations of a user who has been reported

The admin site will be locked so that it can only be accessed by an IP which relates to being on-site.

Billing

Glinda will use the dcPay payment engine to process payments. There will be an invoice table which includes a list of payment transaction. Only verified accounts will be charged monthly. If a payment fails, this will be recorded in the database, and the users account set to “overdue payment”.

Architecture

The architecture will be maintained in-house by the Glinda ops team. A diagram of this is provided in Appendix A.
The application aims to be highly available using multiple nodes in the database, application and web tiers.

The admin tier will only be single mode.

AppService tier

The app service tier will contain the business rules for Glinda, and also act as a webservice conduit between,

- Skype and both the Admin site and Mobile app
- Run payments through dcPay
- Bring through map data via Google maps
- Provide filtered information as required and authorised to the web tier

This architecture layer is usually called the application layer, but to avoid confusion between the application service layer in the architecture and the mobile application itself, we will refer to it as the app service to differentiate.

Web tier

The web tier will create pages from information and authorisations provided by the app tier for consumption on the admin site or user pages

Database tier

Data is replicated to the primary and secondary database.

Drive storage

Video and audio files of admin calls are stored as flat files within the drive storage, which is backed up hourly. Admins will have read-only access to this area.

High availability

Users will be load balanced across nodes on the web and app server as required. If the node a user is on suffers an outage, they will lose their session with different expected results according to where they're using. Users on the web page or admin site will lose their session, and will have to log in again. They might lose some work.
Users on the mobile application whose app node has gone will have their session moved to the other app node. We expect minimal disruption.

Backups

Each tier will have a backup drive which will be triggered hourly. Backup processes should not impact performance. Loss of up to an hour's data during an incident is considered acceptable.
In the event of a database outage, a process will perform a difference check on the primary and secondary database, copying and missing records onto the other database.
It's a requirement that the app or web node can be restored from backup in under an hour.

Performance

The system should be able to support,

- 90% of users should have their registration processed (including payment transaction and photo storage) within 30 seconds with a load of 1,000 concurrent users
- 95% of users should have their messages to a matched user delivered within 5 seconds under a load of 10,000 concurrent users

- 90% of users should be able to perform a search of nearby profiles within 20 seconds under a load of 5,000 concurrent users

Monitoring and alerts

Every physical server (equating to every node) will have monitoring enabled on it. This will allow the ops team to keep tabs on the system.

Monitoring

The following items will be monitored and available to ops staff when required,

- CPU usage
- Memory
- Disk free
- Network traffic – including on the app server separate traffic to web server, Skype, Mobile Phone, dcPay and Google Maps traffic
- Heartbeat

Heartbeat is a repeated ping to the node IP that is performed each minute to confirm it's still working.

