# Safety and Consistency of Subject Attributes for Attribute-Based Pre-Authorization Systems

**Mehrnoosh Shakarami**
**Ravi Sandhu**

**Institute for Cyber Security (ICS)**
**Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)**
**Department of Computer Science**
**University of Texas at San Antonio**

National Cyber Summit
June 2019

# Presentation Outline

1

**Introduction & Motivation**

What is Attribute Based Access Control?

Why I should care about consistency problem?

2

**Proposed Consistency Levels**

Prposed levels in a glance

Level details and properties

3

**Discussion, Conclusion and Future Work**

Special Cases

What has been done? What to do next?

# Introduction

- Access control imposes restrictions on subjects’ access to protected objects according to specified policies.

**SUBJECT**

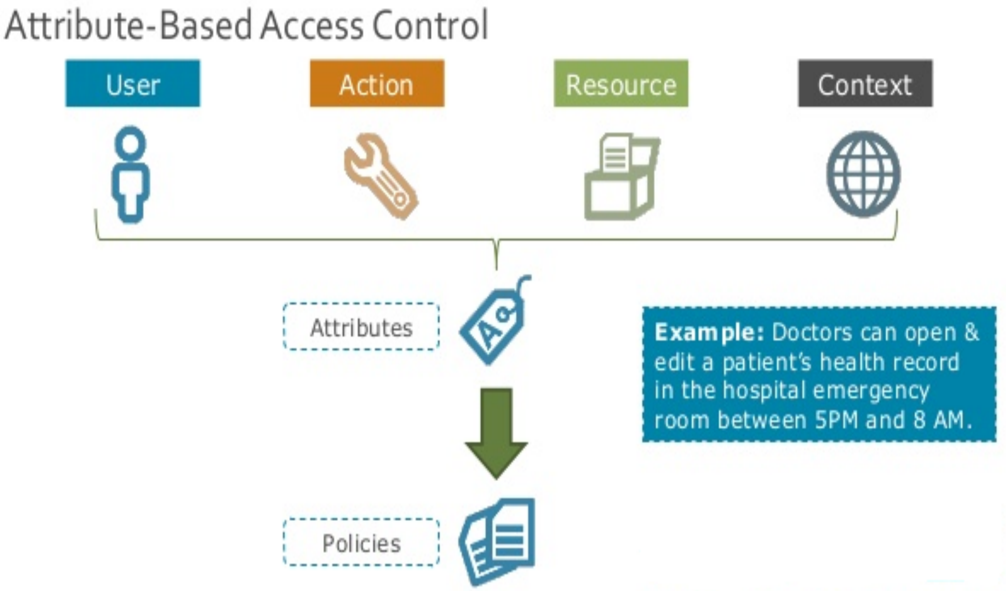
Generally an individual, process, or device causing information to flow among objects or change to the system state.

**OBJECT**

System-related protected entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information.

**Policy**

A set of rules which regulates access of subjects to protected objects in the system.

