Incorporating Off-Line Attribute Delegation into Hierarchical Group and Attribute-Based Access Control

Daniel Servos
Western University
London, Ontario
dservos5@uwo.ca

Michael Bauer
Western University
London, Ontario
bauer@uwo.ca

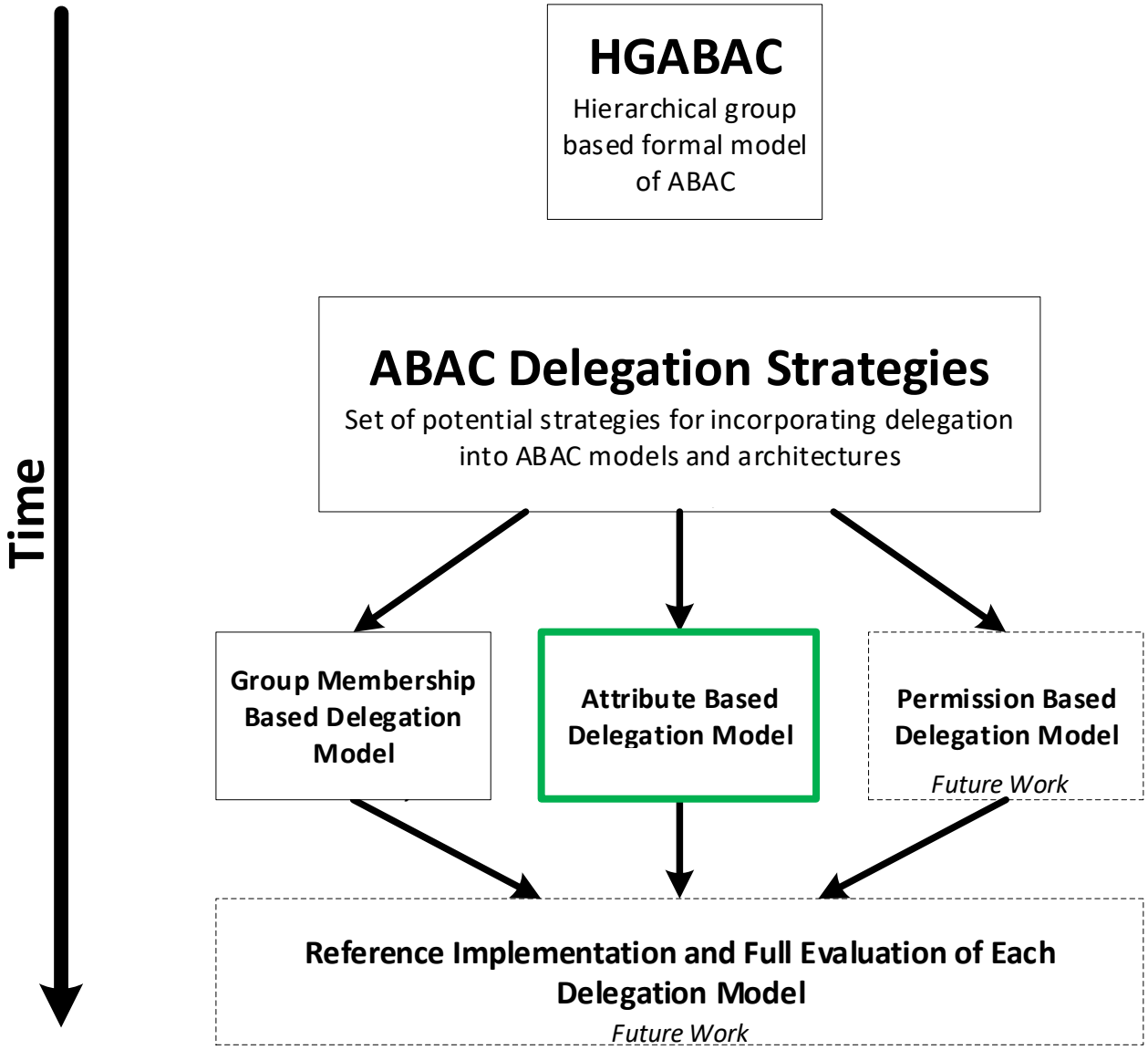
November 5th
FPS 2019

Outline

- **Outline**
- Background
- Attribute Delegation Model
- Attribute Delegation Framework
- Conclusions

Background:
The HGABAC Project

HGABAC Project



HGABAC Project

HGABAC
Hierarchical group based formal model of ABAC

Servos et al., 2014

HGABAC Administrative Model
Model governing the

Hierarchical Group and Attribute-Based Access Control (2014)

- Formal attribute-based access control model.
- Introduces concepts of hierarchical user and object attribute groups.
- Goals:
  - Lightweight
  - Easy to comprehend policies
  - User and object groups to simplify administration
  - Scalable
  - Ability to emulate traditional models (MAC, DAC, RBAC)
- Shown to be capable of emulating MAC, DAC and RBAC.

HGABAC Project

HGABAC

Hierarchical group based formal model of ABAC

Servos et al., 2014

HGABAC Administrative Model

Model governing the administration of attributes, users, etc. in HGABAC

ABAC Delegation Strategies

Set of potential strategies for incorporating delegation into ABAC models and architectures

Servos et al., 2016

HGAA

Strategies for Incorporating Delegation into ABAC (2016)

- Details strategies for incorporating delegation into ABAC.
- Strategies formulated by evaluating each possible combination of ***delegator***, ***delegatee*** and ***delegatable access control component***.
- Resulted in three potential families of strategies that share common properties; ***Group Membership Delegation***, ***Attribute Delegation*** and ***Permission Delegation***.

HGABAC Project

HGABAC
Hierarchical group based formal model

HGABAC Administrative Model
Model governing the administration of attributes, users, etc. in HGABAC

Hierarchical Group Attribute Architecture (2018)