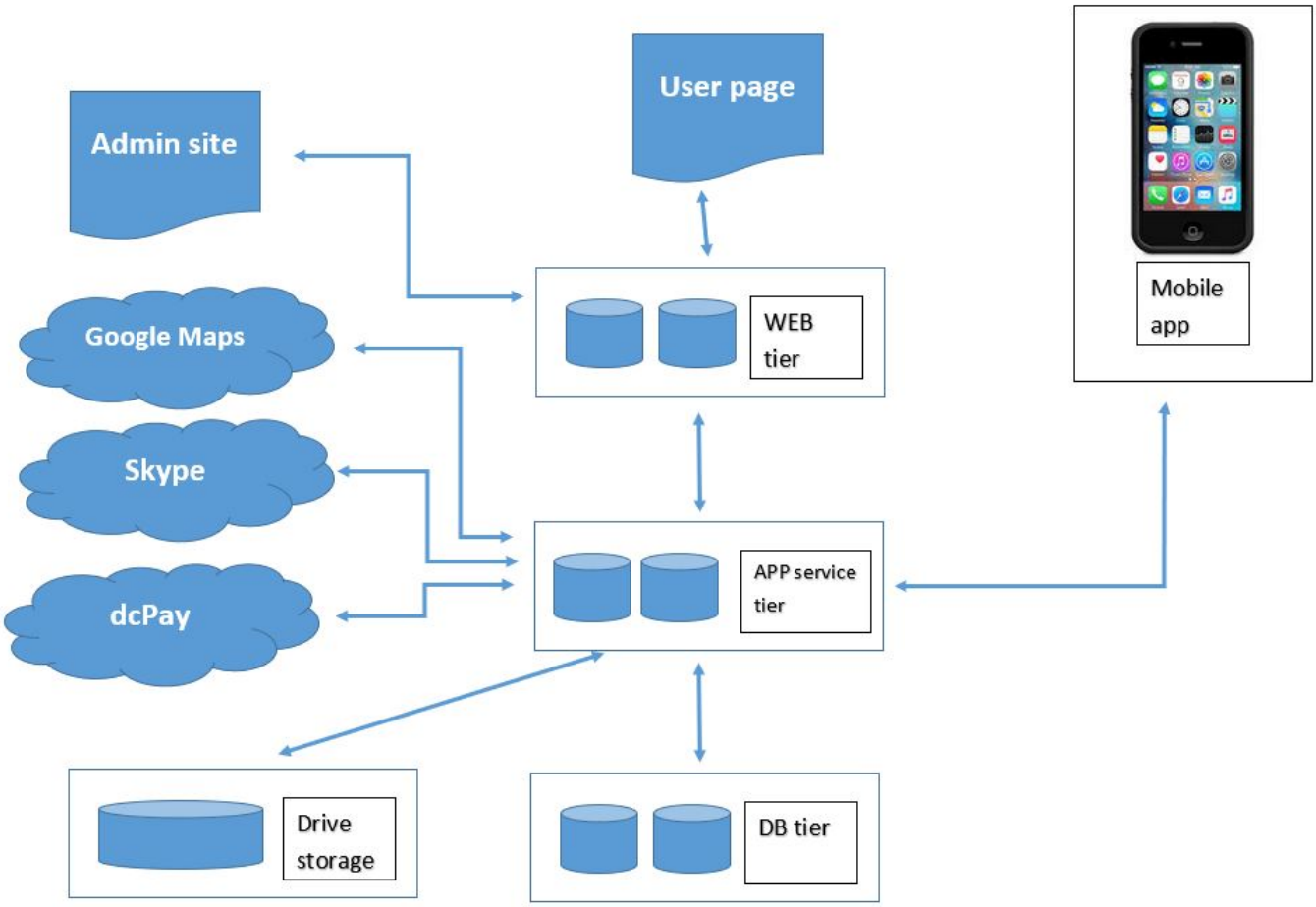
Alerts

The ops team can set thresholds for red and amber alerts for any monitored attribute. When these thresholds are exceeded, an email alert will be triggered to the ops staff informing them. This email alert occurs just once, and will not be repeated if that state remains.
These settings will be adjusted by ops as they go and learn more about the system. It's expected an amber alert will occur if CPU usages is at 90%, with a red alert if CPU usage goes beyond 95%
Likewise if a node heartbeat is zero for 5 minutes it should raise an amber alert, with this raised to a red alert if still down after 15 minutes.

Auditing

All significant actions will be audited, with an entry created in the audit log table.
The initial expected audits are covered in Appendix C. It is expected they will be expanded with the design, and new audits added as needed.
It's important to note – we'll audit the location someone uses dating services from, but we'll not provide historical passive tracking of where users are from our hourly poll. This needs to be communicated to users, and marketing is working on it to make them feel secure and not being spied on.
We do monitor more details on what our admins are doing, as we need to be more accountable.