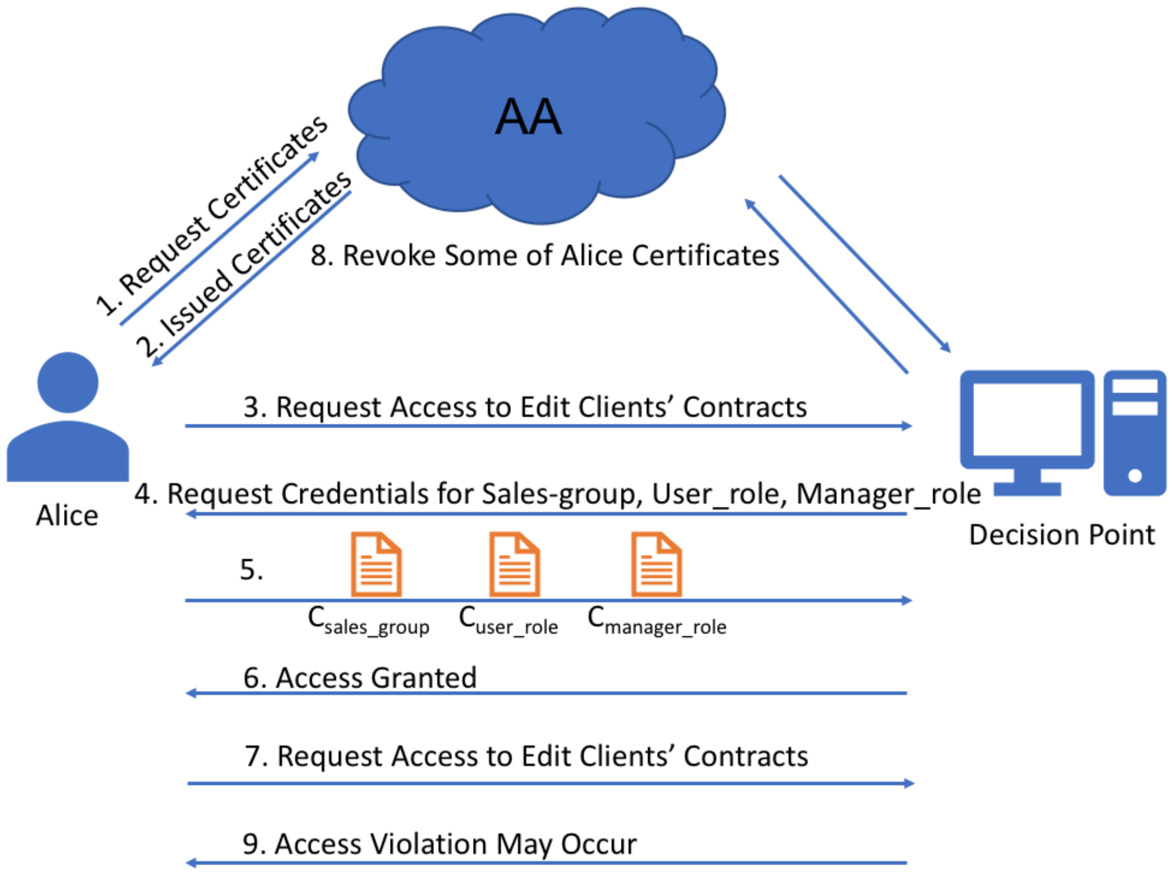


**Example:** Doctors can open & edit a patient’s health record in the hospital emergency room between 5PM and 8 AM.

# Introduction (cont'd)

- Consistency Problem: incorrect access decision resulted from following challenges in a decentralized system:
  - Asynchronous nature of distributed systems.
  - Cached values of attributes.
  - Network and system failures
  - Incremental assembly of subject attributes
  - Differing validity periods for subject attribute values

# Motivating Example


AA
1. Request Certificates
2. Issued Certificates
8. Revoke Some of Alice Certificates
Alice
Decision Point
3. Request Access to Edit Clients' Contracts
4. Request Credentials for Sales-group, User_role, Manager_role
5.
$C_{sales\_group}$
$C_{user\_role}$
$C_{manager\_role}$
6. Access Granted
7. Request Access to Edit Clients' Contracts
9. Access Violation May Occur

# Presentation Outline

1

## Introduction & Motivation

What is Attribute Based Access Control?

Why I should care about consistency problem?

