

A Privacy Oriented Attribute Exchange in Shibboleth

Grid-Middleware Workshop, 23rd APAN
Meeting, Manila, Philippines, Jan. 25, 2007

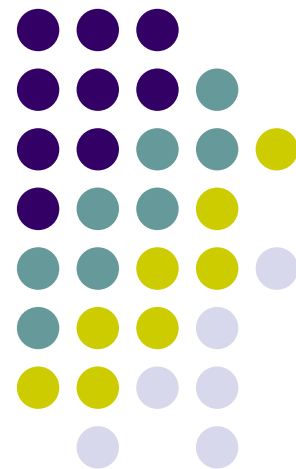
Shoichirou FUJIWARA†

Takaaki KOMURA†† Yasuo OKABE††

† : Graduate School of Informatics, Kyoto Univ.

†† : Academic Center for Computing and
Media

Studies, Kyoto Univ.





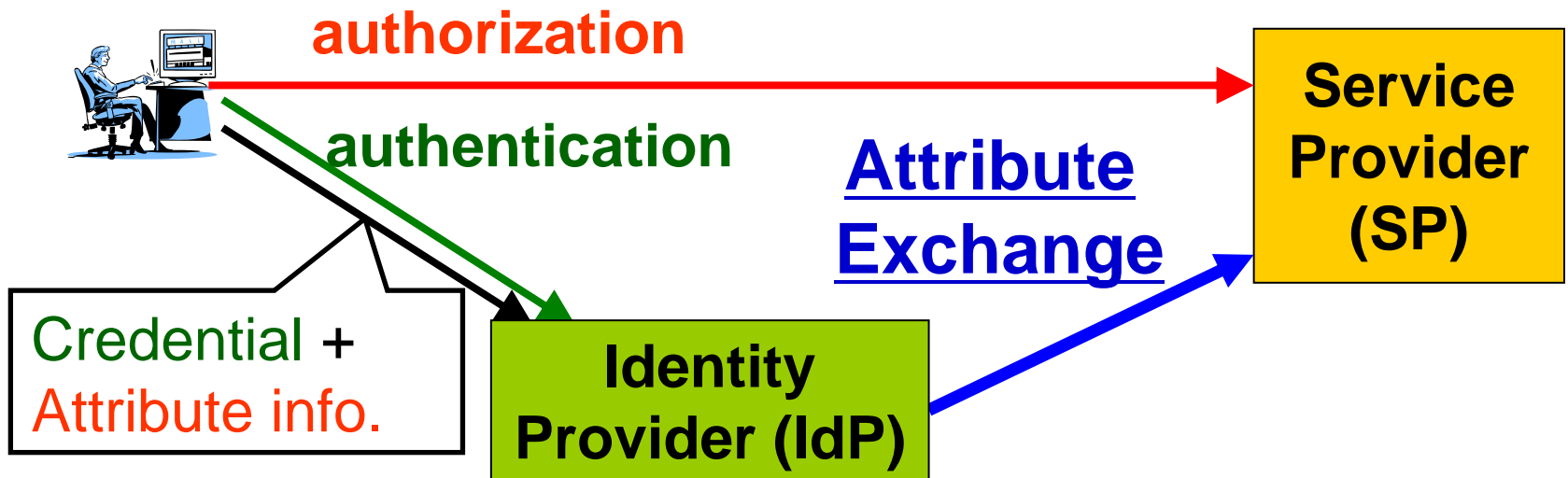
Agenda

- Outline of our work: extending attribute exchange to enhance privacy in Shibboleth ←
- Design and implementation
- Summary and future works



