2015

# KEYFREE: A DEVICE FOR STORING ENCRYPTED INFORMATION USING AUDIO COMMUNICATION

Matt Gern

Taylor Legg

Siena Richard

## Recommended Citation

Gern, Matt; Legg, Taylor; and Richard, Siena, "KEYFREE: A DEVICE FOR STORING ENCRYPTED INFORMATION USING AUDIO COMMUNICATION" (2015). *Honors Theses AY 15/16.* Paper 3.

# KEY-FREE: A DEVICE FOR STORING ENCRYPTED INFORMATION USING AUDIO COMMUNICATION

aYmV:
Matthew Gern
Siena Richard
Taylor Legg

# Table of Contents

# Description of Key-Free:

Key-Free is a secure and reliable way to store passwords or any sensitive information that is hard to remember but shouldn't be written down. It is a compact micro-controller with an audio adapter that communicates via audio jacks to store information on a micro SD card. Information is accessed and stored through a web portal that utilizes JavaScript to encrypt the sensitive information. That way, the user only has to remember one key, rather than all of his/her passwords. This can also allow users to use more secure passwords, that are longer and composed of random characters, and not worry about forgetting them. Basically, it is one password to rule them all!

The web portal uses JavaScript so that all of the encryption can be done client side. This way, sensitive information is not being sent over the Internet, making it susceptible to attacks. As soon as the user hits submit, the sensitive information is encrypted to keep it secure. Currently, 256-AES CBC mode is being used to encrypt the sensitive information. After it has been encrypted, the data is sent to the device, where it reads it in and stores it on the micro SD card under a name that the user chooses. When the user wants to retrieve the information, the user then only has to enter that one key he/she, and the name he/she originally chose to save it under to get it back. The web portal then asks the device for that piece of data, and decrypts it before providing it to the user.

There are several other features that come with Key-Free. One is that because all information is stored on the micro SD card, if for some reason the device fails or is damaged, the user can remove the micro SD card and insert it into a new device, and still have access to his/her sensitive information. Other features *may* include a random password generator, the ability to wipe the micro SD card if too many attempts have been made to unlock it, multi-factor authentication, auto fill in the browser, sending user IP information if the password is wrong, only allowing use on certain approved devices, and rendering the micro SD card unusable if a threat is detected.

Key-Free can allow for more secure practices, in a convenient and reliable way. With major companies being breached more often, it is as important as ever to be aware of best security practices, and be as secure as possible. Key-Free is meant to help with this in any way possible.

# Use Case: 1 Entry

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to store information securely.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has obtained a key-free device and the necessary cords.

**Success End Condition:** User's information is stored on the Key-Free device and is accessible from any device with a headphone and microphone jack or a TRRS jack.

**Failed End Condition:** User's information is not stored correctly and cannot be retrieved later. User's information is compromised and is no longer secure.

**Primary Actor:** User, any person wishing to manage information securely

**Trigger:** User obtains a Key-Free device and wants to securely store information.

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device.
2. User plugs Key-Free device into his/her device [Use case 3 or 4].
3. User navigates to the "Entry" page on the Key-Free.co website.
4. User enters the key he/she wish to use to encrypt his/her information.
5. User enters the description to store the information under.
6. User enters the information he/she wish to store.
7. User clicks the 'Store' button.

8. User’s information is encrypted using AES-256 CBC mode.
9. User’s information is securely stored on the micro SD card of the Key-Free device for later retrieval.
10. User unplugs his/her Key-Free device.
11. User can leave the Key-Free.co website.
12. User wishes to retrieve the information securely stored later.
13. User retrieves previously stored information [use case 2].
14. User is able to use information as he/she need.

# EXTENSIONS

- 3a. The website is down:
  - 3a1. User must wait for the website to come back up in order to retrieve anything from the Key-Free device.
- 5a. User does not enter all fields
  - 5a1. Webpage prompts user to complete remaining fields
- 7a. User enters incorrect information to store.
  - 7a1. If the user realizes this before he/she leave the “Entry” page, he/she can restore the correct information
  - 7a.2 If the user does not realize this, he/she will have incorrect information stored and he/she will have to handle when he/she go to retrieve the information [Use Case: 2 Retrieval].