APPENDIX A - Architecture Diagram



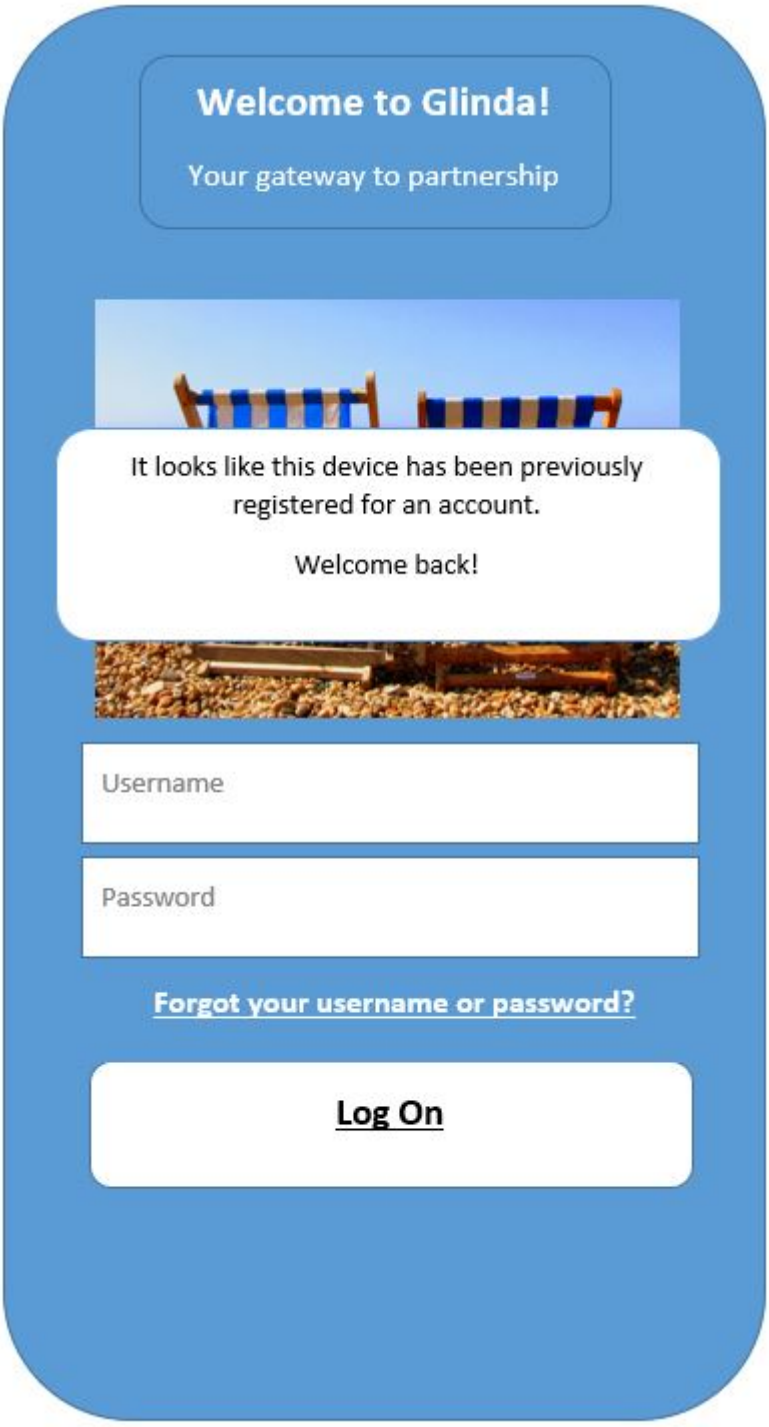
APPENDIX B - Screen Mock Ups

The following are included as examples of key screens, not all screens have been provided.