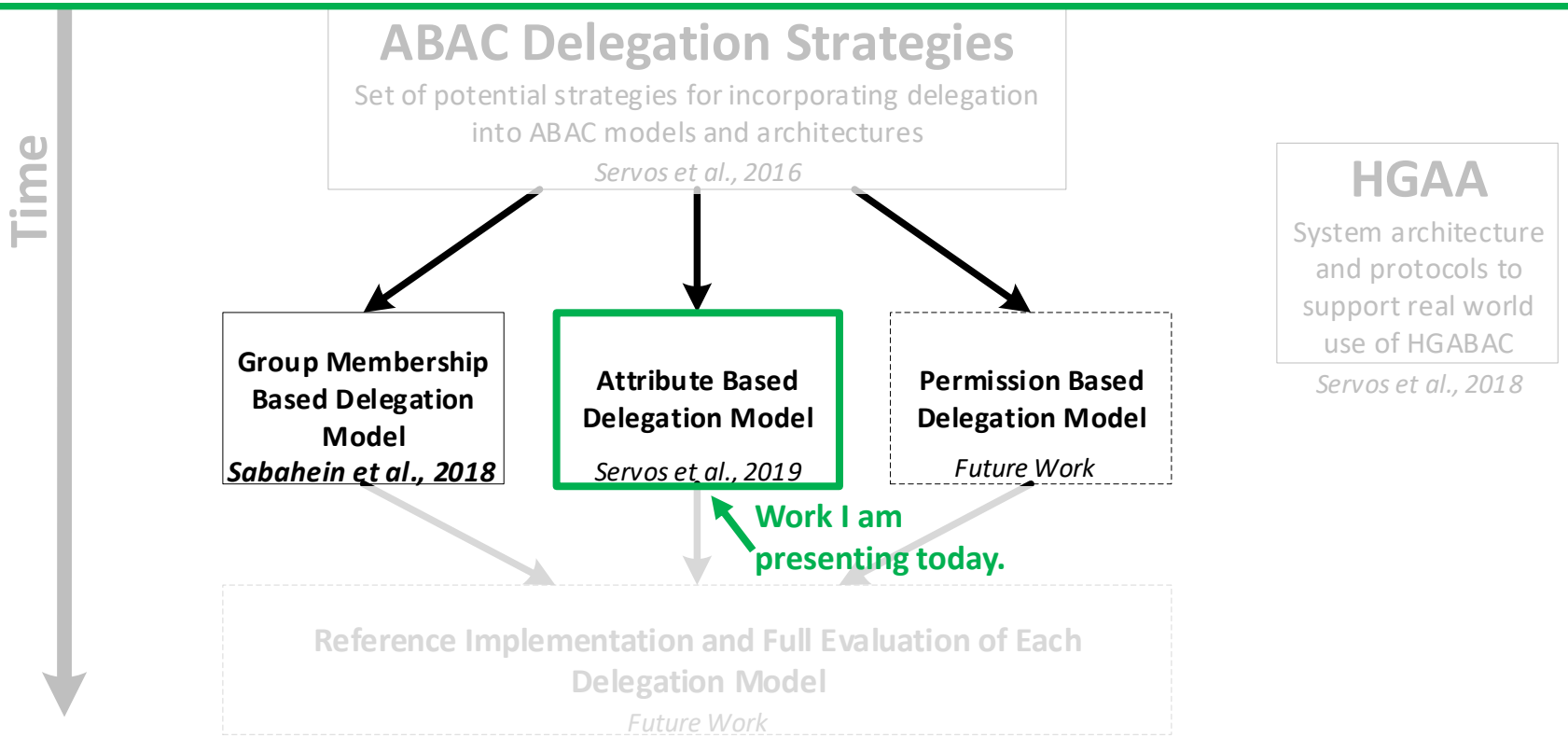
- System architecture and protocols for implementing an HGABAC based system.
- Answers questions like; *"Who assigns the attributes?"*, *"How are attributes shared?"*, *"How is proof of attribute ownership given?"*, and *"where and how are policies evaluated?"*
- Defines ***Attribute Certificate*** format, ***HGABAC Namespace***, and ***core services***.
- Focus on *"Off-Line"* function (no dependence on third party once attribute certificate issued).

HGAA
System architecture and protocols to support real world use of HGABAC
Servos et al., 2018

Future Work

Incorporating Off-Line Attribute Delegation into HGABAC (2019)

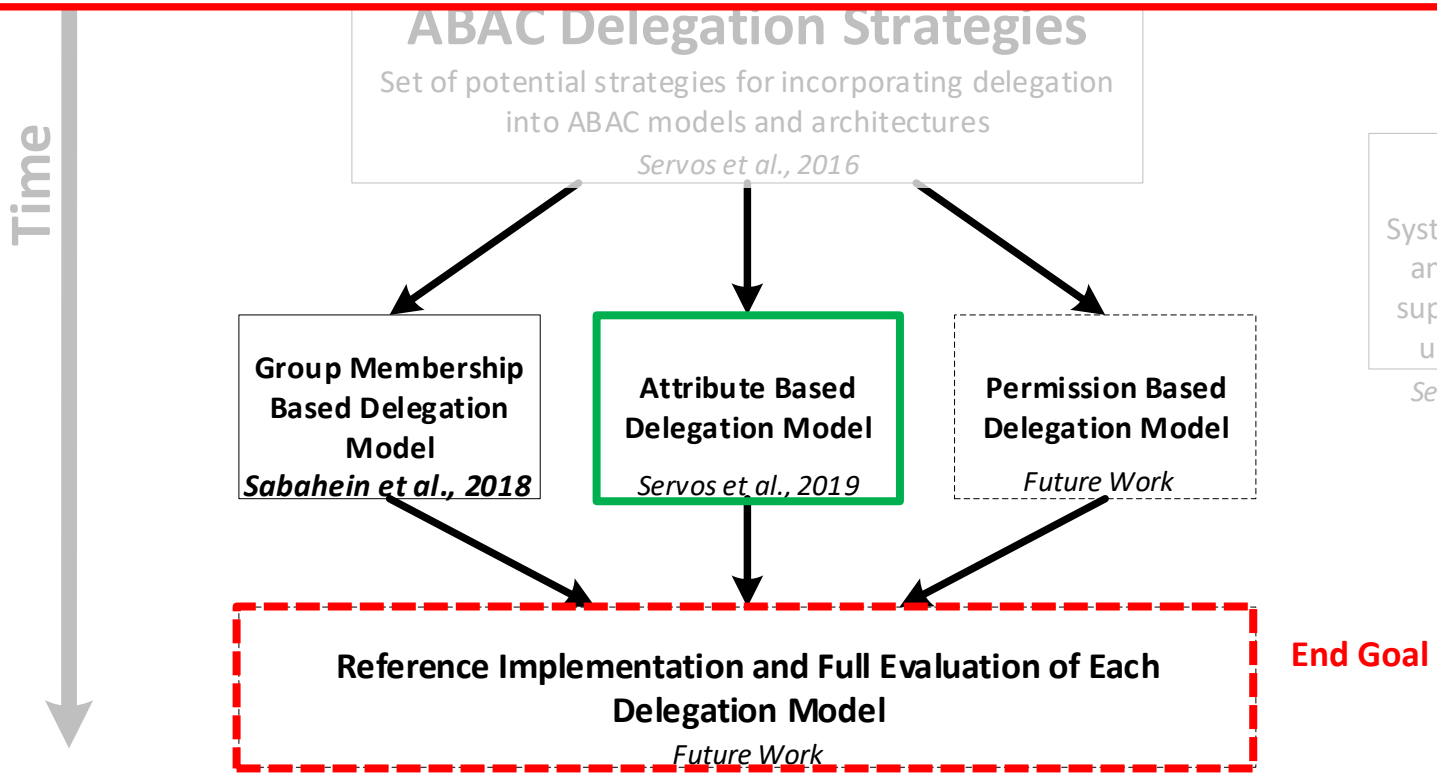
- Current effort, to create formal delegation model for each strategy.
- **Group Membership based model** created by *Sabahein et al.*
- Presenting **Attribute based model** today.
- **Permission based model** still in development.



HGABAC Project

End Goal for Delegation

- Formalization of each ABAC delegation model.
- Creation of reference implementation for each model.
- Full evaluation and comparison.

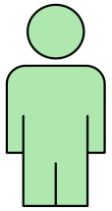


Attribute Delegation Model

Attribute Delegation Example

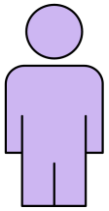
Year: *4*
Role: *undergrad*
Department: *CompSci*

Alice



Role: *faculty*
Department: *SoftEng*

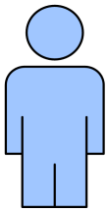
Bob



Year: *3*
Role: *grad*
Department: *SoftEng*

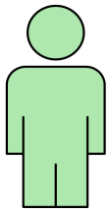
Charlie

Attribute Delegation Example



Year: *4*
Role: *undergrad*
Department: *CompSci*

Alice



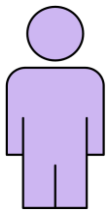
Role: *faculty*
Department: *SoftEng*

Bob

Alice wishes to delegate her access to the CS student lounge to **Charlie** so he can pick up a textbook for her.