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website
- 2a. User may supply his/her own cables

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process

**Frequency:** As often as someone logs into accounts (10/day)

**Superordinate Use Case:**

**Subordinate Use Cases:**

- Retrieval [use case 2]
- TRRS Jack [use case 3]
- 2 x TRS Jacks [use case 4]

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if there is no Micro SD card in the Key-Free device?
- What happens if the device does not have power?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 2 Retrieval

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to retrieve information that had already been stored securely.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has obtained a key-free device and the necessary cords. User has already stored the information [use case 1].

**Success End Condition:** User's information previously stored on the Key-Free device is securely accessible via a single TRRS or two TRS jacks [use cases 3 and 4].

**Failed End Condition:** User's stored information has not been retrieved successfully and it is lost.

**Primary Actor:** User, any person wishing to manage passwords securely

**Trigger:** User obtains a Key-Free device and wants to retrieve stored information.

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device.
2. User plugs Key-Free device into his/her device [use case 3 or 4]
3. User stores information securely for another account [use case 1].
4. At a later time, user needs the information he/she have already stored.

5. User plugs in his/her key-free device to his/her personal device.
6. User navigates to the “Retrieval” page on the key-free.co website.
7. User enters the ‘Key’ he/she encrypted the information with when he/she stored it.
8. User enters the ‘Description‘ he/she stored the information under.
9. User clicks the ‘Retrieve’ button.
10. The user’s information is retrieved from the Key-Free device via the headphone jack(s).
11. The information is displayed for the user to see and use.
12. The user uses this information however he/she need.
13. The information is still stored on the Key-Free device for later retrieval.

# EXTENSIONS

- 6a. The website is down:
    - 6a1. User must wait for the website to come back up in order to retrieve anything from the Key-Free device.
    - 6a2. An advanced user can pull the information off themselves, by removing the micro SD card and reading the files from it, and use a third party to decrypt the data themselves.
- 10a. User enters incorrect retrieval information.
    - 10a1. The website informs the user that something is wrong with the information he/she entered, and the user can re-enter the correct information.
- 10b. User attempts to retrieve account information that has not been stored
    - 6b1. Webpage alerts user of the incorrect key/description combination
    - 6b2. User stores the information [use case 1] for that account, and then retrieves it.
- 11a. The retrieved information is incorrect
    - 11a1. User can update the stored information by saving new information under the same description as the incorrect information.

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website
- 2a. User may supply his/her own male-male TRS cords or 2 male TRS to 1 male TRRS cord
- 5a. User may supply his/her own male-male TRS cords or 2 male TRS to 1 male TRRS cord

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]

**Subordinate Use Cases:**

- TRRS Jack [use case 3]
- 2 x TRS Jacks [use case 4]

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if the device is lost?
- What happens if keys/descriptions are entered incorrectly too many times?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 3 TRRS Jack

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to manage information from a device which has one single TRRS jack (Mobile Phone or Tablet).

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has created accounts (usernames/passwords)

**Success End Condition:** User's account information is stored on the Key-Free device and is accessible from mobile devices

**Failed End Condition:** User's account information has not been stored on the Key-Free device and is not accessible.

**Primary Actor:** User, any person wishing to manage account information securely

**Trigger:** User obtains a Key-Free device

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device
2. User uses a converter to plug Key-Free into TRRS audio jack of mobile device.
3. User visits key-free.co using a web browser on the mobile device
4. User follows steps for entry and/or retrieval of information [use case 1 or 2].

5. The user disconnects the key-free device.

# EXTENSIONS

- 2a. User plugs the Key-Free device in incorrectly:
  - 2a1. The website informs the user the device is plugged in incorrectly, and provides suggestions for fixing it.
- 10a. User enters incorrect key:
  - 10a1. Webpage alerts user of the incorrect key/description combination
  - 10a2. User enters correct key
- 10b. User attempts to retrieve account information that has not been stored
  - 10b1. Webpage alerts user of the incorrect key/description combination
  - 10b2. User enters correct information

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website
- 2a. User may supply two male-male TRS cords and a single 2-female TRS to male TRRS converter
- 2b. User may supply a single 2-male TRS jacks to a single male TRRS jack cord.