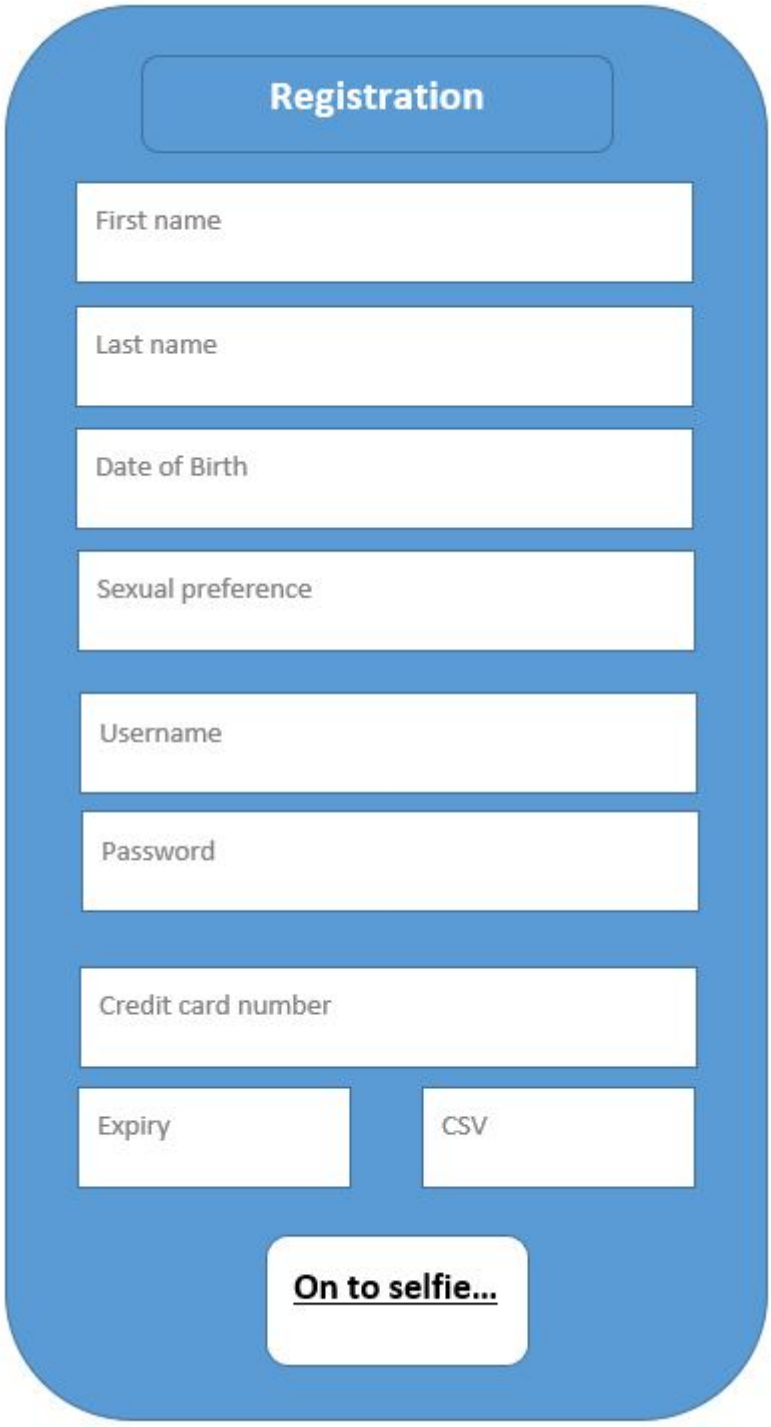
Welcome Page

Previously Registered Page

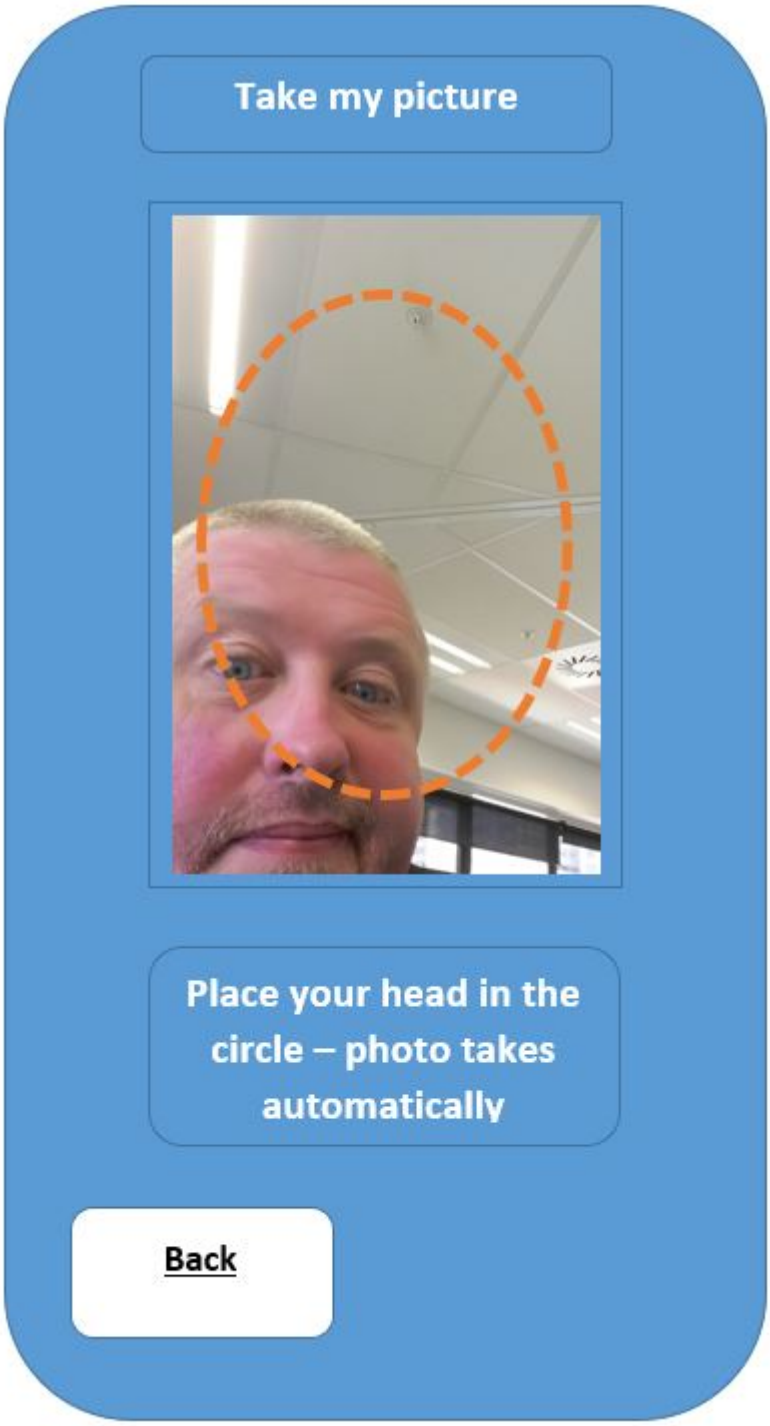
Notice how the Registration button has been removed.



Registration Page



Take My Picture Page



Review My Picture Page

Admin Video Call Page

This runs a Skype video call within our mobile application.

Find A Match Page

This page will use the location provided by the mobile phone, and overlay maps provided by Google maps service.

Profile Page

Match Chat Page

APPENDIX C - Auditing

Below is a table of expected results. Key field descriptions,

- ID is a number to categorise the audit number
- UserID is the unique identifier of the user who owns the account
- Body is the descriptor for the audit
- MatchID is the unique identified of a second user – typically that the main actor is interacting with through viewing profile or matching
- AdminID is only filled in for functions where an admin is looking up a user

ID	UserID	Body	MatchID	AdminID
101	N/A	Registration initiated	N/A	N/A
102	N/A	Selfie initiated	N/A	N/A
103	N/A	Photo taken	N/A	N/A
104	N/A	Review my picture	N/A	N/A
