Spring 2015

Homesafe: A mobile application utilizing encryption and access control

Kenneth Trumpoldt
James Madison University

Homesafe: A Mobile Application Utilizing Encryption and Access Control

---

An Honors Program Project Presented to

the Faculty of the Undergraduate

College of Integrated Science and Engineering

James Madison University

---

by Kenneth Michael Trumpoldt

May 2015

Accepted by the faculty of the Department of Computer Science, James Madison University, in partial fulfillment of the requirements for the Honors Program.

FACULTY COMMITTEE:

____

Project Advisor: Michael Kirkpatrick, Ph.D.
Assistant Professor, Department of Computer Science

____

Reader: Chris Mayfield, Ph.D.
Assistant Professor, Department of Computer Science

____

Reader: John Burgess, MFA
Assistant Professor, School of Theatre and Dance

HONORS PROGRAM APPROVAL:

____

Philip Frana, Ph.D.,
Interim Director, Honors Program

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at the Computer Science External Advisory Group Annual Meeting on 4/17 .

Table of Contents

List of Figures

Figures

Acknowledgements Page

I would like to thank Dr. Michael Kirkpatrick for acting as my advisor on this project for two semesters. He dedicated an hour of his time every week to meetings that ensured my understandings of new concepts were correct and that the project was moving forward. He suggested the inclusion of cyber security features within the application. These features are vital to the success of an application that may contain sensitive child information. He also inspired some of the graphical user interface designs that led to high usability.

Abstract

Our society is becoming more virtual and mobile everyday. The purpose of this application is to transform a physical card system into a virtual card system that meets the demands of a technologically-oriented society. Parents will be able to create their own child identification cards more quickly and cost efficiently. Cards can be easily edited instead of having to order an updated replacement. Immediate and frequent alteration of cards allows for information to be more accurate. Cards can be shared globally and instantly via the Internet or shared connections such as Bluetooth. The fast access to and virtual duplication of identification cards lends itself to effective emergency situations and convenience. However, risks in cyber security are attached to the introduction of identification cards to the virtual world. Potential threats must be evaluated and proactively minimized. Cards may be re-distributed undesirably. Sensitive information may be read by those who have malicious intentions. To protect sensitive information, cards can be encrypted with keys to protect sensitive data for improved security. Roles can also be assigned to users to determine who should have access to what sections of data. While the virtualization of child identification cards is much more efficient in many aspects, it is also much more dangerous if exercised without caution. Homesafe was developed by taking all of these factors into consideration. Its graphical user interfaces were designed for simplicity and convenience. Bluetooth has been implemented for remote connection with other devices. Selective encryption using keys and role based access control has been integrated into the application. It is a project with much potential in virtualizing the IDK business safely and efficiently.

Homesafe Purpose

Ident-A-Kid Services of America (IDK) creates child identification cards for kids from preschool to middle school (ages 0-15). These cards include information such as date of birth, address, parent's names, hair color, eye color, height, weight, safety tips, and, most importantly, fingerprints. These cards can act as tools in an emergency situation that can pass on information to police and emergency responders quickly.

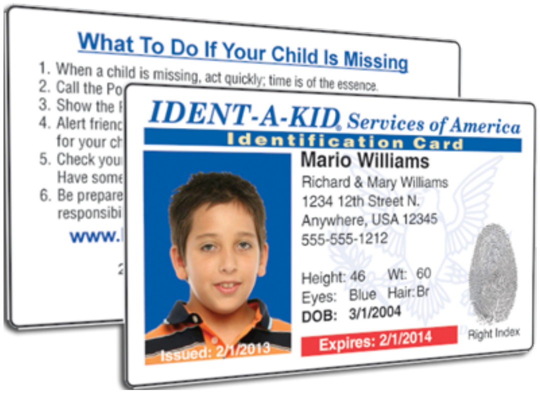


Figure 1 - Sample Ident-A-Kid Card

This business could become more effective and convenient through the creation of a mobile app. This would virtually store all of the information the paper version stores and would also include several new features to expand its purpose.

The virtualization of the Ident-A-Kid Service would fix many existing problems with the physical cards. The Ident-A-Kid card has a limited reach leaving out many families who attend schools that were not solicited by IDK. With the introduction of a mobile application anyone could create their own child identification cards at any time and any location. This removes limitations of potential customers. A virtual card cannot be lost unless deleted from memory. Physical cards become outdated very quickly whereas a virtual card can be easily updated within seconds. Physical cards are not efficient in emergencies. The information can only be shared with one person within physical reach. A virtual card can be instantly shared via Bluetooth or the Internet with any amount of people at any distance. With physical cards any child who does not attend a school where the IDK franchise has visited is left out. Virtual cards can be created immediately under any circumstances. Physical cards are also limited by physical space. This means that certain information may have to be left out. Virtual space is much more dynamic and could host a seemingly infinite amount of information about a child. Virtualization can also add an extra layer of security. Virtual cards can be encrypted using many different methods and access to the card by non parent users can be managed. Overall the concept of a mobile application designed to host Ident-A-Kid cards could provide services for a much larger population, provide up-to-date information in the case of a non emergency or emergency situation, and make the ownership of a child identification card more secure.

Homesafe Usability

Homesafe has been designed with usability as a priority to compliment the convenience of having a virtual card. Graphical user interfaces (GUI) have ease of use and strong learnability. Activities are constructed to minimize clicks and time necessary to achieve actions desired by the user.