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]
- Retrieval [use case 2]

**Subordinate Use Cases:**

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What version of TRRS is being used (Apple standard or Android standard)?
- What happens if the user doesn't have cell service?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 4 2 x TRS Jacks

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to manage account information using a device which has 2 TRS jacks (one for microphone, one for headphone).

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has created accounts (usernames/passwords)

**Success End Condition:** User's account information is stored on the Key-Free device and is accessible.

**Failed End Condition:** User's account information has not been stored on the Key-Free device and is not accessible.

**Primary Actor:** User, any person wishing to manage account information securely

**Trigger:** User obtains a Key-Free device

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device
2. User connects the mic jack of his/her computer to the pink socket on the Key-Free device and connects the headphone jack of his/her computer to the green socket of the Key-Free device.
3. User visits the entry page of key-free.co

4. User follows steps for entry [use case 1].
5. User visits the retrieval page of key-free.co at a later time.
6. User follows steps to retrieve information [use case 2].

# EXTENSIONS

- 2a. User accidentally connects the Key-Free device to the wrong jacks of his/her computer.
  - 2a1. Webpage alerts user that the device was not detected.
  - 2a2. User switches the two TRS cables.
- 2b. User does not connect the Key-Free device to his/her computer.
  - 2b1. Webpage alerts user that the device was not detected.
  - 2b2. User plugs in the Key-Free device.

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website
- 2a. User may supply two of his/her own male-male TRS cords.

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]
- Retrieval [use case 2]

**Subordinate Use Cases:**

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if the device is lost?
- What happens if keys/descriptions are entered incorrectly too many times?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 5 Personal Use

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to manage information for personal accounts.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has created accounts (usernames/passwords)

**Success End Condition:** User's account information is stored on the Key-Free device and is accessible from PC and mobile

**Failed End Condition:** User's account information has not been stored on the Key-Free device and is not accessible.

**Primary Actor:** User, any person wishing to manage account information securely

**Trigger:** User obtains a Key-Free device

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device
2. User plugs Key-Free device into the audio jack(s) of his/her computer [use case 3 or 4].
3. User visits key-free.co using a web browser on his/her device
4. User follows steps for entry and/or retrieval of information [use case 1 or 2].

5. The user disconnects the key-free device.

## EXTENSIONS

- 4a. User stores personal information
  - 4a1. Information (e.g. Facebook username and password) [use case 7].
  - 4a2. Information relating to personal life (e.g. list of Christmas gifts) [use case 8].

## SUB-VARIATIONS

- 1a. Multiple users share a single Key-Free device.
  - 1a1. Each user has his/her own encryption key.
  - 1a2. Users must coordinate so that the same description name is not used more than once.

## RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]
- Retrieval [use case 2]
- TRRS Jack [use case 3]

- 2 x TRS Jack [use case 4]

**Subordinate Use Cases:**

- Storing Passwords [use case 7]
- Sensitive Information  [use case 8]

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if multiple users select the same key?
- What happens if multiple users use the same description?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 6 Professional Use

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to manage information for professional accounts or information.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has created accounts (usernames/passwords)

**Success End Condition:** User's account information is stored on the Key-Free device and is accessible from PC and mobile

**Failed End Condition:** User's account information has not been stored on the Key-Free device and is not accessible.

**Primary Actor:** User, any professional wishing to manage account information securely

**Trigger:** User obtains a Key-Free device

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device
2. User plugs Key-Free device into the audio jack(s) of his/her computer [use case 3 or 4].
3. User visits key-free.co using a web browser on his/her device.
4. User follows steps for entry and/or retrieval of information [use case 1 or 2].

5. The user disconnects the key-free device.

# EXTENSIONS

- 4a. User stores professional information
  - 4a1. Work-related information (e.g. corporate email account username and password) [use case 7].
  - 4a2. Information relating to professional life (e.g. list of projects to be completed) [use case 8].