2

## Proposed Consistency Levels

Prposed levels in a glance

Level details and properties

3

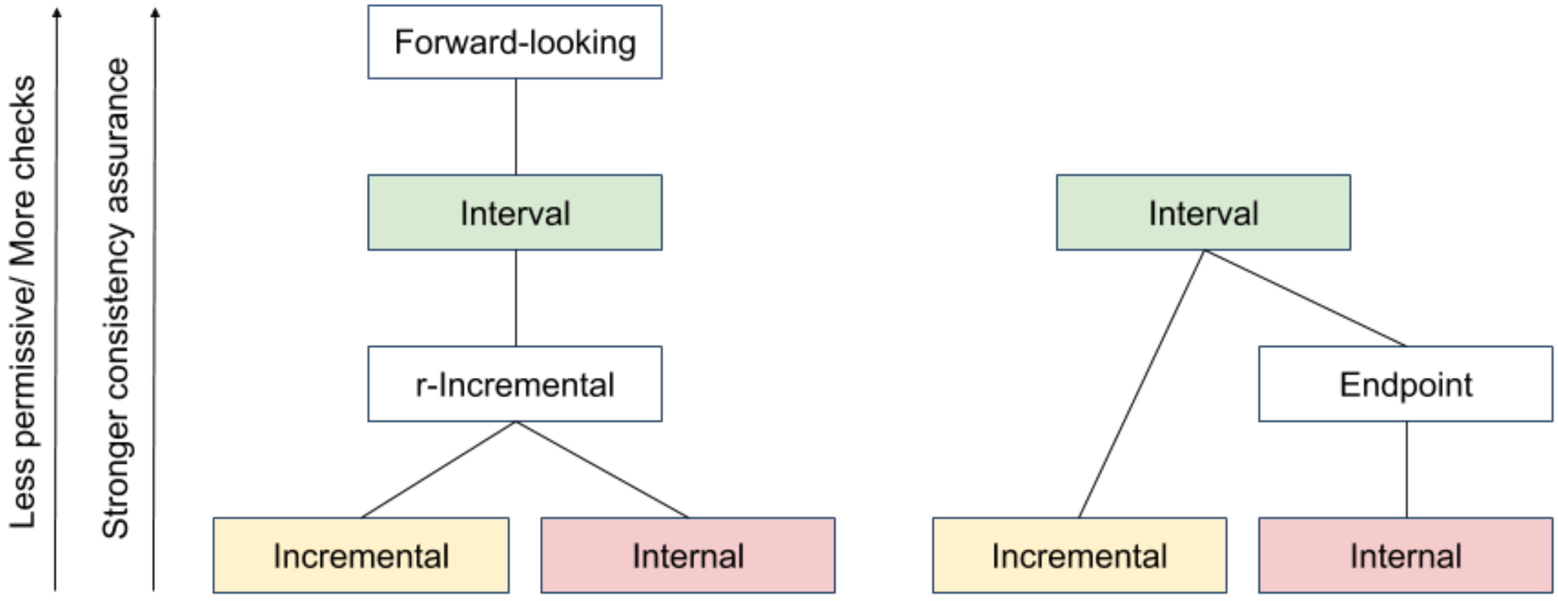
## Discussion, Conclusion and Future Work

Special Cases

What has been done? What to do next?

# Consistency Levels

- Five increasingly powerful consistency levels each of which imposes more restrictive constraints on timing and sequencing of attribute revocation checks

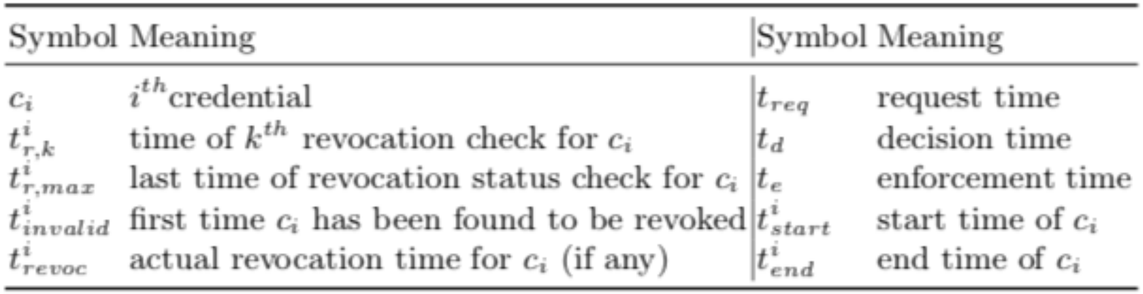


(a) (b)

# Problem Statement

- We assume that an ABAC model is in place, on top of which we define our consistency notions.
- The value of a subject attribute is referred to as a *credential* which requires to have a determined lifetime interval.
- We refer to the set of subjects credentials available at the decision point as the *view* of the decision point.

