# Chapter 1

# Certified Security by Design (CSBD) &

# Access-Control Logic (ACL)

## 1.1 Certified Security by Design (CSBD)

## 1.2 Access-Control Logic (ACL)

### 1.2.1 Principals

### 1.2.2 Well-formed Formulas Formulas

### 1.2.3 Kripke Structure

#### 1.2.3.1 satisies

#### 1.2.3.2 soundness

### 1.2.4 Well formed statements

### 1.2.5 Inference Rules

### 1.2.6 Complete mediation

## 1.3 ACL in HOL

### 1.3.1 satList

### 1.3.2 Complete Mediation