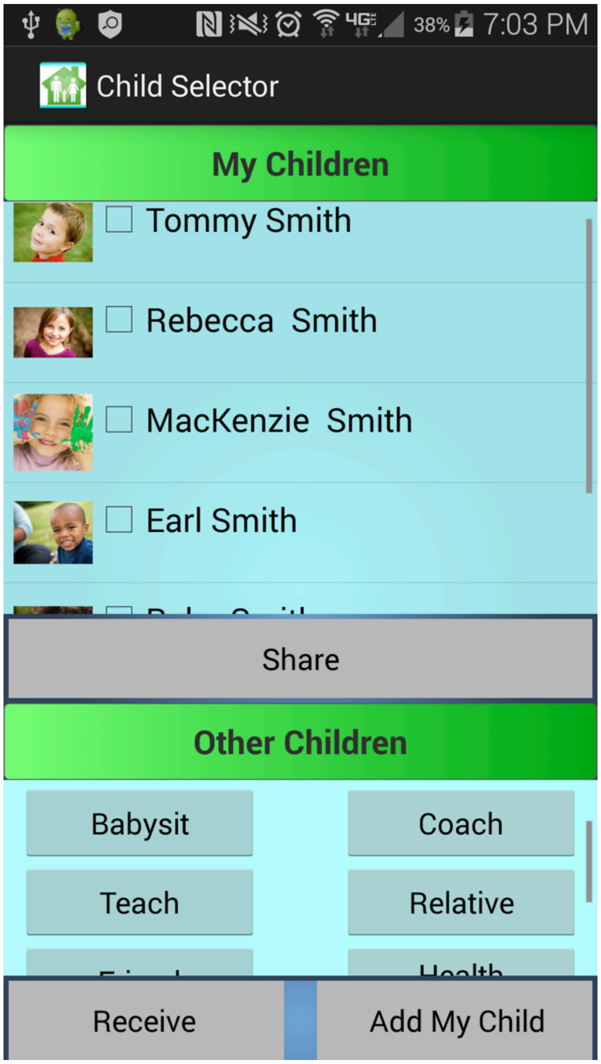


Figure 2 - Child Selector Activity of Homesafe

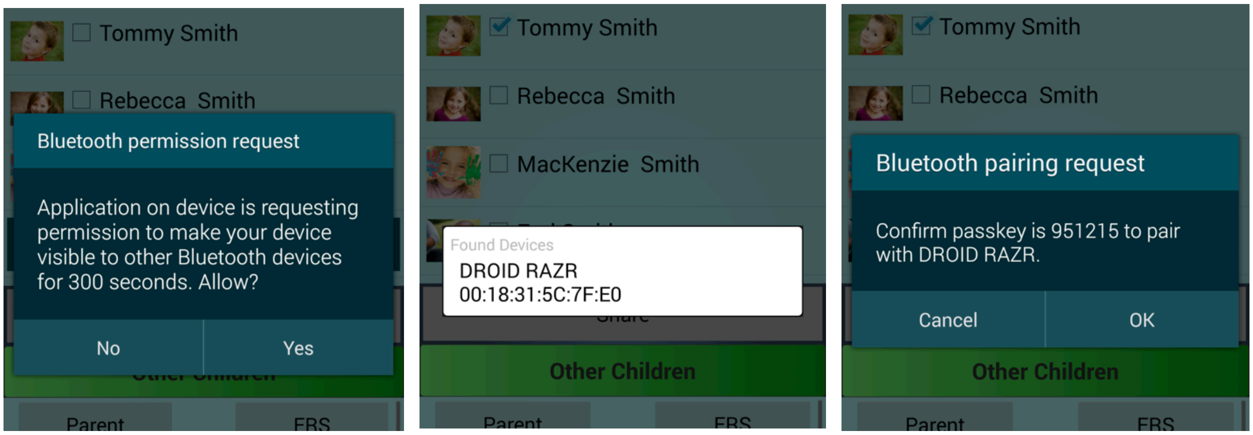
Figure 2 is an example of one GUI of Homesafe. From this one user interface many actions can be sensibly performed. Child identification cards can be viewed by clicking the name of the child. When the activity is loaded the parent's children are listed by default. Different child lists can be displayed by clicking a button labeled with the respective category below the ‘Other Children’ text. This view is scrollable so that all buttons can be viewed regardless of the view size on the user’s phone. The checkboxes next to the children’s picture can be selected to allow the ‘Share’ button to send one or many virtual cards with one click. The ‘Receive’ button allows users to establish a Bluetooth connection with other users and receive virtual cards that they require access to. The ‘Add My Child’ button allows parents to create a virtual card for their child which can then be managed. Ultimately this single user interface allows complete management of all identification cards created by the user and identification cards received from other users that they connect with.

The child identification cards are contained in a view supported by a list adapter. Every time a new child card is added to storage by the application it is added to a resizable child list. The list adapter then takes the child list as an argument to set itself. The view is then set to the adapter and displays the child cards in the child list to the user. When the child category is changed the adapter sets itself to a different child list and the view changes accordingly by setting itself to the new adapter. If all of the child cards imported from the child list do not fit within the view, the List View will become scrollable so that all cards can be accessed.

There are additional Homesafe features that could be implemented for greater usability. Some examples involving the Child Selector Activity include sorting the List View alphabetically and integrating a search feature that can search for names by matching typed keywords. The search feature would be helpful for large child lists that become difficult to manage. Another example involves the process required to log in to the user’s Homesafe application. Currently the user must log in with a username and password combination. In an emergency situation this can be a slow process or the login details may be forgotten. Possible solutions that utilize fast access would include thumbprint scanning or swiping a screen pattern pre-set by the user.

Bluetooth

Homesafe implements Bluetooth to wirelessly exchange data between devices that are sending and receiving child identification cards. This process is initiated when one user clicks a ‘Share’ button to share a card and another user hits ‘Receive’ to receive a card. Both users will be prompted to turn on Bluetooth if Bluetooth was not already enabled. The device with the intent to share a card will enter device discovery mode. This user will be presented with a List View of all devices in range that have Bluetooth enabled and are discoverable. The device with the intent to receive a virtual card will display a prompt to the user asking them if it is ok if the device is made discoverable for a certain amount of time. In Homesafe the time is set to 300 seconds. If the user selects “Yes” the device will enable discoverability. Once the device is discoverable it will appear on the List View of the sending device. The sender will then click the device name on the List View that they wish to pair to. At this point both users will be presented with a passkey. If the two passkeys match the users are assured that the connection to be established will be between those two devices. When both devices are paired the connection is now ready to be created.



Bluetooth permission request

Application on device is requesting permission to make your device visible to other Bluetooth devices for 300 seconds. Allow?

Found Devices

DROID RAZR
00:18:31:5C:7F:E0

Bluetooth pairing request

Confirm passkey is 951215 to pair with DROID RAZR.

Figure 3 – The process of pairing two devices within Homesafe

In order to create a connection between two devices, both the server-side and client-side mechanisms must be implemented, because one device must open a server socket and the other one must initiate the connection. In Homesafe the receiving device was chosen to act as the server by holding an open BluetoothServerSocket. This socket listens for incoming connection requests among paired devices and provides a BluetoothSocket when a connection is accepted. In Homesafe the sending device acts as the client. The client is more proactive than the server in the sense that it attempts to initiate a connection while the server waits to receive a connection. The sending device obtains a BluetoothDevice object that represents the receiving device. This object is then used to acquire the BluetoothSocket that the receiving device was holding. The BluetoothSocket (a connection point) allows an application to exchange data with another Bluetooth device via InputStream and OutputStream. Once both devices obtain this socket they are ready to send and receive data between each other. In Homesafe the thread that was waiting to accept a connection on the receiving device and the thread that proactively tried to connect on the sending device are both sent to the same handler. Both threads are passed to the handler with an intent that will allow the handler to distinguish which thread is to do which job. The sending device will use this thread to open an OutputStream on the shared BluetoothSocket and write bytes to the stream using a buffer. The receiving device will use this thread to read bytes from buffer on the InputStream on the shared BluetoothSocket. Data transfer is complete when the receiving device has read all bytes from the buffer.

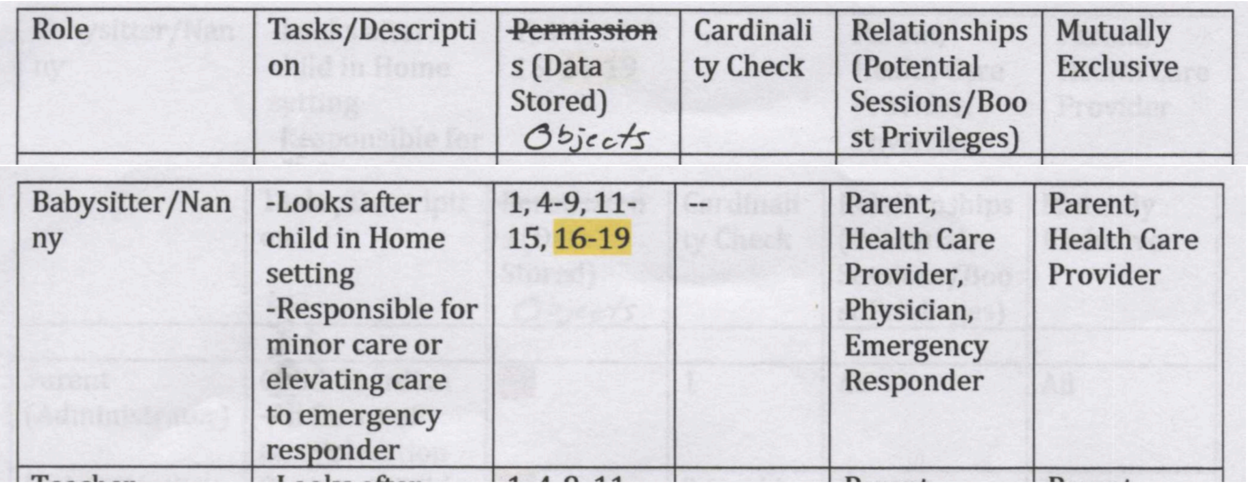
Bluetooth allows for convenient transfer of virtual cards within Homesafe. Bluetooth capability is present in almost all (if not all) modern smartphones meaning users can always be connected. There is no need for Internet access or phone service to take advantage of a