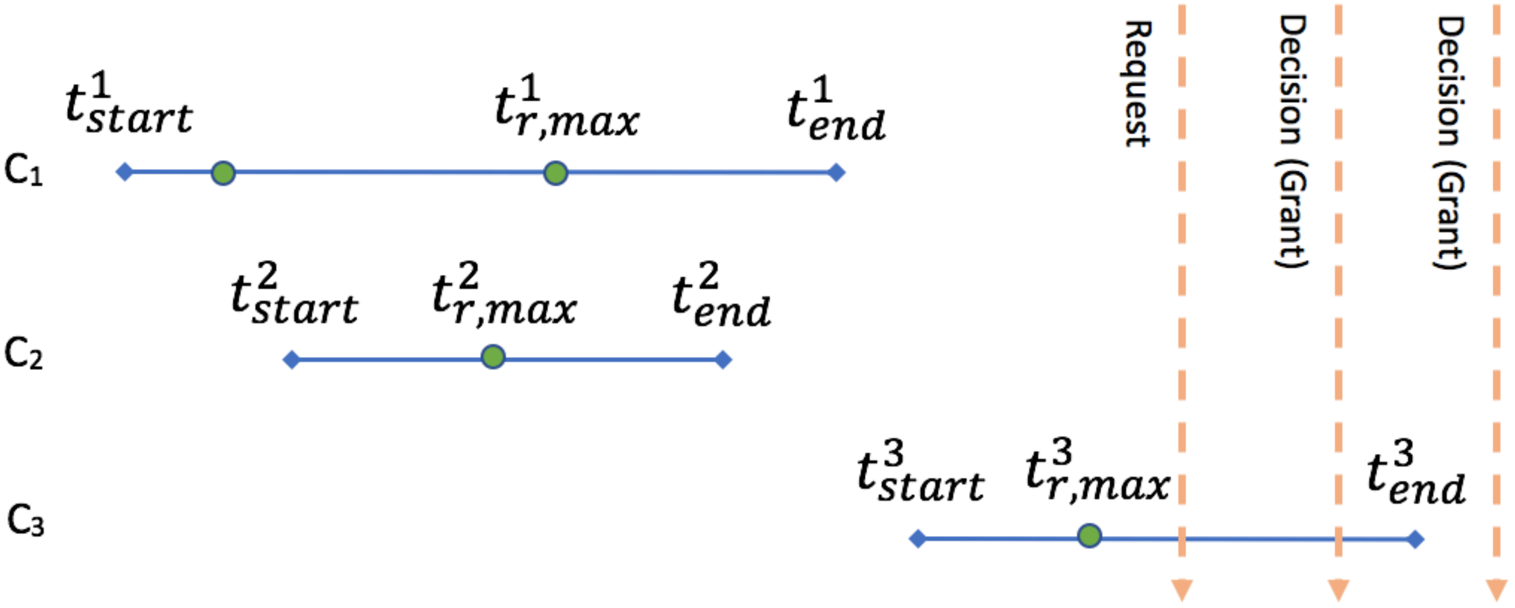
**Table 1.** Table of Symbols



| Symbol | Meaning | Symbol | Meaning |
|---|---|---|---|
| $c_i$ | $i^{th}$credential | $t_{req}$ | request time |
| $t^i_{r,k}$ | time of $k^{th}$ revocation check for $c_i$ | $t_d$ | decision time |
| $t^i_{r,max}$ | last time of revocation status check for $c_i$ | $t_e$ | enforcement time |
| $t^i_{invalid}$ | first time $c_i$ has been found to be revoked | $t^i_{start}$ | start time of $c_i$ |
| $t^i_{revoc}$ | actual revocation time for $c_i$ (if any) | $t^i_{end}$ | end time of $c_i$ |

