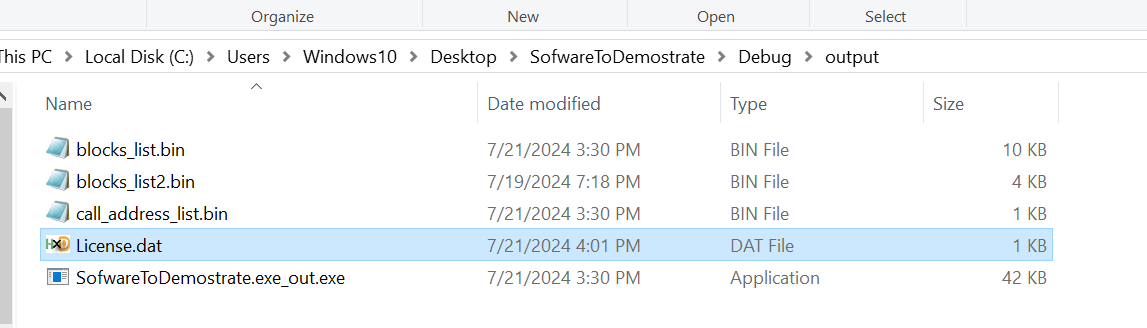
1. What

2.1 Product Overview

* The product contains two main parts, server program and activation system.

The server system should be installed on the server machine. And needs to be activate with the path to the software you want to protect for each new license you want. The license will get from the user his identifier, and will create protected version of the software, the license, and some supporting files. 

The server will send all of those to the client, along with the activation file.

The client side –

The client will use the protected version only with the activation system.

* The protected program only on the machine to which it had been created for. (even if the license is being shared).
* It impossible to activate the protected software without the license and the activation program.
* it’s very hard for reverse engineering, and thus, all the intellectual properties are protected.
* Easy portable and ensure simple use.

2.2 Target Market

1. Software Companies and Developers

Software companies, from large enterprises to independent developers, form a significant portion of the target market for DRM systems. They use DRM to protect their intellectual property and prevent unauthorized use or distribution of their software.

2. Enterprise Software Providers

Enterprise software providers, especially those offering high-value applications such as CAD software, financial tools, and data analysis platforms, are key targets for DRM solutions.

1. Video Game Industry

The video game industry, including both PC and console games, is a major user of DRM systems to prevent piracy and protect game assets.

* and Security examines DRM techniques in the gaming industry [3].

1. Educational Software Providers

Educational institutions and e-learning platforms use DRM to protect course materials and manage access to educational software.

Not good! Need to fix:

**The global Digital Rights Management (DRM) market, which includes software protection, is experiencing significant growth. According to a report by MarketsandMarkets, the DRM market is expected to grow from $3.5 billion in 2020 to $6.1 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 11.8% [1].**

**A more recent report by Grand View Research estimates that the global DRM market size was valued at $3.69 billion in 2021 and is expected to expand at a CAGR of 15.1% from 2022 to 2030 [2].**

Business Requirements:

Certainly. I'll write the business requirements for a DRM system focused on software protection following the pattern you've provided:

\*\*3. Business Requirements\*\*

\* \*\*Purpose\*\*:

The purpose of our DRM system is to provide robust protection for software assets, preventing unauthorized use, distribution, and modification while ensuring a seamless experience for legitimate users. This aligns with our business objective of safeguarding intellectual property and maintaining revenue streams from software sales and licensing.

\* \*\*Objectives\*\*:

1. Increase software revenue by reducing piracy rates by at least 30% within the first year of the publishment.

2. Enhance customer trust by providing a secure, tamper-resistant software environment.

3. Enable flexible licensing models (e.g., subscription-based, pay-per-use) to adapt to evolving market demands and increase recurring revenue by 25%.