Bluetooth connection which lends itself to high availability. This is especially vital if information needs to be transferred in an emergency situation and standard cellular services are not available.

Homesafe Cyber Security

While the virtualization of the IDK service into a mobile application is both convenient and efficient, it introduces new threats present in the cyber world. Homesafe must not only provide a service but implement cyber security measures to safeguard that service. The goal of cyber security is to protect data both in transit and at rest. For Homesafe this translates to protecting the confidentiality of child information that is in storage on the phone and child information that is being transferred over connections such as Bluetooth. Potential threats include those trying to intercept information being sent from one device to another, untrusted users who may use the information maliciously, or thieves who have stolen the device. Homesafe security is largely accomplished through the use of Role Based Access Control (RBAC) and encryption.

Child identification cards contain personal information. In some cases the information may be sensitive. Sensitive information may include the fingerprint on the card, medical information, home address, special needs, and more. Therefore it is crucial that this information is only distributed on a need-to-know basis. This means that access to information should only be given to a person if it is necessary for their role or position. If the information is outside the scope of their role access should be denied. To achieve this within Homesafe, users need to be assigned roles to the children contained in their phone. For example when creating a card for their own child the user is assigned the parent role. When sending their child's card to another user the parent must assign a role to that user such as 'babysitter' or 'teacher'. The user receiving the card will only have access to the information that a babysitter or teacher should. Once all roles and information pertinent to each role has been decided access needs to be controlled to protect confidentiality.

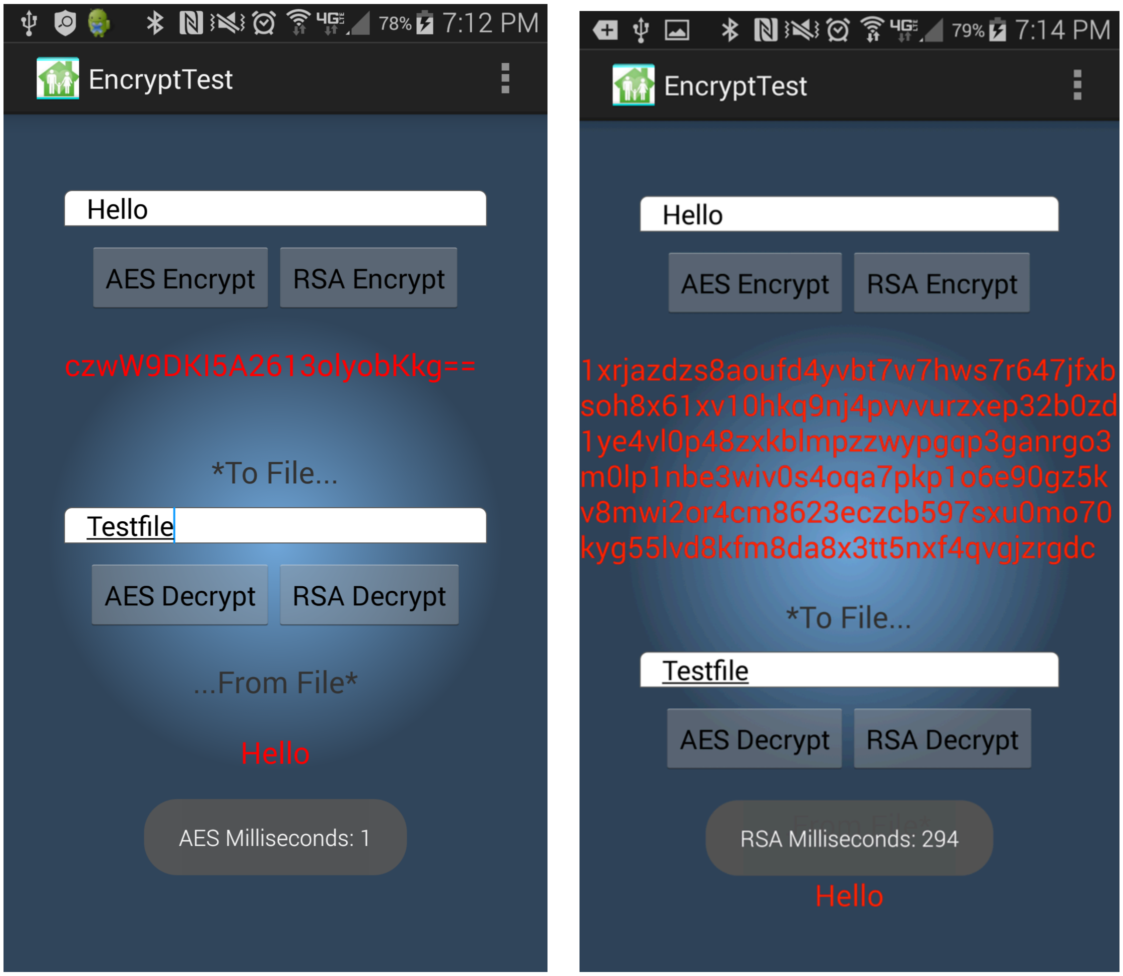


Role	Tasks/Description	~~Permission~~s (Data Stored) Objects	Cardinality Check	Relationships (Potential Sessions/Boost Privileges)	Mutually Exclusive
Babysitter/Nanny	-Looks after child in Home setting -Responsible for minor care or elevating care to emergency responder	1, 4-9, 11-15, 16-19	--	Parent, Health Care Provider, Physician, Emergency Responder	Parent, Health Care Provider

Figure 4 - Sections of documents representing roles and the information they should be able to access using 'Babysitter' as an example. Numbers underneath "Objects" refer to information such as age or date of birth. Highlighted numbers are potentially sensitive. The cardinality check ensures integrity.

Protecting the data at rest (child cards stored on a device) is as simple as requiring a username and password combination or any other modern security feature, such as a fingerprint scan, for a user to log into their application. When data is in transit protecting the confidentiality of information becomes much more difficult. It would be easy and straightforward if the only type of data transfer was from a parent to another user. Then only the information needed by that user would be sent. However this is not the case. Using an emergency situation as an example, what happens when the emergency respondent cannot receive the information they need because the babysitter did not need it and did not receive it? The RBAC model now comes into play. The babysitter must be able to receive all of the information on the card but not be given access to certain information based on their role. The emergency responder can then receive all of the information on the card and is respectively given access to what information they need to know to do their job successfully. Using RBAC all users are receiving all of the information but what information they can actually access or view is limited. Therefore it is crucial that access by controlled or enforced by some mechanism. Homesafe uses encryption as the mechanism for confidentiality and RBAC.