105	N/A	Retake photo	N/A	N/A
106	N/A	Submit registration	N/A	N/A
201	N/A	Registration payment successful	N/A	N/A
202	N/A	Registration payment failed – dcPay down	N/A	N/A
203	N/A	Registration payment failed – incorrect card details	N/A	N/A
204	N/A	Registration payment failed – insufficient funds	N/A	N/A
211	YES	Monthly payment failed – dcPay down	N/A	N/A
212	YES	Monthly payment	N/A	N/A

		failed – incorrect card details		
212	YES	Monthly payment failed – insufficient funds	N/A	N/A
220	YES	User has changed payment details	N/A	N/A
300	YES	Device ID ####### locked to user account	N/A	N/A
301	YES	User logged into app – automatic registration	N/A	N/A
302	YES	User logged into app – logged in via log on page	N/A	N/A
303	YES	User logged into webpage	N/A	N/A
310	YES	Login attempted, user ID relates to no known user	N/A	N/A
320	YES	Incorrect login	N/A	N/A
321	YES	Account locked for one hour after 3 consecutive incorrect logins	N/A	N/A
322	YES	Repeated login attempt during lock out	N/A	N/A
330	YES	User has attempted to login to a device locked to another user	N/A	N/A
1000	YES	User account created, state SUBMITTED.	N/A	N/A