The normal policy governing access is:

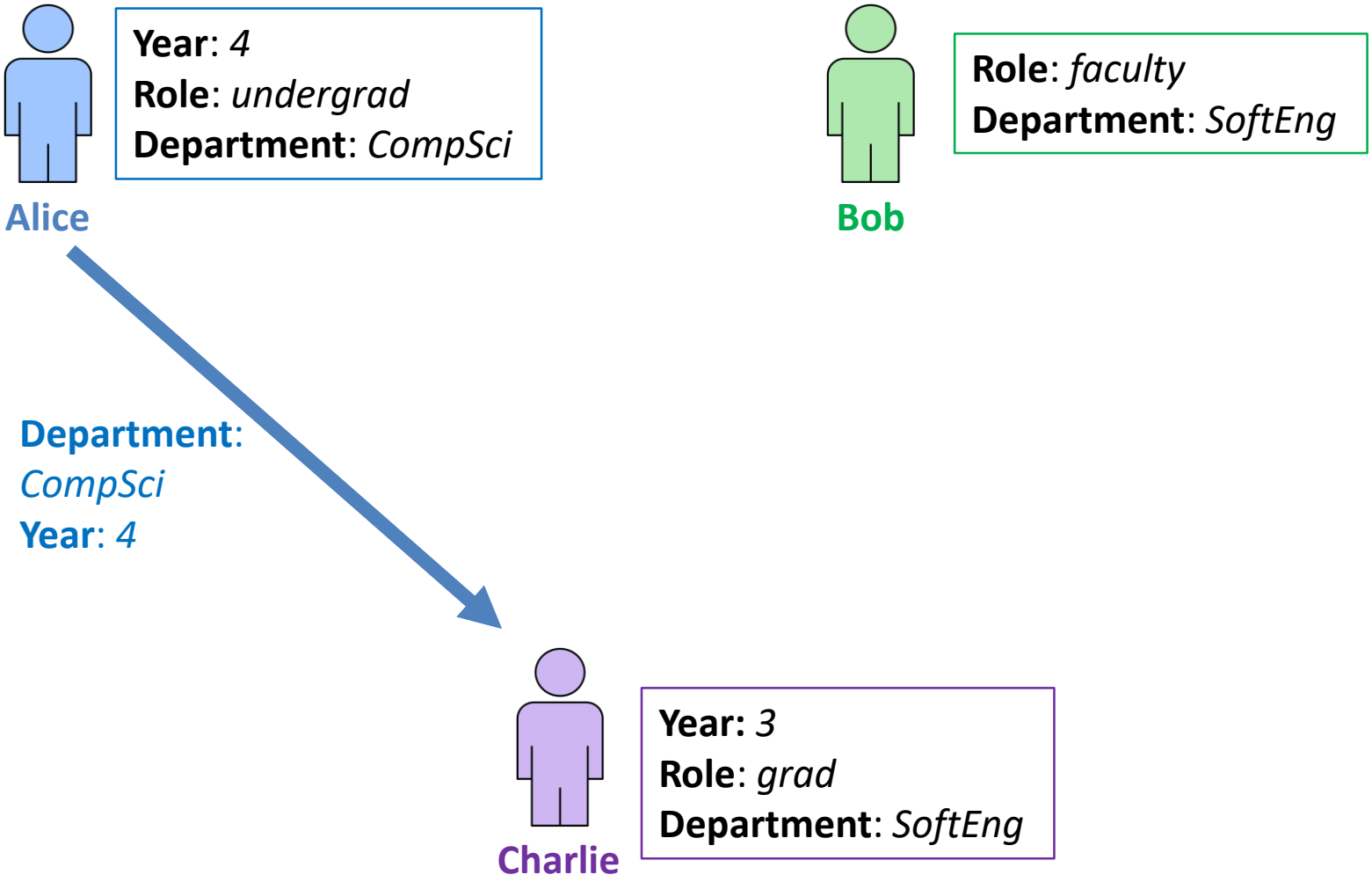
```
Department = "CompSci" AND year >= 4
```



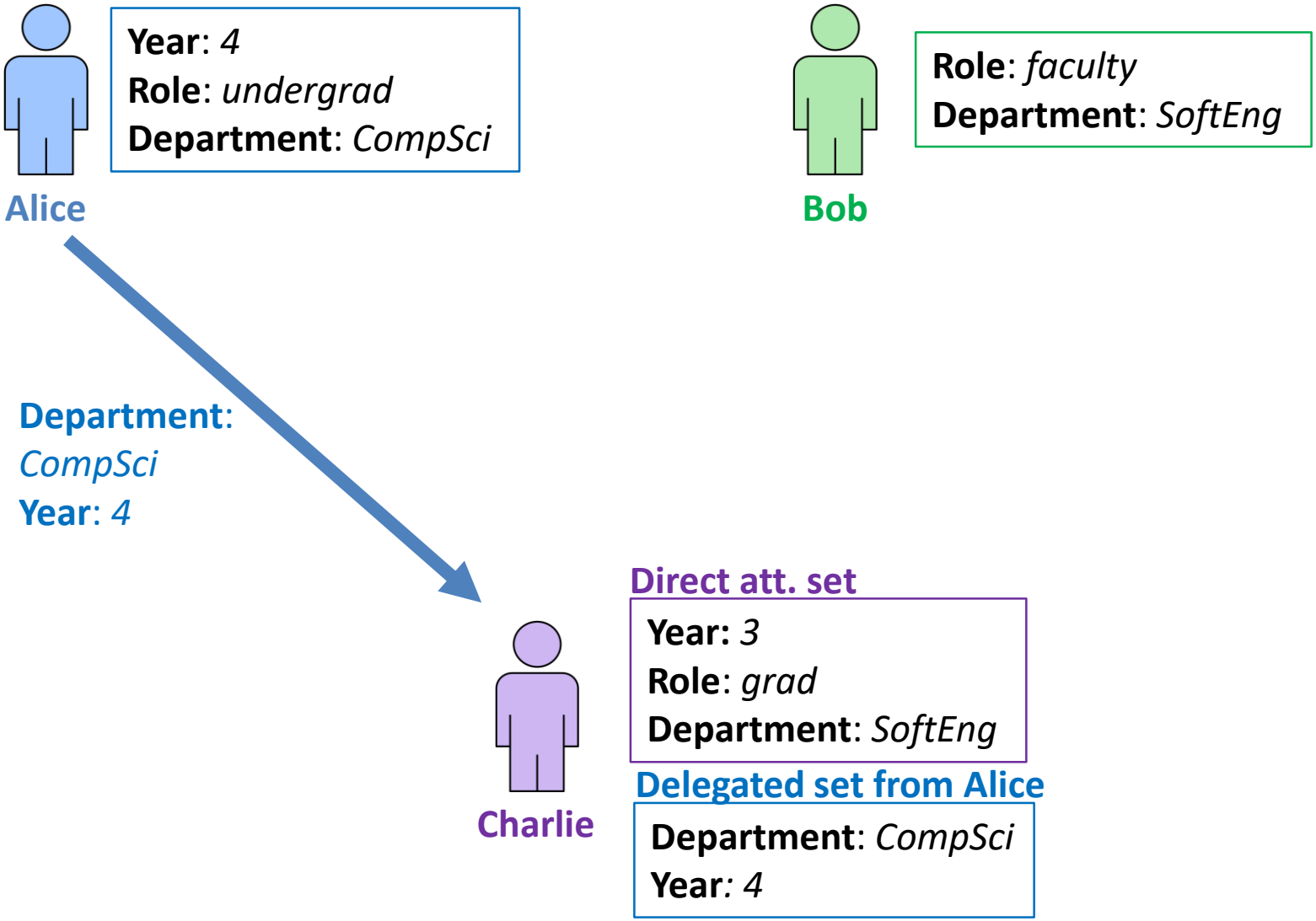
Year: *3*
Role: *grad*
Department: *SoftEng*

Charlie

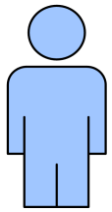
Attribute Delegation Example



Attribute Delegation Example

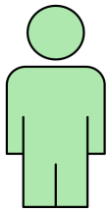


Attribute Delegation Example



Year: *4*
Role: *undergrad*
Department: *CompSci*

Alice



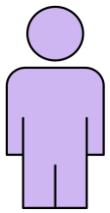
Role: *faculty*
Department: *SoftEng*

Bob

Bob wishes to delegate his access to the faculty software engineering lab to **Charlie** while **Bob** is away temporarily.