Encryption compliments RBAC by encoding messages or information in such a way that only authorized users can read it. The messages or information are encrypted using encryption algorithms. In most encryption schemes these algorithms generate encryption keys that are responsible for encoding and decoding the information. These encryption keys can be symmetric, meaning the same key used to encrypt the message is also used to decrypt it, or asymmetric, meaning separate keys are used to encrypt and decrypt the message. Generally in asymmetric encryption one key is made public and can be used by anyone to encrypt messages but only the authorized reader possesses the private key to decrypt the message. The developer version of Homesafe has a proof of concept activity that can encrypt and decrypt messages using AES (symmetric) encryption and RSA (asymmetric) encryption to demonstrate what happens to the child information in transit. For both encryption types a message is entered, encrypted, and written to a file. To decrypt the message the process is reversed. The encrypted message is read from the selected file, decrypted using either the symmetric or asymmetric key, and then displayed in the text view. RSA is computationally expensive when compared with AES. This is because RSA algorithms involve very large numbers in encryption and decryption whereas AES can be implemented with simple bit operations. To remedy this computational demand when encrypting large amounts of data, AES encryption can be used to encrypt the data and RSA encryption can be used to encrypt the symmetric AES keys. This approach is a basic method of encryption and utilizes the heightened security of RSA encryption without sacrificing fast execution time. This approach would be most effective in Homesafe concerning both security and processing time. However the current version of Homesafe only implements hard-coded AES keys that encrypt information and are then transferred to the receiver for decryption.



Hello

```
czwW9DKI5A2613olyobKkg==
```

Testfile

Hello

AES Milliseconds: 1

Hello

```
1xrjazdzs8aoufd4yvbt7w7hws7r647jfxb
soh8x61xv10hkq9nj4pvvvurzxep32b0zd
1ye4vl0p48zxkblmpzzwypgqp3ganrgo3
m0lp1nbe3wiv0s4oqa7pkp1o6e90gz5k
v8mwi2or4cm8623eczcb597sxu0mo70
kyg55lvd8kfm8da8x3tt5nxf4qvgjzrgdc
```

Testfile

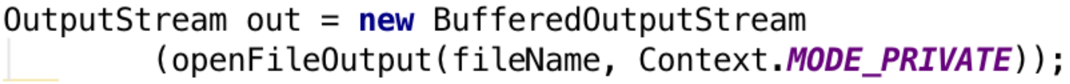
RSA Milliseconds: 294

Hello

Figure 5 – Developer proof of concept activity: AES and RSA encryption and the time needed to generate keys and encrypt comparison

Storing Data with Homesafe

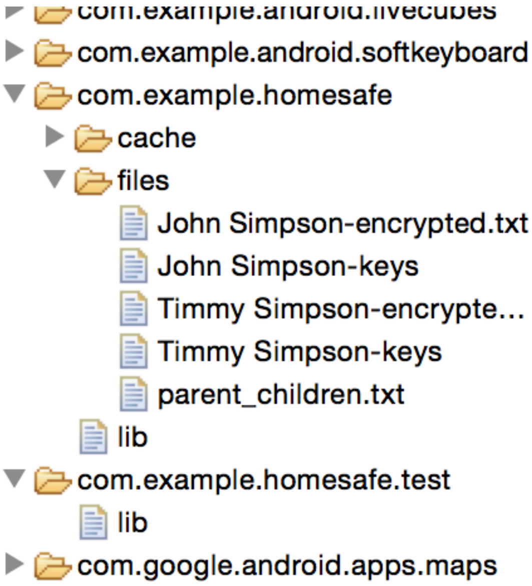
Without the use of the cloud or an online database all data generated by Homesafe must be stored within memory of the device. Android Libraries provide for many methods of storage and access of files in memory. Figure 6 illustrates how OutputStreams are created in Homesafe using the Android 'Context.MODE_PRIVATE' operation to write to files within the scope of the mobile application.



```
OutputStream out = new BufferedOutputStream
        (openFileOutput(fileName, Context.MODE_PRIVATE));
```

Figure 6 - Creating a file in Android within the context of the application

This is most convenient when attempting to read files. Typically a file path must be passed as an argument to find files or directories within devices. For files written within the context of the application only the file name needs to be passed as an argument. All files are stored in the directory of the application itself. Figure 7 is an image of how files are stored on a device running Homesafe.

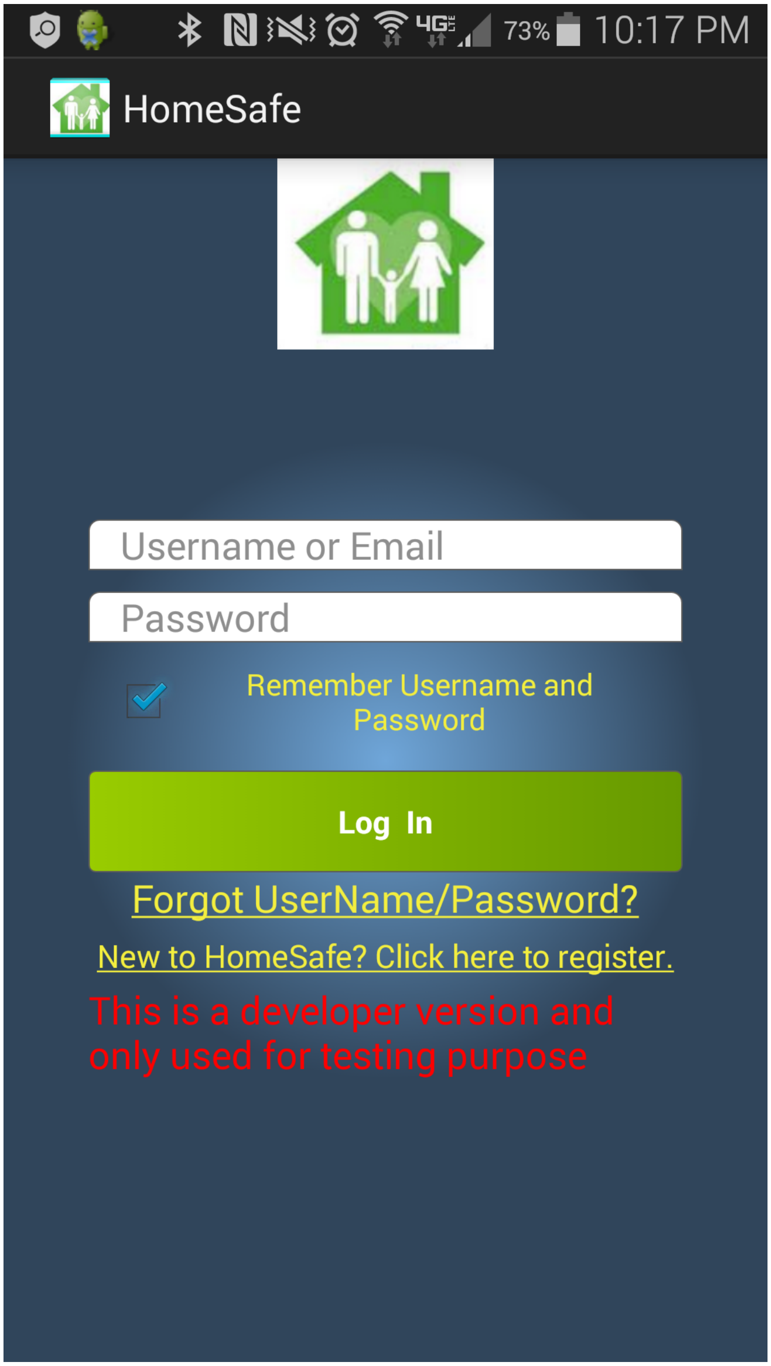


```
▶ com.example.android.livecubes
▶ com.example.android.softkeyboard
▼ com.example.homesafe
    ▶ cache
    ▼ files
          John Simpson-encrypted.txt
          John Simpson-keys
          Timmy Simpson-encrypte...
          Timmy Simpson-keys
          parent_children.txt
      lib
▼ com.example.homesafe.test
      lib
▶ com.google.android.apps.maps
```