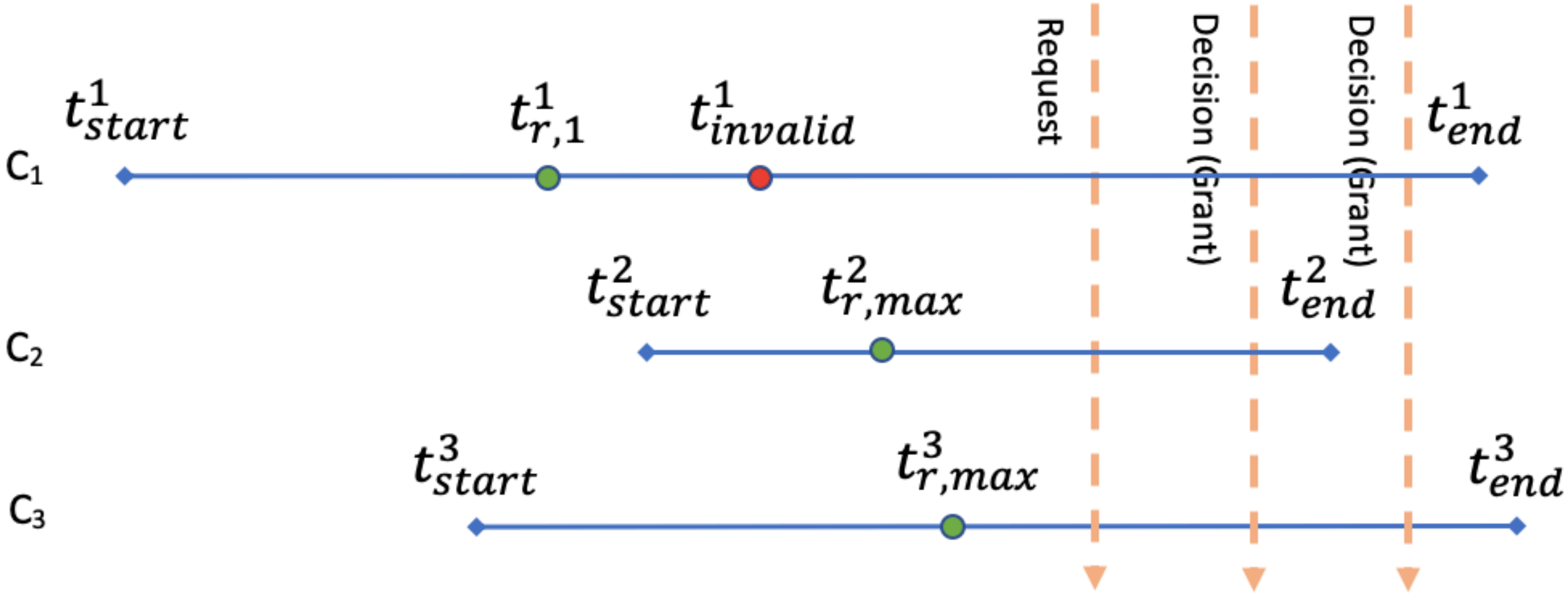
# Incremental Consistency

- The most permissive level: each credential has been validated once before the decision time