The normal policy governing access is:

```
Department = "SoftEng" AND Role = "faculty"
```



Charlie

Direct att. set

Year: *3*
Role: *grad*
Department: *SoftEng*

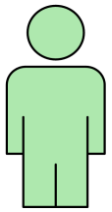
Delegated set from Alice

Department: *CompSci*
Year: *4*

Attribute Delegation Example

Year: *4*
Role: *undergrad*
Department: *CompSci*

Alice



Role: *faculty*
Department: *SoftEng*

Bob

Role: *faculty*
Department: *SoftEng*

Direct att. set

Year: *3*
Role: *grad*
Department: *SoftEng*

Charlie

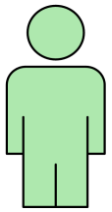
Delegated set from Alice

Department: *CompSci*
Year: *4*

Attribute Delegation Example

Year: *4*
Role: *undergrad*
Department: *CompSci*

Alice



Role: *faculty*
Department: *SoftEng*

Bob

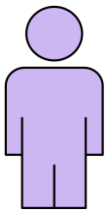
Role: *faculty*
Department: *SoftEng*

Direct att. set

Year: *3*
Role: *grad*
Department: *SoftEng*

Delegated set from Bob

Role: *faculty*
Department: *SoftEng*

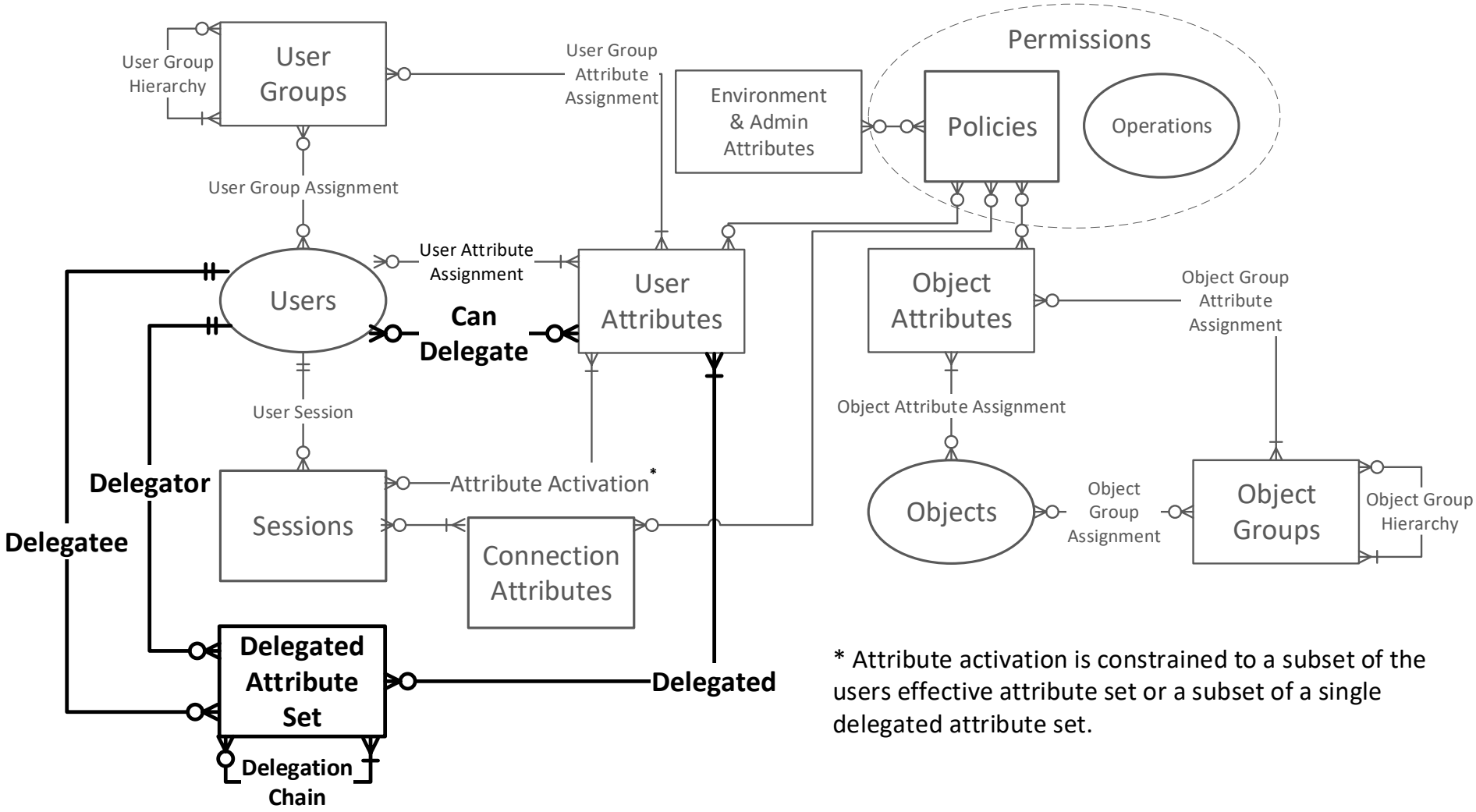


Charlie

Delegated set from Alice

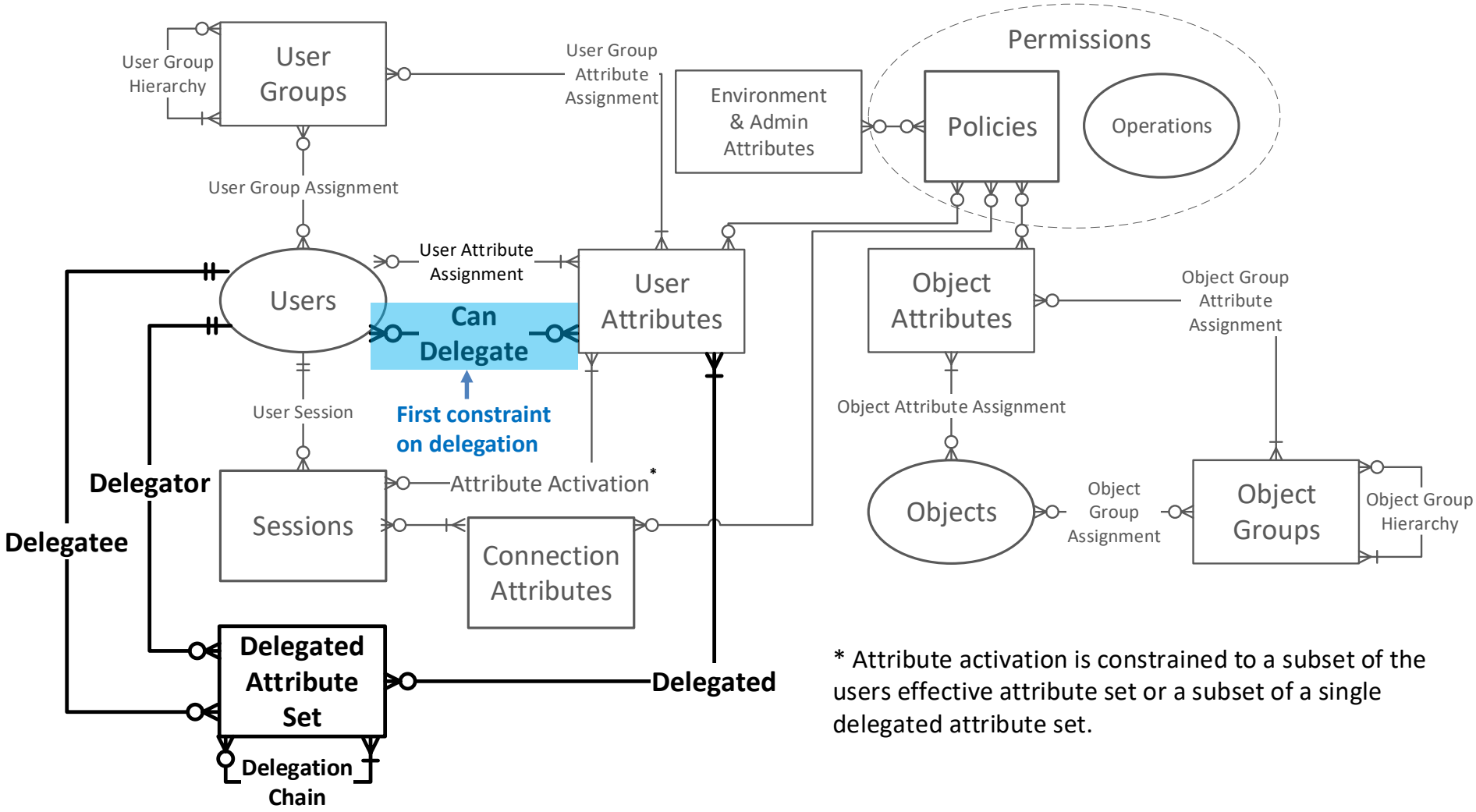
Department: *CompSci*
Year: *4*

Incorporating into HGABAC



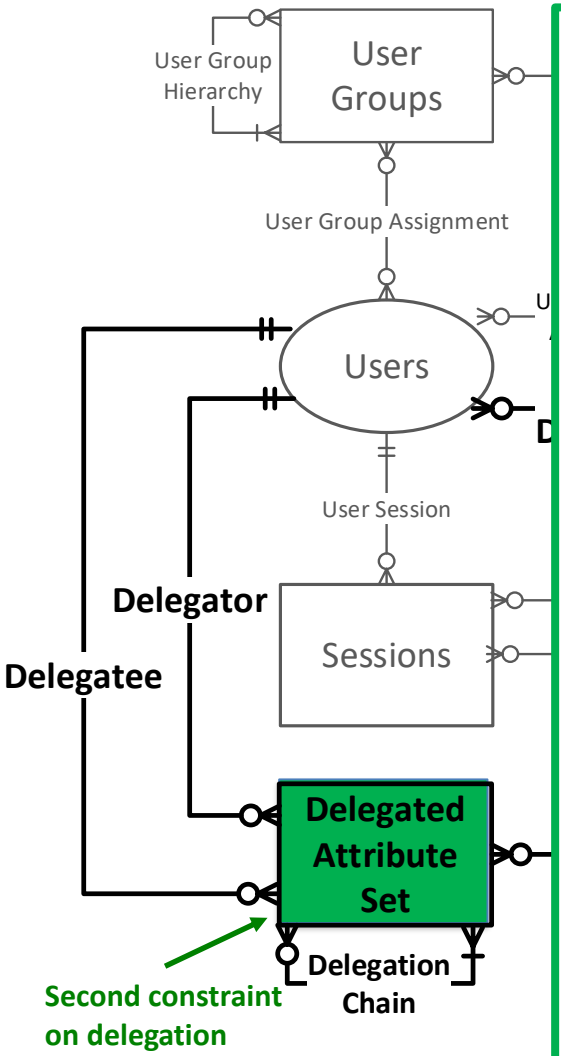
* Attribute activation is constrained to a subset of the users effective attribute set or a subset of a single delegated attribute set.

Incorporating into HGABAC



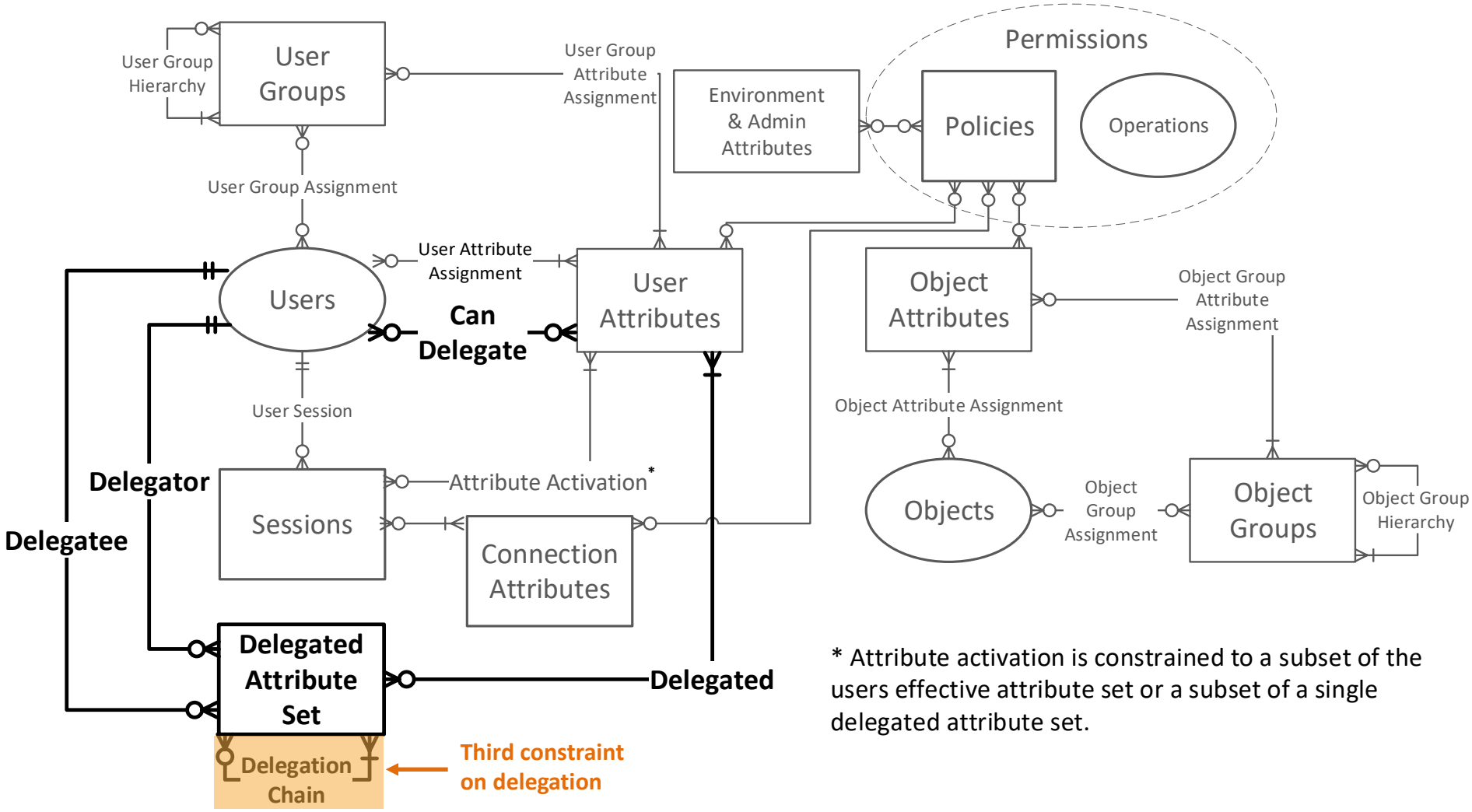
* Attribute activation is constrained to a subset of the users effective attribute set or a subset of a single delegated attribute set.