Figure 7 - Capture of the device file system using the Android Device Monitor

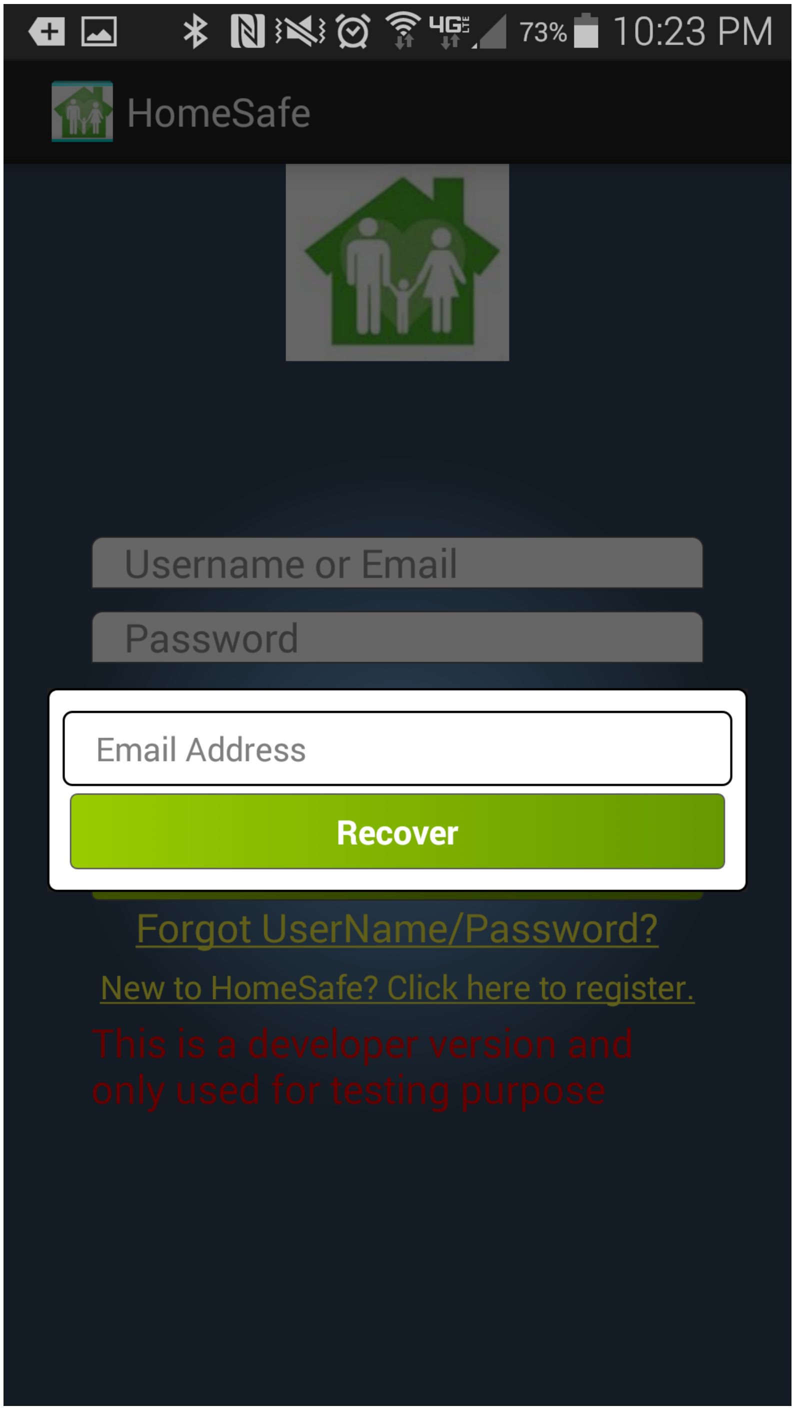
When a child identification card is created or received multiple files are created or modified on the device. The child's name is appended to "-encrypted.txt" and the encrypted text of child information is stored within that file. The child's name is also appended to "-keys" where the AES keys responsible for encrypting and decrypting the information are stored as bytes. Lastly a "_children.txt" file is created or modified with the name of that child. The prefix to this file is the role that the child was assigned to on that device. For example the "parent_children.txt" file holds a list of all child names whom the user is the parent of. If a parent sends a child identification card to a user who is supposed to babysit the child, the child's name would be added to a file named "babysitter_children.txt". These files are important in the Child Selector Activity. When a button is clicked to view children of a certain role the button text is matched with the prefix of the file. An array of child names is then created from the file. This array is then used to retrieve the child information for each child and build the list of children into the List View for selection. Currently the storage of images, for the purpose of managing the child's picture, has not been implemented in Homesafe.

Appendix/Appendices


73%
10:17 PM
HomeSafe
Username or Email
Password
☑ Remember Username and Password
Log In
Forgot UserName/Password?
New to HomeSafe? Click here to register.