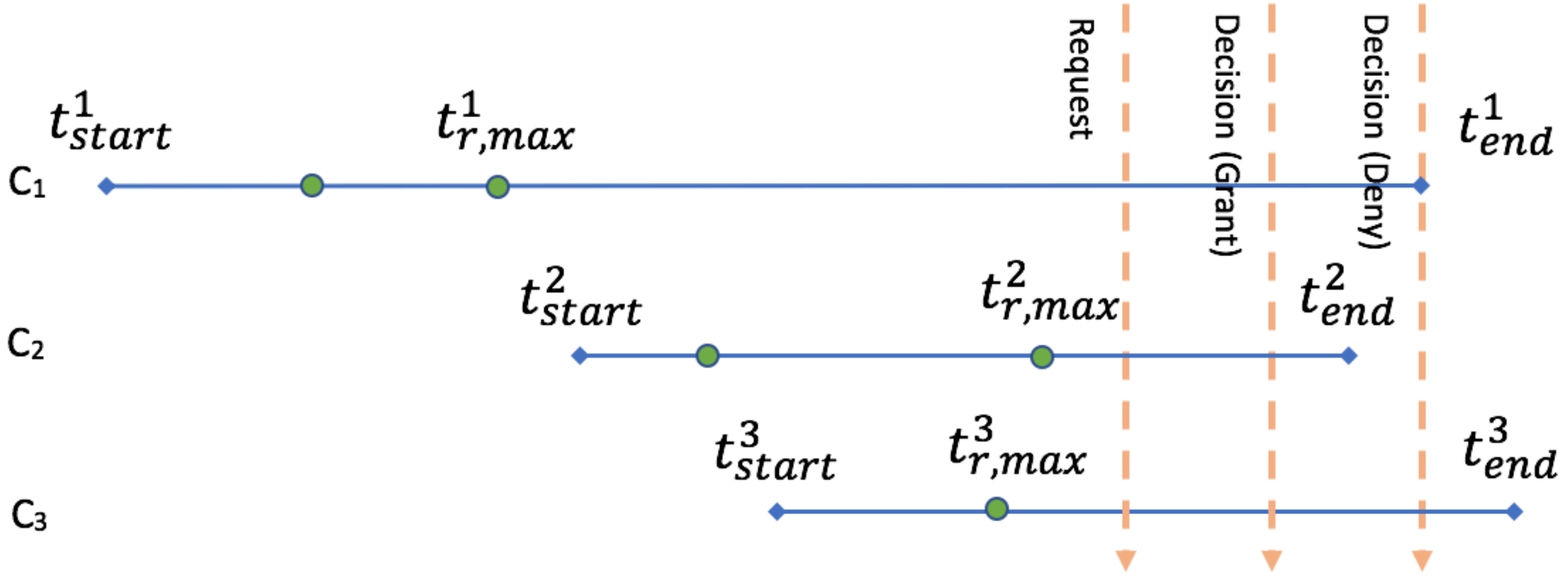
# Internal Consistency

- Lifetime overlap of all credentials guaranteed. If a credential is revoked, this revocation should happen after all credentials have started.



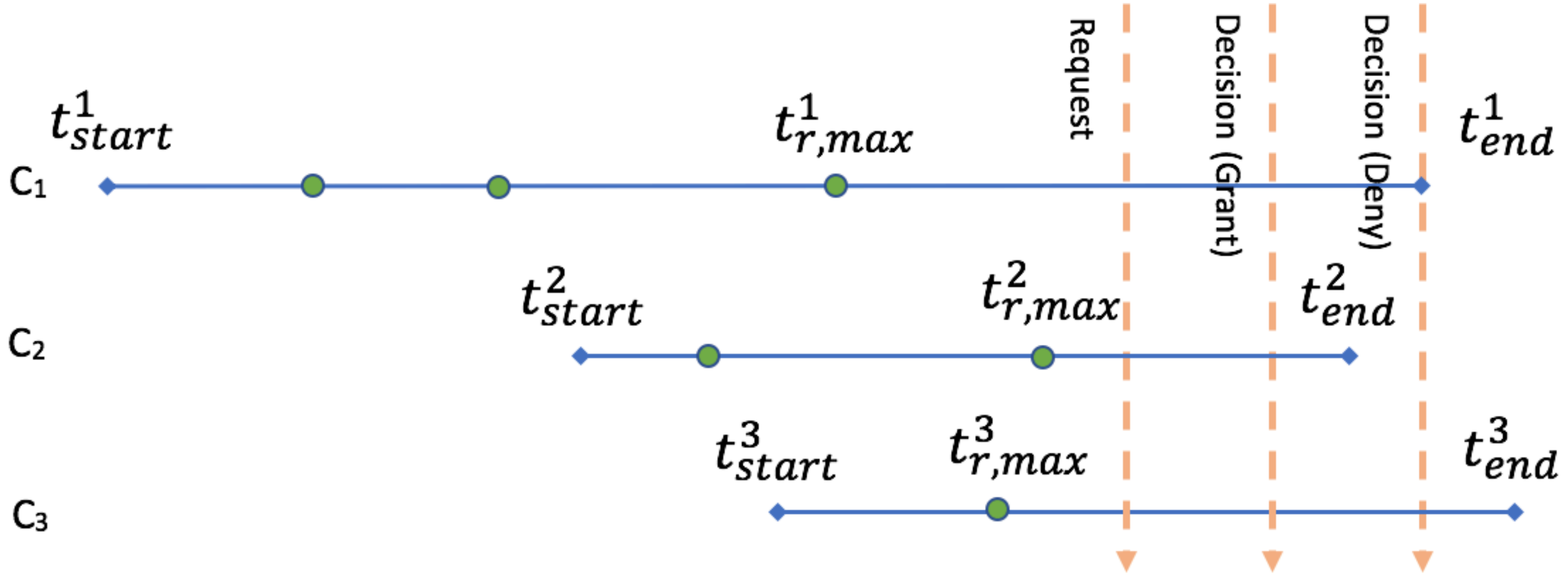
# Restricted Incremental Consistency (r-Incremental)

- No expired credential is accepted, lifetime overlap of all credentials are guaranteed.