1001	YES	User unique Skype account created ID #####	N/A	N/A
1002	YES	User account PART VERIFIED	N/A	YES
1003	YES	User account FULLY VERIFIED	N/A	YES
1004	YES	User account SUSPENDED reason FRAUD	N/A	YES
1005	YES	User account SUSPENDED reason ABUSIVE BEHAVIOUR	N/A	YES
1006	YES	User account RESUBMIT REQUIRED	N/A	YES
1007	YES	User account OVERDUE PAYMENT	N/A	N/A
1008	YES	User account ON HOLD	N/A	N/A
1009	YES	User account DORMANT	N/A	N/A
2000	YES	User initiated dating services match from location ####	N/A	N/A
2001	YES	User initiated dating services match – location not found	N/A	N/A
2010	YES	User shown member profile	N/A	N/A
2011	YES	User has shown interest in other user	YES	N/A
2012	YES	User has shown disinterest in other user	YES	N/A
2013	YES	User has chosen to block other user	YES	N/A

2020	YES	Full match has occurred between users	YES	N/A
2100	YES	Skype message set to other user	YES	N/A
3001	N/A	Admin login from IP ##.##.##.##	N/A	YES
3002	YES	Admin has looked up user	N/A	YES
3003	YES	Admin initiates Skype call	N/A	YES
3004	YES	Skype call ends	N/A	YES
3005	YES	Skype call fails	N/A	YES
3006	YES	Skype call unanswered	N/A	YES
3005	YES	Video chat stored as file ID ####	N/A	YES

Poza reprezentativa:

SEE LESS

+ ADD CHECKLIST

+ Add relationship

Attachments

You created this task — Nov 13 at 1:05 am

You assigned to: You — Nov 13 at 1:05 am

You uploaded 12 files

Nov 13 at 2:11 pm

image.png

image.png

image.png

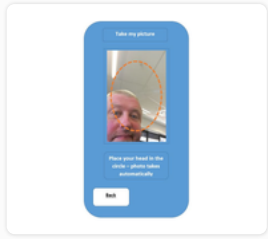


image.png

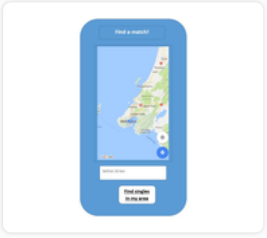


image.png

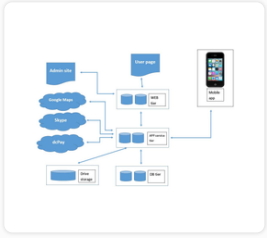


image.png

image.png

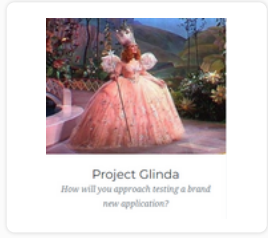


image.png

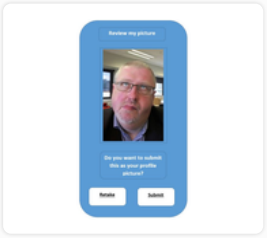


image.png

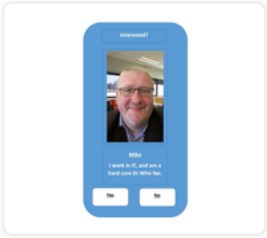


image.png

image.png

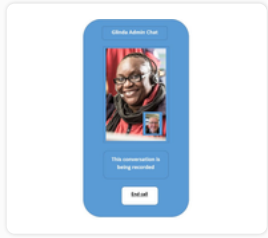


image.png

You changed status from Backlog to Complete

Nov 13 at 7:17 pm