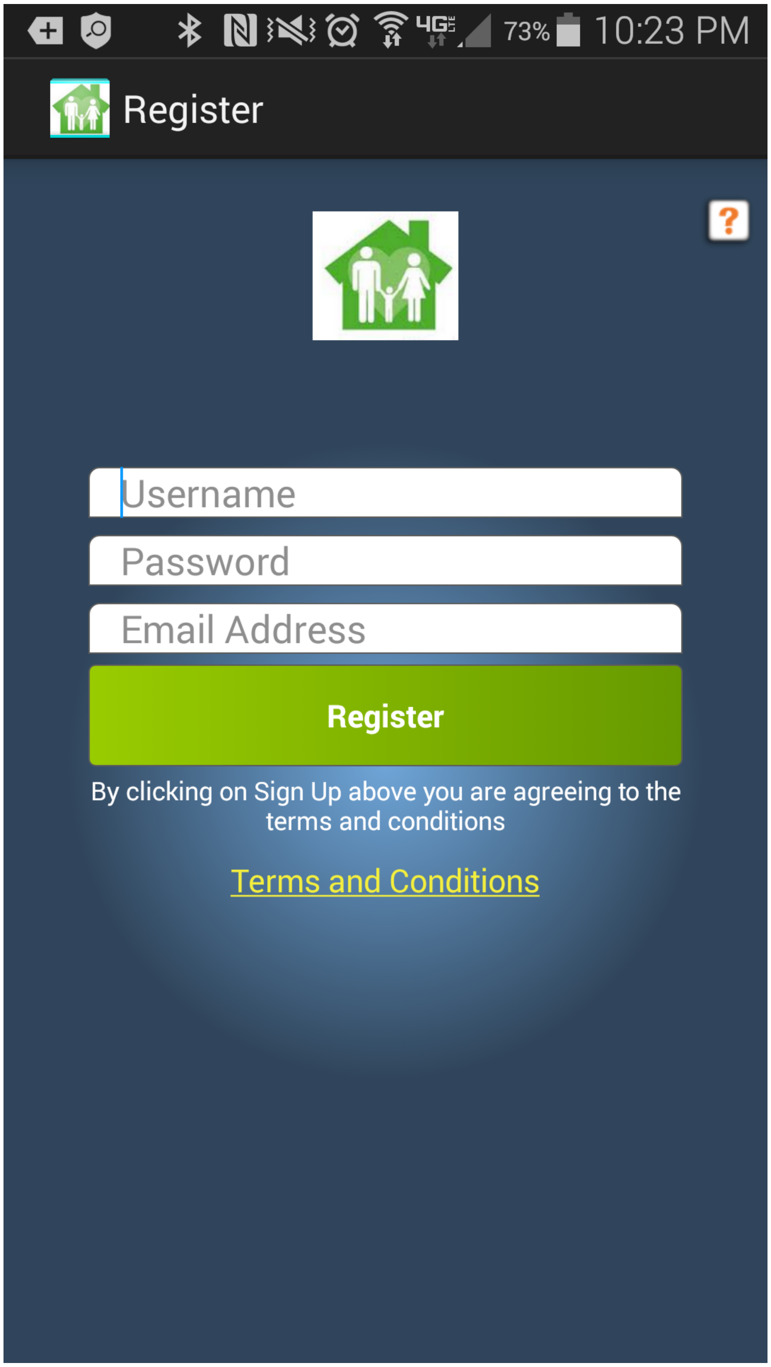
This is a developer version and only used for testing purpose

Layout 1 - Main Login Screen Activity


73%
10:23 PM
HomeSafe
Username or Email
Password
Email Address
Recover
Forgot UserName/Password?
New to HomeSafe? Click here to register.