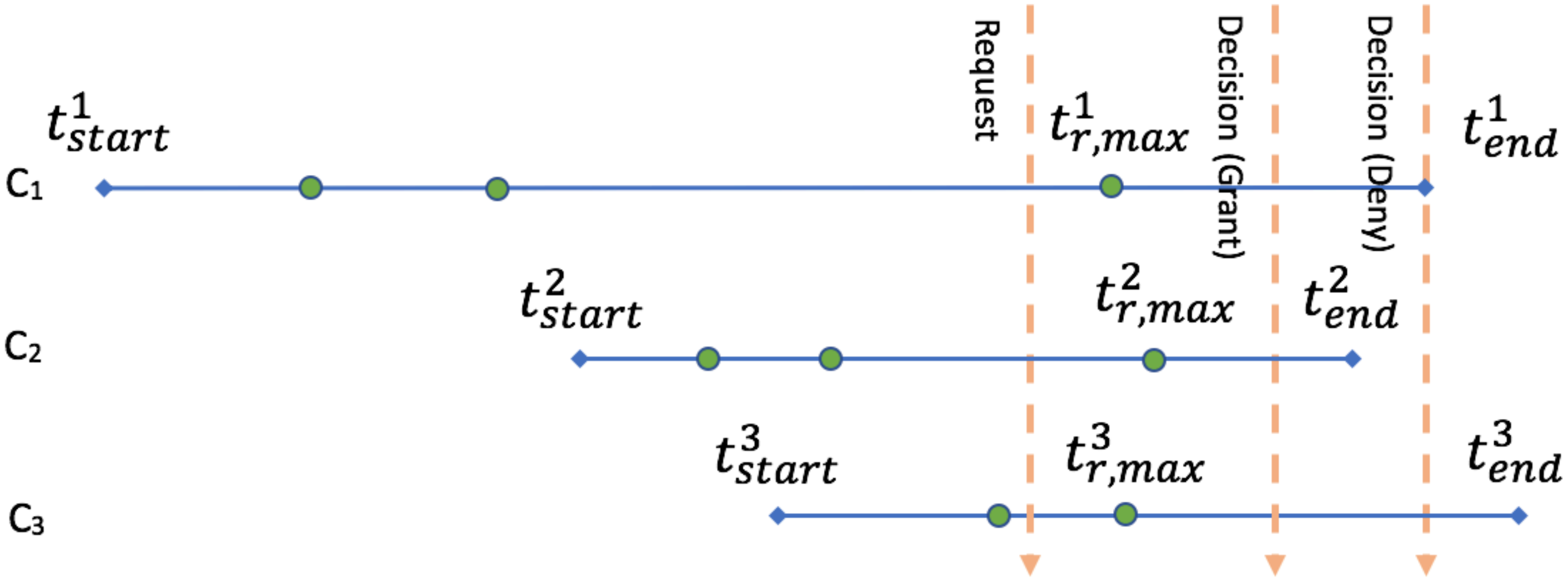
# Interval Consistency

- All relevant credentials are valid simultaneously during some time interval.



# Forward-looking Consistency

- All credentials have been valid simultaneously at some point after the *request time.*



# Presentation Outline

1 **Introduction & Motivation**

What is Attribute Based Access Control?

Why I should care about consistency problem?

2 **Proposed Consistency Levels**

Prposed levels in a glance

Level details and properties

3 **Discussion, Conclusion and Future Work**

Special Cases

What has been done? What to do next?

# Discussion and Conclusion

- Our proposed levels of consistency could be applied on:
  - Short-lived vs. long-lived credentials
  - Different revocation scenarios
  - Considering enforcement time

- Proposed approach provides:
  - Precise definition of safety and consistency
  - Foundational rigor and precision
  - Higher safety assurance

# Future Work

- Moving toward Freshness checking vs. Revocation checks
- Consider other access control information could be stale as well
- Develop models for ongoing authorization

# Questions?