# SUB-VARIATIONS

- 1a. An office buys a single Key-Free device for users to share.
  - 1a1. Each user has his/her own encryption key.
  - 1a2. Users must coordinate so that the same description name is not used more than once.
  - 1a3. Users can all securely access shared information.

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]

- Retrieval [use case 2]
- TRRS Jack [use case 3]
- 2 x TRS Jack [use case 4]

**Subordinate Use Cases:**

- Storing Passwords [use case 7]
- Sensitive Information  [use case 8]

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- If a professional leaves his/her company and the company takes back the device, how does the device get wiped?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 7 Storing Passwords

## CHARACTERISTIC INFORMATION

**Goal in Context:** Person uses the Key-Free device to store a password securely.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has obtained a Key-Free device and the necessary cords.

**Success End Condition:** User's passwords are stored on the Key-Free device and are accessible.

**Failed End Condition:** User's passwords have not been stored on the Key-Free device and are not accessible.

**Primary Actor:** User, any person wishing to manage passwords securely.

**Trigger:** User obtains a Key-Free device.

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device.
2. User plugs Key-Free device into the audio jack(s) of his/her computer [use case 3 or 4].
3. User stores a password for another account [use case 1].
4. At a later time, user needs that password to login to that account.

5. User plugs Key-Free device into the audio jack(s) of his/her computer [use case 3 or 4].
6. User retrieves the password he/she stored for that account [use case 2]
7. The user’s password is retrieved from the Key-Free device via the audio jack(s).
8. The user logs into his/her other account.

# EXTENSIONS

- 1a. User wishes to store information other than passwords.
    - 1a1. User refers to use case 8.

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website

# RELATED INFORMATION

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]
- Retrieval [use case 2]
- TRRS Jack [use case 3]
- 2 x TRS Jack [use case 4]
- Personal [use case 5]

- Professional [use case 6]

**Subordinate Use Cases:**

- Sensitive Information [use case 8]

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if the device is lost?
- What happens if keys/descriptions are entered incorrectly too many times?

# SCHEDULE

**Due Date:** Release 1.0

# Use Case: 8 Storing Information

## CHARACTERISTIC INFORMATION

**Goal in Context:** User uses the Key-Free device for sensitive information, excluding passwords.

**Scope:** Key-Free device

**Level:** Summary

**Preconditions:** User has obtained a Key-Free device and the necessary cords.

**Success End Condition:** User's information previously stored on the Key-Free device is securely accessible.

**Failed End Condition:** User's stored information cannot be retrieved successfully and it is lost.

**Primary Actor:** User, any person wishing to manage information securely.

**Trigger:** User obtains a Key-Free device and wants to retrieve stored information.

## MAIN SUCCESS SCENARIO

1. User obtains a Key-Free device.
2. User stores the sensitive information [use case 1].
3. At a later time, user needs the information he/she has already stored.
4. User retrieves the information he/she stored [use case 2].
5. User uses the information.

# EXTENSIONS

- 1a. User wishes to store passwords.
  - 1a1. User refers to use case 7.

# SUB-VARIATIONS

- 1a. User may obtain a Key-Free device by ordering on the website

# RELATED INFORMATION (optional)

**Priority:** Top

**Performance Target:** 5 minutes for a first time user, 2 minutes for someone experienced with the process.

**Frequency:** As often as someone logs into accounts (10/day).

**Superordinate Use Case:**

- Entry [use case 1]
- Retrieval [use case 2]
- TRRS Jack [use case 3]
- 2 x TRS Jack [use case 4]
- Personal [use case 5]
- Professional [use case 6]
- Passwords [use case 7]

**Subordinate Use Cases:**

**Channel to primary actor:** Website, Interactive

**Secondary Actors:** Key-Free device

**Channel to Secondary Actors:** Audio jack(s)

# OPEN ISSUES

- What happens if the device is lost?
- What happens if keys/descriptions are entered incorrectly too many times?

# SCHEDULE

**Due Date:** Release 1.0