This is a developer version and only used for testing purpose

Layout 2 - Recover login details dialog box



Username

Password

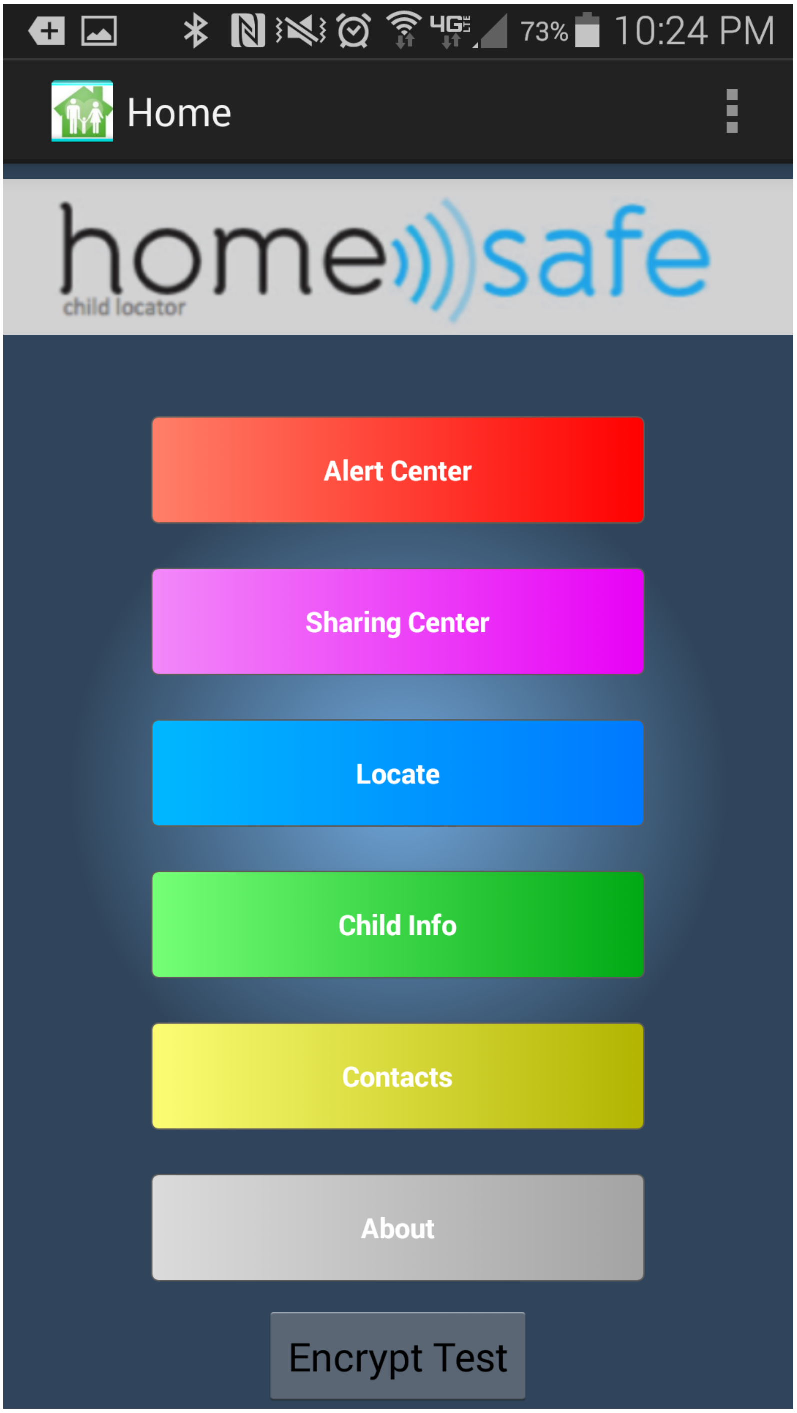
Email Address

Register

By clicking on Sign Up above you are agreeing to the terms and conditions

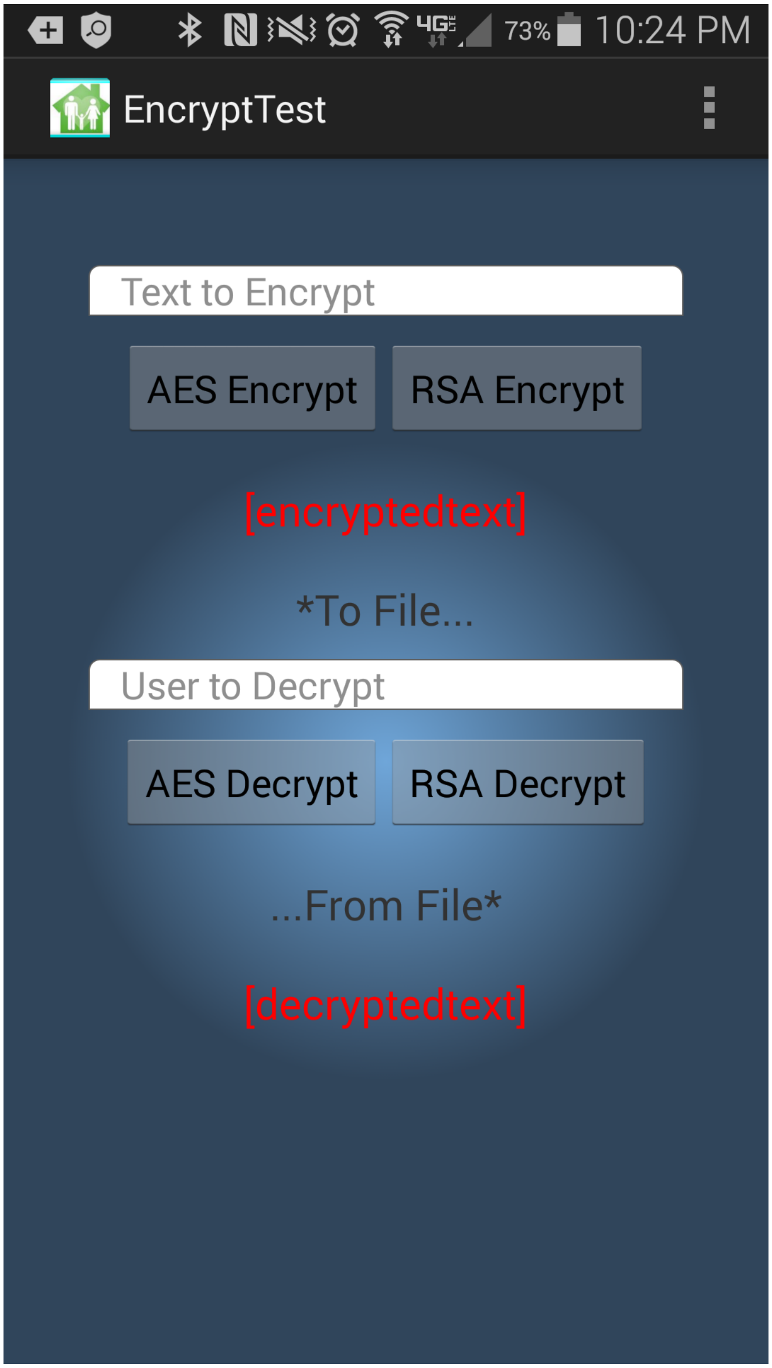
Terms and Conditions

Layout 3 - Register Activity

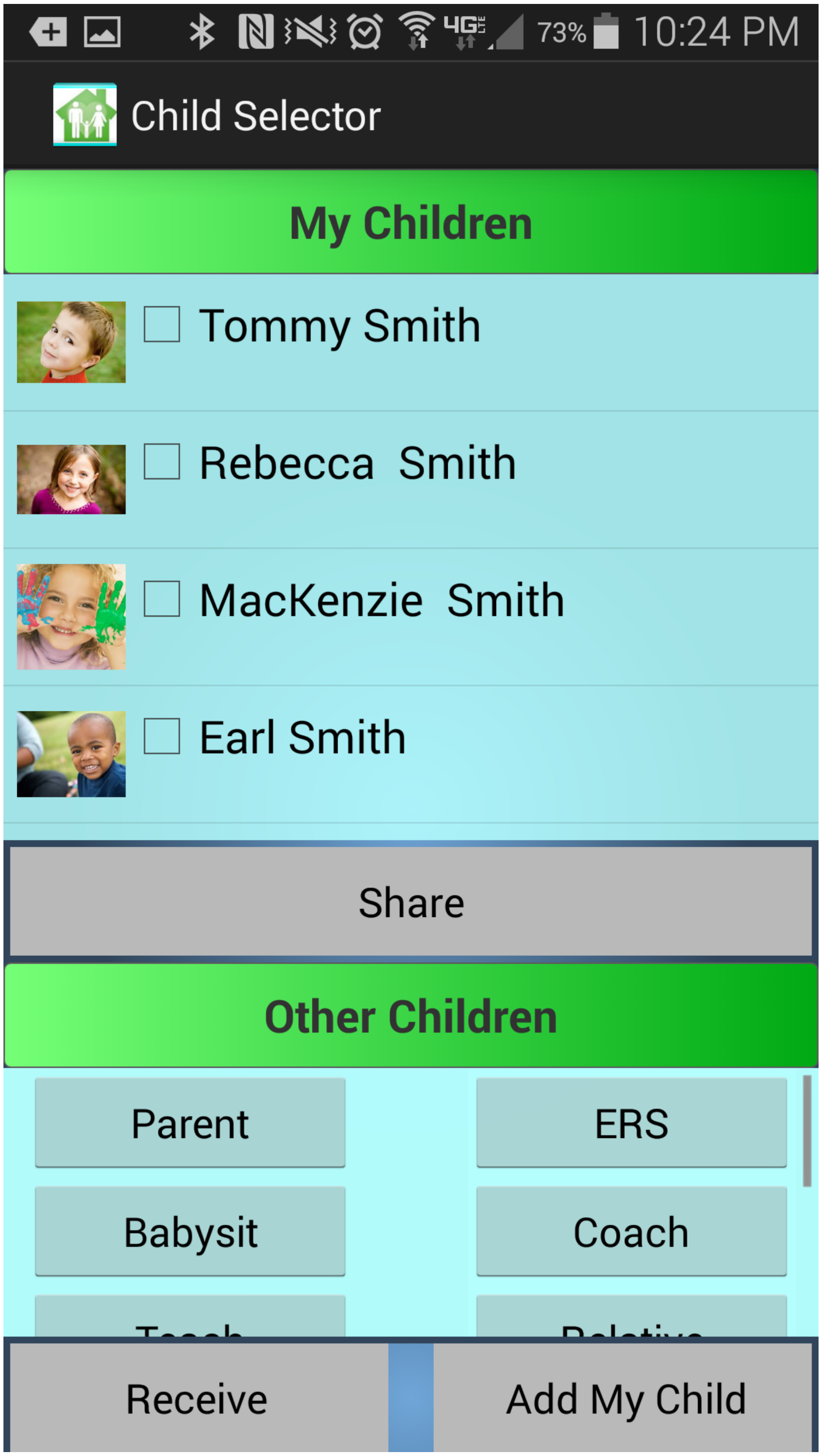


Layout 4 - Home Activity

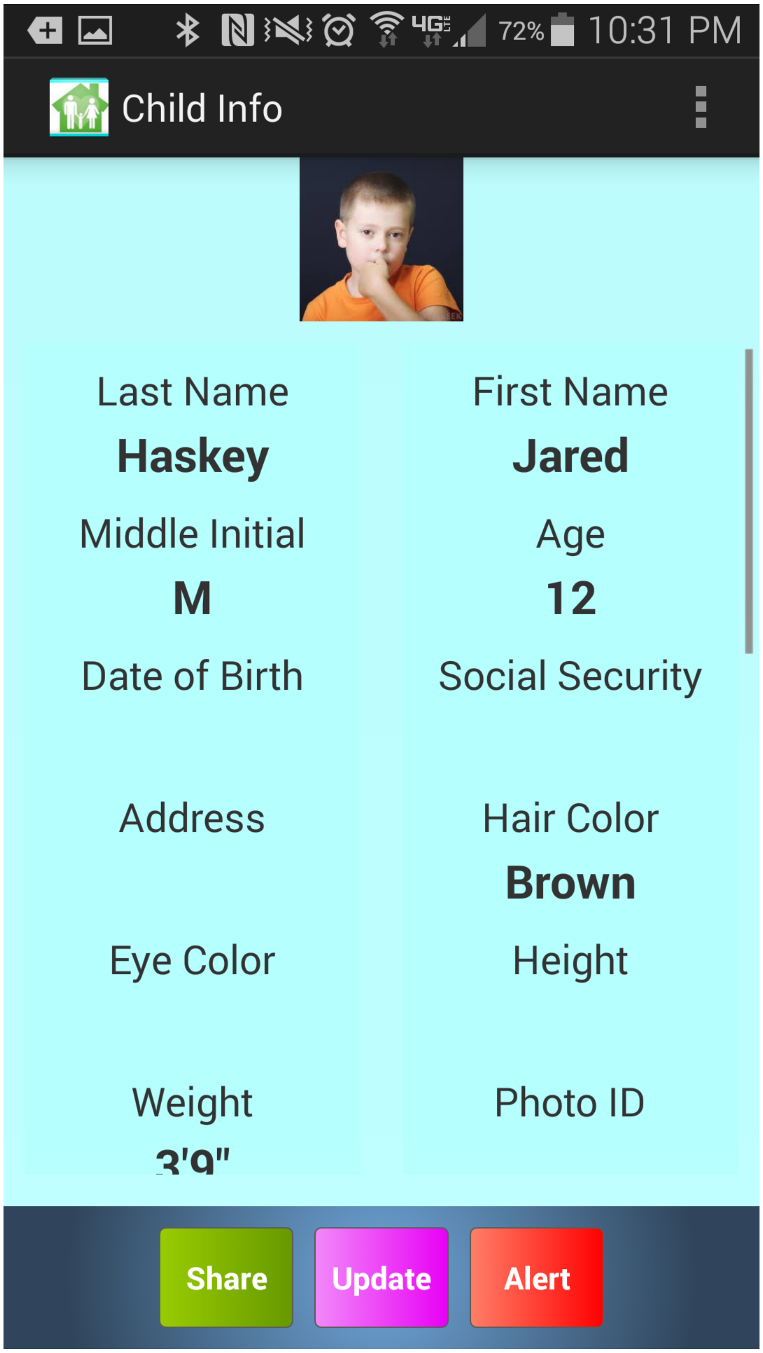
(encrypt test developer only) (some options not designed or undecided, for example Locate feature may be a potential threat in the wrong hands)



Layout 5 - Encrypt Test Activity



Layout 6 - Child Selector Activity



Child Info

Last Name
Haskey

First Name
Jared

Middle Initial
M

Age
12

Date of Birth

Social Security

Address

Hair Color
Brown

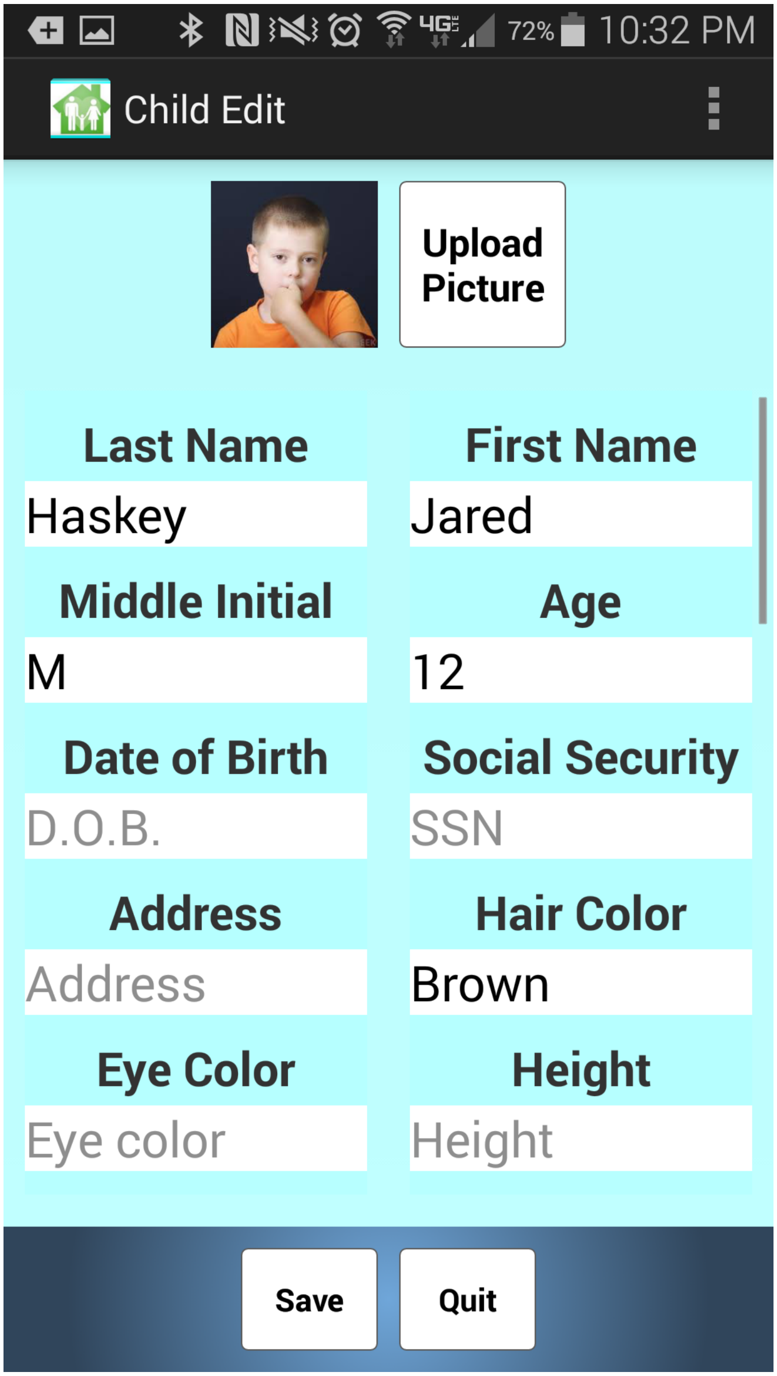
Eye Color

Height

Weight
3'9"

Photo ID

Layout 7 - Child Info Activity (accessed by clicking a name in the Child Selector Activity)



Last Name: Haskey

First Name: Jared

Middle Initial: M

Age: 12

Date of Birth: D.O.B.

Social Security: SSN

Address: Address

Hair Color: Brown

Eye Color: Eye color

Height: Height

Layout 8 - Child Edit Activity (also used to create new cards by a parent)

References

A. Gupta, S. Sultana, M. S. Kirkpatrick, E. Bertino, “A selective encryption approach to fine-grained access control for P2P file sharing”. In: Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on, 9–12 October ,pp.1–10 (2010)

D. Richard Kuhn, “Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems,” Proceedings of the second ACM workshop on Role-based access control, p.23-30, November 06-07, 1997, Fairfax, Virginia, USA

E. Bertino, M. S. Kirkpatrick, "Location-based Access Control Systems for Mobile Users: Concepts and Research Directions," in Proceedings of the 4th ACM SIGSPATIAL Int' 1 W' shop on Security and Privacy in GIS and LBS, pp. 49-52. ACM, 2011

M. Bishop, (2005). “Introduction to computer security” (p. 784). Boston: Addison-Wesley.

N. Doty, E. Wilde, "Geolocation Privacy and Application Platforms," ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, November 2010

R. Sandhu, E. Coyne, H. Feinstein, C. Youman, “Role-Based Access Control Models,” Computer, v.29 n.2, p.38-47, February 1996