4. Reduce support costs related to license management by 40% through automation and self-service capabilities.

5. Achieve compliance with industry standards and regulations (e.g., GDPR, CCPA) to expand market reach.

6. Increase software usage analytics capabilities to inform product development and marketing strategies.

7. Maintain software performance, ensuring that DRM implementation does not increase load times by more than 5%.

8. Achieve a customer satisfaction rate of at least 85% regarding the licensing and activation process.

\* \*\*Constraints and Assumptions\*\*:

Constraints:

1. Budget: The development team is only two workers for now, in order build strop development team, we need at least 50 workers, offices and equipment. Estimated cost is at least 15 million shekels , with option options.

4. Compatibility: The system must be compatible with major operating systems (Windows, macOS, Linux) and support both desktop and mobile applications.

5. Performance: The DRM solution must not increase application startup time by more than 2 seconds.

Assumptions:

1. The current infrastructure can support the additional load from DRM processes without significant upgrades.

2. Users will have a consistent internet connection for initial activation and periodic license verification.

3. The legal framework for software protection will remain stable in our key markets over the next three years.

4. Our software partners and distributors will be willing to integrate our DRM solution into their products and platforms.

5. The development team has the necessary expertise to implement advanced cryptographic techniques required for robust DRM.

6. Users will accept the DRM system if it provides a seamless experience and clear value proposition.

7. The benefits of reduced piracy will outweigh any potential loss of users who refuse to use software with DRM.

These business requirements provide a clear direction for the development of the DRM system, aligning it with key business objectives while acknowledging the constraints and assumptions that may impact its implementation. The specific objectives are measurable, allowing for clear evaluation of the system's success post-implementation.2.3 Value Proposition

* Unique selling points
* Benefits to users

2.4 Technical Specifications

* Core technologies used
* System architecture (if applicable)

2.5 User Experience

* Interface design
* Usability considerations

2.6 Competitive Landscape

* Key competitors
* Differentiating factors

2.7 Regulatory Compliance

* Relevant standards and regulations
* Compliance measures taken

Certainly. I'll provide you with a list of business requirements for a good Digital Rights Management (DRM) system. These requirements take into account various stakeholders' needs and the overall effectiveness of the system:

These business requirements aim to create a DRM system that balances robust content protection with user-friendliness, while also providing the flexibility and features needed by content owners and distributors. The specific priority of these requirements may vary depending on the particular use case and industry.

Revenue Protection: Ensuring that only paying customers have access to the software helps protect the revenue stream of the software provider by preventing unauthorized use or distribution.

Preventing Piracy: Generating licenses with unique identifiers or activation keys helps deter software piracy by making it more difficult for unauthorized users to access or distribute the software.

Program protection properties:

Hacked after 60 days because all sales are in 30-60 first days.

Expirated date:

Easy portable:

Performances:

Modulables:

Functional requirements:

To implement this system effectively, we first need to identify a robust PC ID to serve as the foundation for the license generator. Additionally, we will establish a validation mechanism for the program through a dedicated License Server, integrate advanced packing techniques, and conduct thorough testing to ensure the system's resilience.

• Find good PC ID: Find unique and universal and permanent machine’s attribute to activate as computer identifier. The attribute should be hard to temper or to steal. The pc id must be easily accessible.

• License Generator system: Develop a robust license generator capable of receiving PC ID as input and generating a unique license for each machine.

• License validation: Implement a system to validate license. The license will be valid only on the machine to which it was given to.

• Resistance to bypassing and patching: Find a way to protect our system.

• Demonstration and Testing: Be the hacker to think how to break our system.

• Ease of Portability and Integration: Design the system in a modular and portable manner to facilitate easy integration into other projects. The system should get the path of exe file and create license file and new lock exe file for each PC ID.

High Level Architecture:

High Level Security Objectives:

Ensure Confidentiality and Prevent Unauthorized Modification: Ensuring the confidentiality of customer data and preventing unauthorized modification by unprivileged software adversaries is a key security objective. This will involve implementing robust encryption mechanisms to protect sensitive data and adopting strict access controls to limit data access only to authorized users.

Secure Authentication Mechanisms: Implement robust authentication mechanisms to verify the identity of users accessing the software, ensuring that only authorized individuals can use the program.