Incorporating into HGABAC



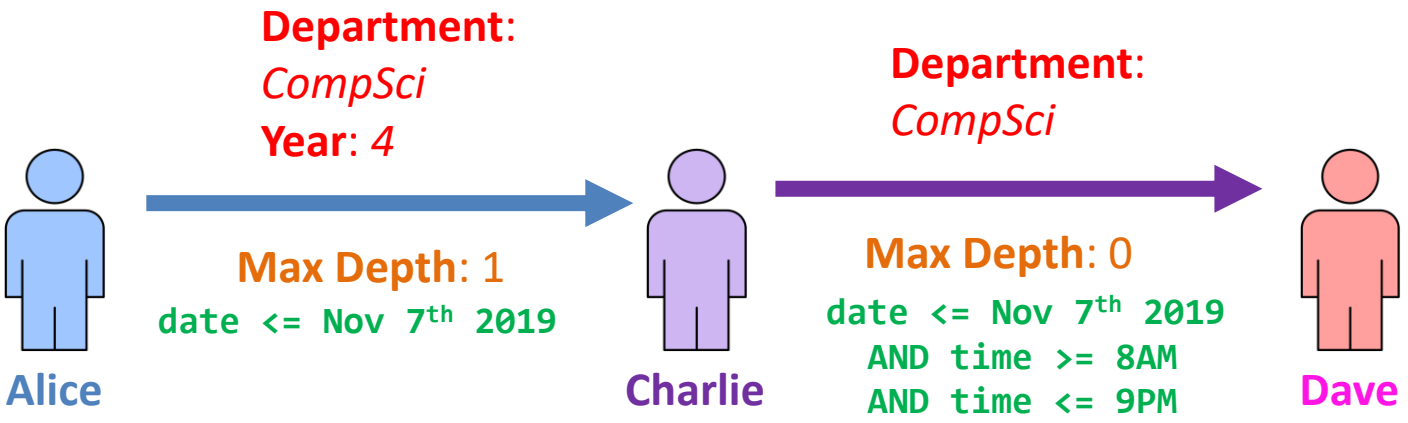
- Each delegated attribute set is issued with constraints in the form of a set of HGPL policies.
- If any policy in the set is not satisfied the delegation is considered revoked.
- These policy constraints can include environment, user and connection attributes.
- **Examples:**
  - `user.age > 18`
  - `connection.ip = 192.168.1.1`
  - `env.date <= Nov 7th 2019`

Incorporating into HGABAC



* Attribute activation is constrained to a subset of the users effective attribute set or a subset of a single delegated attribute set.

Delegation Chain



Constraints on Subsequent Delegations:

1. Can't have a depth deeper than that defined by the original delegator.
2. Each subsequent delegated attribute set must be $\subseteq$ the parent set.
3. Policy constraints on original delegation must be maintained or strengthened.

