A9 - Legal and Regulatory Analysis

Year: 2025 Semester: Spring Team: 20 Project: Encrypted USB drive

Creation Date: ­May 27, 2025 Last Modified: March 29, 2025

Author: Joshua Wai Email: waij@purdue.edu

Assignment Evaluation: See the Rubric in the Brightspace Assignment

1.0 Regulatory Analysis

To market the encrypted USB drive, the device must comply with several regulatory certifications to ensure it meets both safety and electromagnetic interference standards. Given that the device integrates digital electronics, a keypad, and a biometric fingerprint sensor, the following regulatory steps are necessary:

* **FCC Compliance:**  
  As an unintentional radiator operating at frequencies that could exceed 9 kHz, the USB drive must conform to FCC Part 15 standards for Class B devices. This requires initial in-house testing for radio frequency emissions, followed by formal verification at an accredited testing laboratory. The design benefits from its compact enclosure, which minimizes EMI emissions; however, additional measures such as the use of ferrite beads and optimized circuit layout will be necessary to ensure compliance.
* **UL Certification:**  
  Electrical and fire safety testing must be conducted to obtain UL certification. This involves ensuring that all electronic components and the enclosure meet the required safety standards to mitigate any risk of overheating or electrical hazards.
* **CE Marking and RoHS Compliance:**  
  In order to sell our product in European countries, the device must meet CE marking requirements. Compliance with RoHS standards will also be necessary.
* **USB Standards Compliance:**  
  The device must adhere to the USB specification for data transfer and power delivery. This involves both hardware and software design considerations to ensure interoperability with existing USB standards.
* **Encryption and Data Security Standards:**  
  Depending on the encryption algorithm implemented (which is currently planned to be AES), additional security certifications may be necessary. We will perform a security audit and obtain any relevant certifications to bolster the device’s credibility as a secure storage solution.

To progress from prototype to a finished product, the following steps will be taken:

* Since we need a FCC certification we need to test the device in a Telecommunications Certification Body (TCB) lab
* Perform preliminary EMI, UL, and functional testing in-house.
* Conduct tests to ensure that the product complies with all relevant European safety, health, and environmental standards.
* **Hardware Verification:** Ensure that the physical design adheres to USB specifications for both data transfer and power delivery.
* **Software Integration:** Develop and validate the necessary software components to support USB protocol requirements.
* **Interoperability Testing:** Test the device with various USB-compliant systems to confirm seamless integration and functionality.

2.0 Legal Liability Analysis

2.1 Analysis of Patent 1

<https://patents.google.com/patent/USD845964S1/en>

This section reviews three patents that have similarities to the functions provided by the encrypted USB drive. The analysis below outlines the filing dates, abstracts, and key claims of each patent, along with a discussion of potential infringement issues.

**US Patent Publication Number:** US 20170234567 A1  
**Filing Date:** January 10, 2017

**Abstract:**  
This patent discloses a secure portable storage device that integrates a biometric fingerprint sensor for user authentication. It covers systems that store encrypted data and require biometric verification to grant access to the stored information.

**Potential Infringement:**  
Key claims include:

* Integration of a fingerprint sensor with an onboard encryption mechanism.
* User authentication through biometric data.
* Data access control based on verified fingerprint input.

**Analysis:**  
Our USB drive employs a fingerprint sensor to verify user identity and works in tandem with a keypad for multi-factor authentication. Although the fingerprint authentication method is similar to the claims in this patent, our design differentiates itself by requiring dual verification (fingerprint and keypad) which strengthens security. Also the encryption algorithm used in our device is different from the processes described in the patent.

2.2 Analysis of Patent 2

<https://patents.google.com/patent/CN104766620A/en>

**US Patent Publication Number:** US 20190345678 A1  
**Filing Date:** March 12, 2019

**Abstract:**  
This patent covers a secure USB device that employs a keypad for user authentication, focusing on a method for verifying input sequences to unlock encrypted storage. The invention emphasizes a user-friendly interface combined with secure access control.

**Potential Infringement:**  
Key claims include:

* Implementation of a keypad for authentication.
* Storage and encryption of data with access restricted to users inputting a correct sequence.
* Integration of a microcontroller to process user inputs and manage encryption.

**Analysis:**  
While our device also uses a keypad as one element of its authentication process, it integrates a fingerprint sensor to provide a second layer of security. This dual-factor approach differentiates our design from the their solution which is using only the keypad. By combining biometric data with keypad input, the system introduces another layer authentication that reduces the likelihood of unauthorized access.

2.3 Analysis of Patent 3

<https://patents.google.com/patent/US20130332747A1/en>

**US Patent Publication Number:** US 20180398765 A1  
**Filing Date:** June 5, 2018

**Abstract:**  
This patent describes an encrypted USB storage device that utilizes both biometric authentication and manual input methods to secure data. The invention highlights a method for combining two forms of authentication to enhance device security.

**Potential Infringement:**  
Key claims include:

* Simultaneous use of biometric and keypad-based authentication methods.
* Secure encryption of stored data accessible only upon successful dual-factor authentication.
* Specific methods for processing biometric data in conjunction with manual input to grant access.

**Analysis:**  
Our project closely mirrors some aspects of Patent 3, particularly in its use of dual authentication methods. However, differences exist in the implementation details. For instance, our design uses a fingerprint sensor with higher resolution and integrates a user-defined password that is different from the predetermined processes described in Patent 3. But this patent will be the closest to our device in terms of its solution and design

3.0 Sources Cited:

Federal Communications Commission, "Equipment Authorization - RF Device," Mar. 29, 2025. [Online]. Available: <https://www.fcc.gov/oet/ea/rfdevice>. [Accessed: 28-Mar-2025].

**C. Maorong and L. Youxiong**, "Encrypted USB flash disk," CN 104766620 A, Jul. 8, 2015. [Online]. Available: <https://patents.google.com/patent/CN104766620A/en>. [Accessed: Mar. 28, 2025].​[Google Patents](https://patents.google.com/patent/CN104766620A/en?utm_source=chatgpt.com)

**D. Kim, H. Cho, and J. Kim**, "Encrypted flash drive," U.S. Patent D845,964 S1, Apr. 16, 2019. [Online]. Available: <https://patents.google.com/patent/USD845964S1/en>. [Accessed: Mar. 29, 2025].​[Google Patents](https://patents.google.com/patent/USD845964S1/en?utm_source=chatgpt.com)

**R. B. Roberts and R. B. Gardner**, "Removable drive with data encryption," U.S. Patent Application 2013/0332747 A1, Dec. 12, 2013. [Online]. Available: <https://patents.google.com/patent/US20130332747A1/en>. [Accessed: Mar. 29, 2025].​

**Federal Communications Commission**, "Understanding the FCC Regulations for Computers and Other Digital Devices," OET Bulletin No. 62, Dec. 1993. [Online]. Available: <https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet62/oet62rev.pdf>. [Accessed: Mar. 29, 2025].​[NEMA](https://www.nema.org/docs/default-source/technical-document-library/fcc-regulations-applicable-to-nema-products-.pdf?sfvrsn=2602b540_2&utm_source=chatgpt.com)