# Third Deliverable: Architecture and Design

Architecture overview, how the system interaction with external systems puts it at risk.

Variation of the boundaries of the system vary from deployment

In your opinion, are there locations in the architecture where too many assets reside?

Analysis of your threat Model. More explanation about boundaries of the system.

The purpose of this deliverable is to come up with the architecture and design of your product. Your deliverable must include:

* **Architecture Overview**. Describe the architecture of the system. Please answer the following questions:
  + What are the subsystems? What does each subsystem do?
  + Are there subsystems that are expressly security features? (e.g. encryption, authentication) Describe these in more depth.
  + Consider the cost of developer mistakes in terms of subsystems. For example "if a developer makes a mistake in this subsystem, what happens?"
  + Do some subsystems appear to be more susceptible to code-level vulnerabilities?
  + Do you see security built into system at this architectural level? (e.g. distrustful decomposition)
  + How might compromising one subsystem affect the security (integrity, reliability, etc.) of the others or of the system as a whole?
  + How does the system interaction with external systems put it at risk?
  + Consider how the architecture might change over time.
* **Threat Model**. Build a threat model diagram and conduct an analysis using the Microsoft tool. Write up your analysis.
  + What are the machine boundaries of the system? Does this vary from deployment to deployment?
  + What are the trust boundaries of the system? Are there any trust boundaries more important than others?

Please make this diagram legible - I would rather you show the riskiest parts of the threat model than enumerate every possibility. As a guide, threat models get pretty confusing after about 12 primitives per diagram. If you feel your diagram must be more complex, feel free to break it up into multiple diagrams.

* **Assets to Threat Model Tracing** Provide a mapping from your assets in deliverable 1 to the elements in your threat model. Discuss this mapping:
  + Does the location in the architecture affect the p(exploit) of an asset? Why or why not?
  + Are there locations in the architecture where no assets reside? Did you miss any assets there?
  + In your opinion, are there locations in the architecture where too many assets reside?
* **Detailed Design** show class diagrams of your detailed design. Please show and discuss any secure design pattern, guideline, principle that you built in your design.

# Grade: **5%**

* + **1 pt** - Overview and subsystems
  + **1 pt** - Threat Model diagram and description
  + **1 pt** - Mapping to Assets
  + **2 pt** – Detailed Design (Secure Design principles and patterns)

# Deadline: **Day Date**