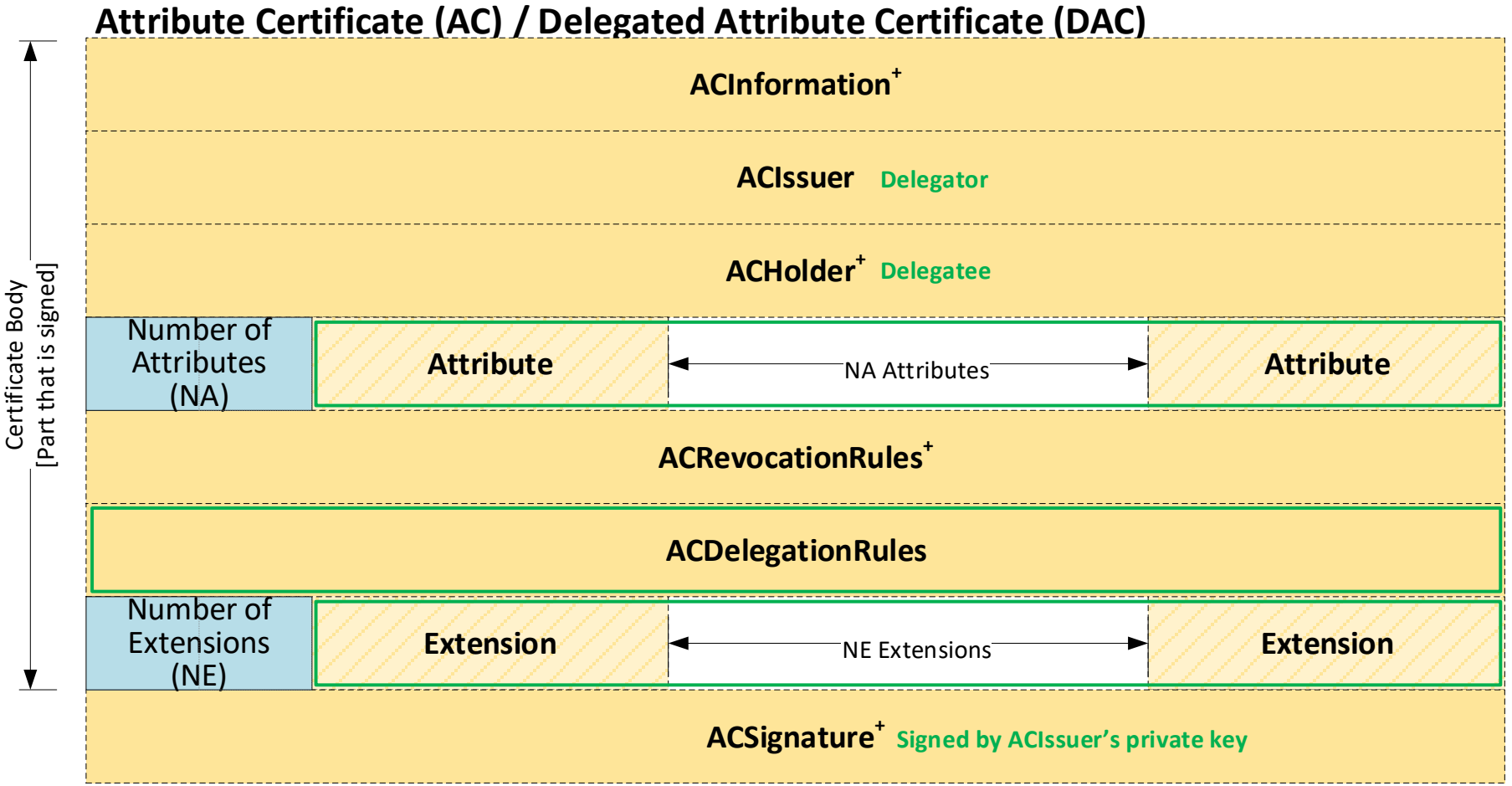
Attribute Delegation Framework

Attribute Delegation Framework

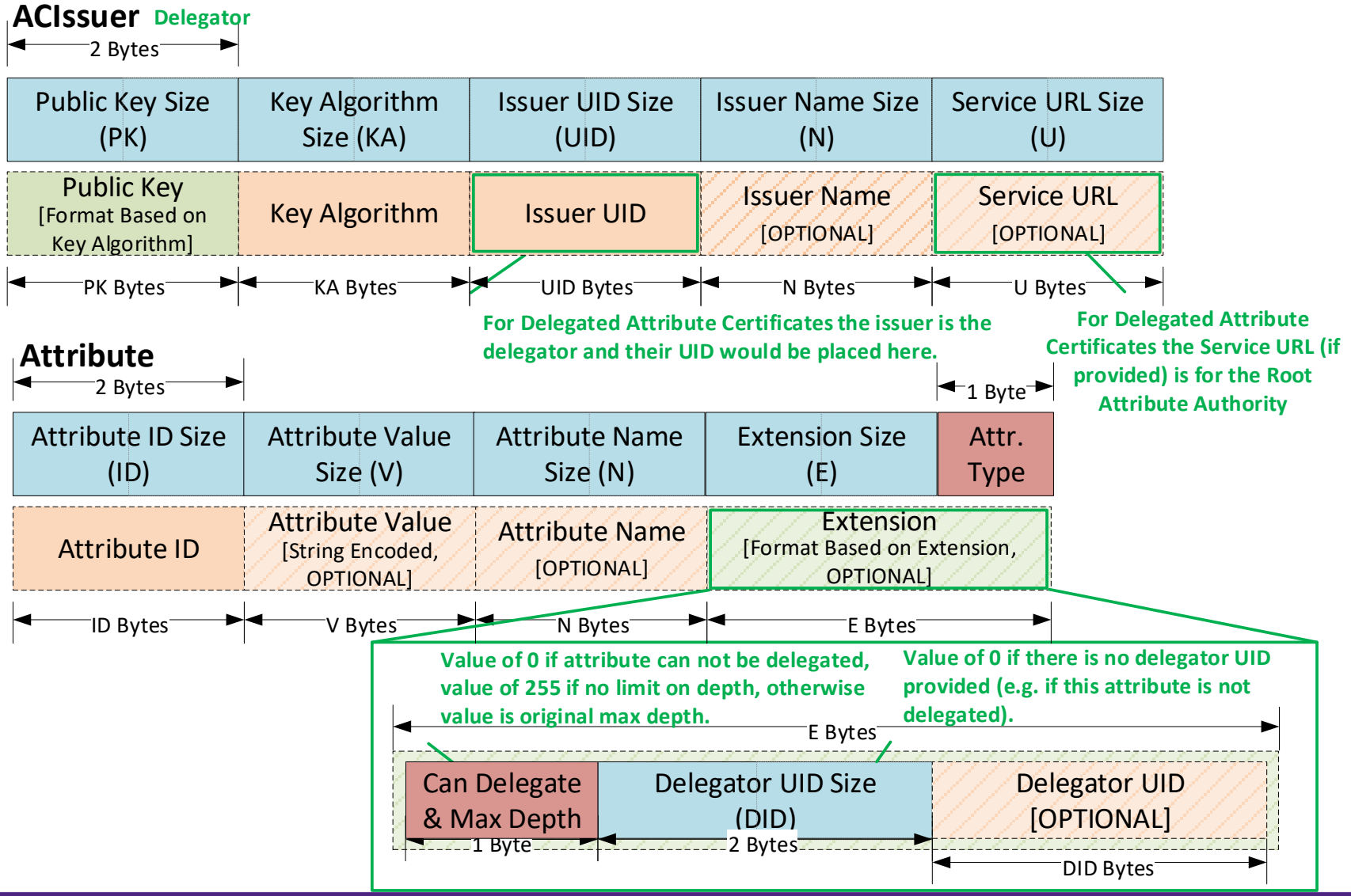
- Extended Hierarchical Group Attribute Architecture (HGAA) to support Attribute Delegation.
- Main additions are to the Attribute Certificate format.

- **HGAA Attribute Certificate:**
  - Cryptographically signed proof of a users attributes
  - Issued by Attribute Authority
  - Allow sharing attributes *"Off-Line"*

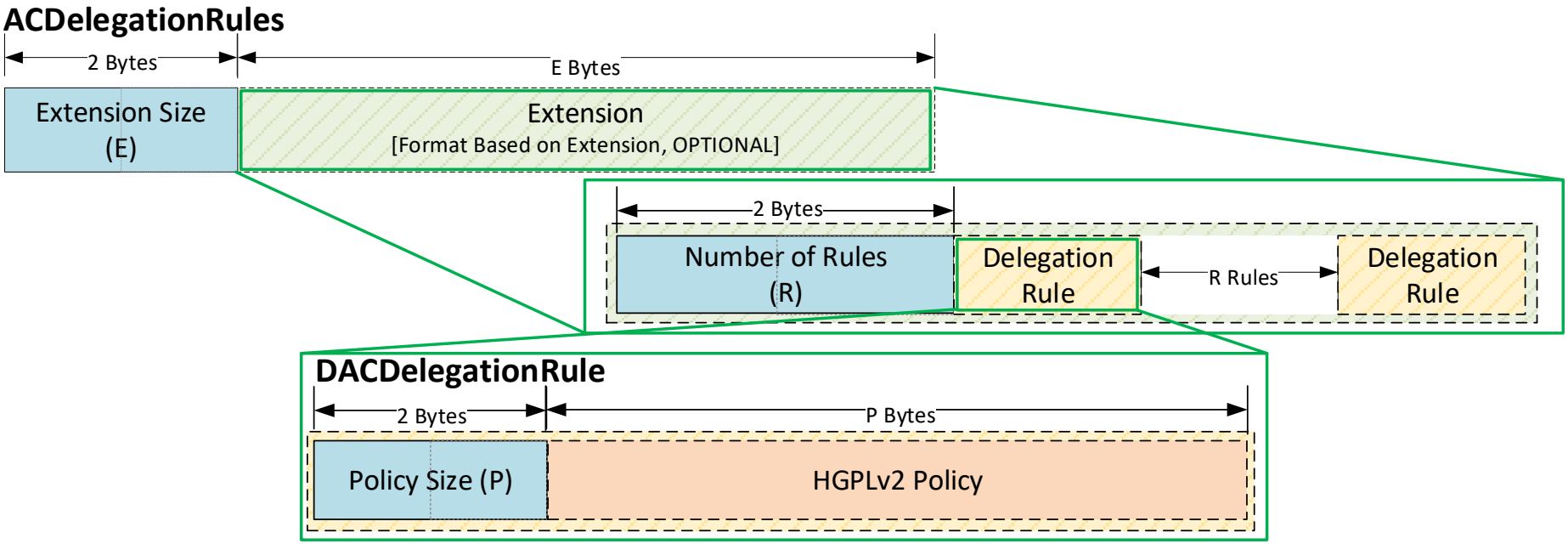
Attribute Certificate Extensions



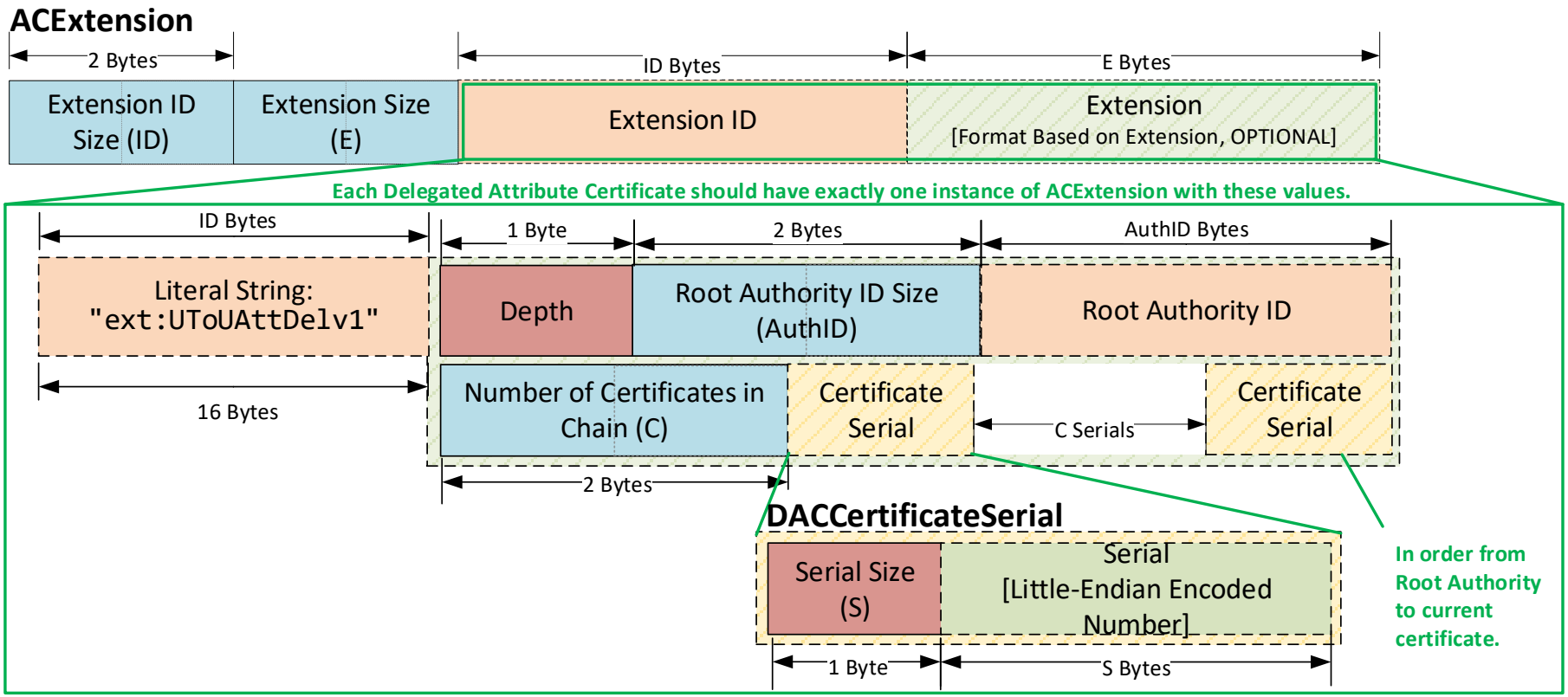
Attribute Certificate Extensions



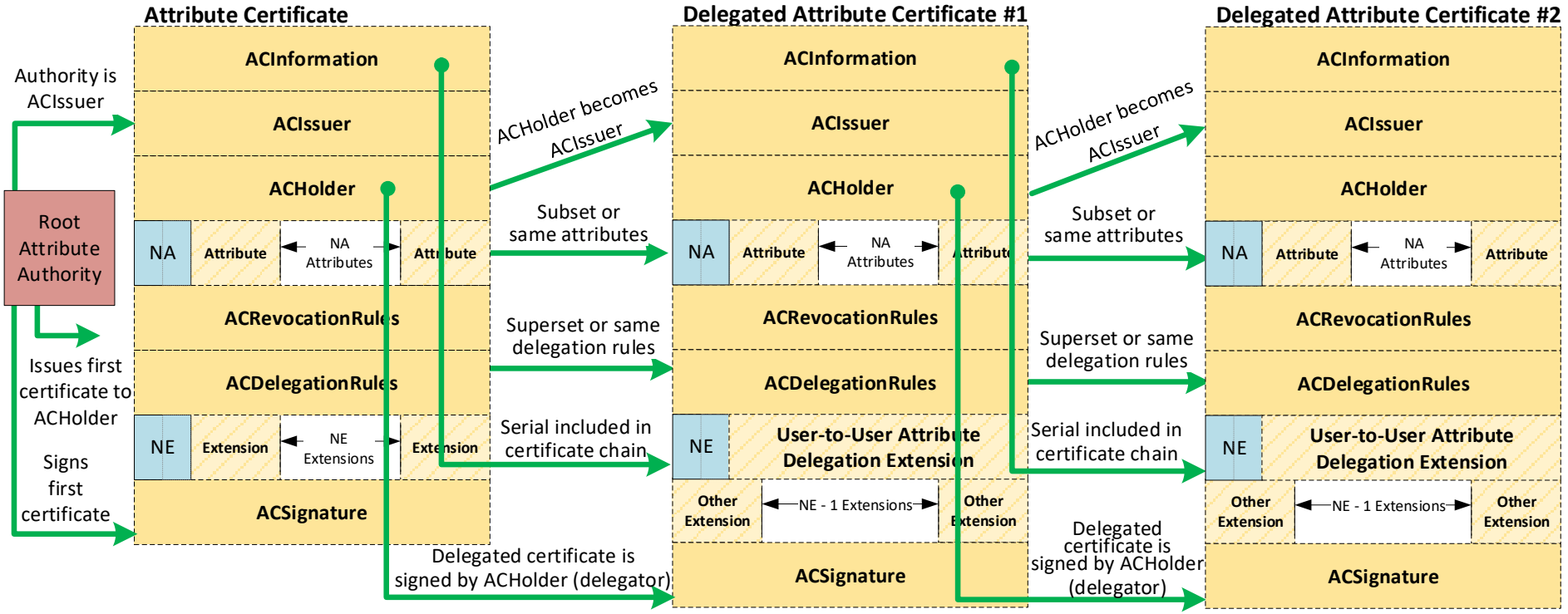
Attribute Certificate Extensions



Attribute Certificate Extensions



Delegated Certificate Chain



Delegation Revocation

- Revocation can happen in one of three ways:
  - Policy constraints are no longer satisfied
  - Certificate expires
  - Certificate added to revocation list (optional feature)
- Revocations are **cascading** but **not live**:
  - If parent certificate in chain is revoked, all descendants are as well.
  - Revocation is evaluated only when certificate is validated (maybe no feedback to issuer/delegator).

Conclusions & Future Work

Conclusions

- First model of User-to-User Attribute Delegation.
- Extensions to HGABAC and HGAA to support Attribute Delegation.
- Backwards compatible update to Attribute Certificate format.
- Support for *"off-Line"* authentication and policy evaluation.

Directions for Future Work

For Attribute Delegation:

- Explore using *"Can Receive"* relation in place of *"Can Delegate"* in current model.
- More thorough evaluation: formal validation and experimental evaluation.
- Useability and user comprehension issues.

For ABAC delegation strategies:

- Formalization of permission delegation model.
- Reference implementation of each delegation model.
- Full evaluation and comparison of each strategy.

Thank You for Listening!

Past papers and slides related to the HGABAC project can be found on my website:

http://cs1.ca