Background

- Necessary processes and a deployment framework for Web services

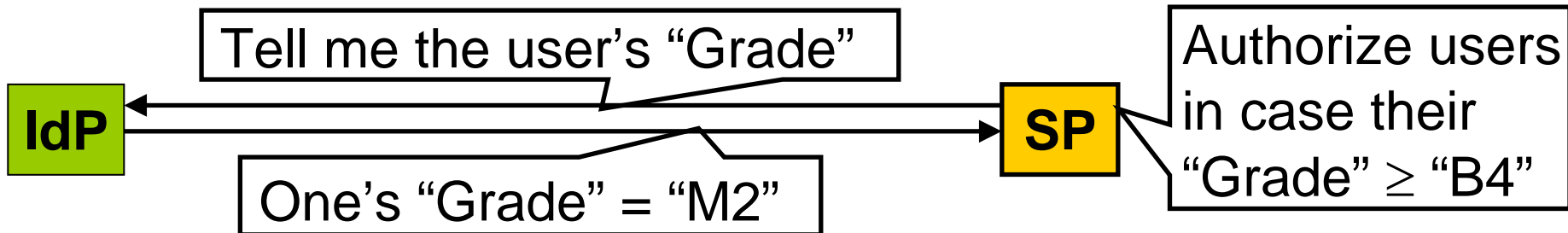


- Identity: Information required for AuthN/AuthZ
- Shibboleth: a project of Internet2/MACE

What we did: Extension of Attribute Exchange in Shibboleth



- Current protocol

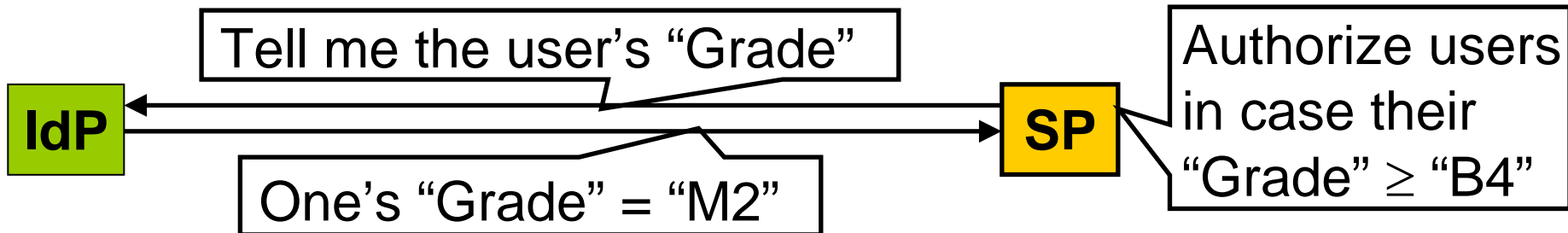


- **privacy risk: attribute information for the SP is often unnecessarily detailed**

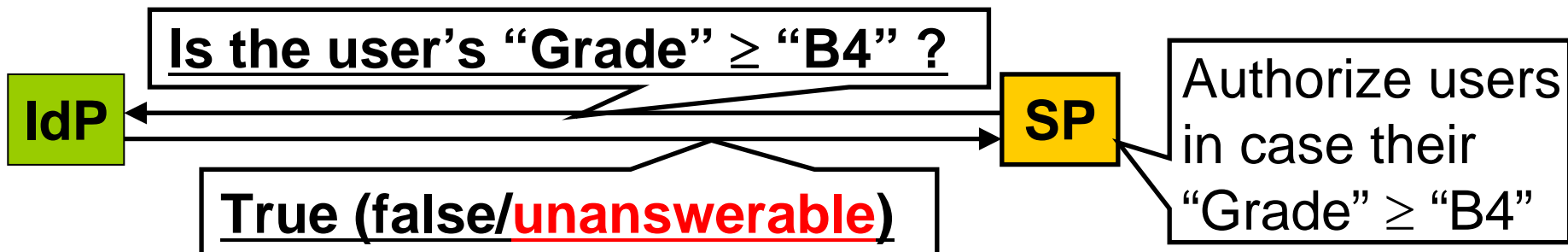
What we did: Extension of Attribute Exchange in Shibboleth



- Current protocol



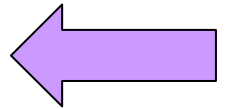
- **privacy risk: attribute information for the SP is often unnecessarily detailed**
- Proposal: SP presents AuthZ conditions





Agenda

- Outline of our work: extending attribute exchange to enhance privacy in Shibboleth
- **Design and implementation**
- Summary and future works



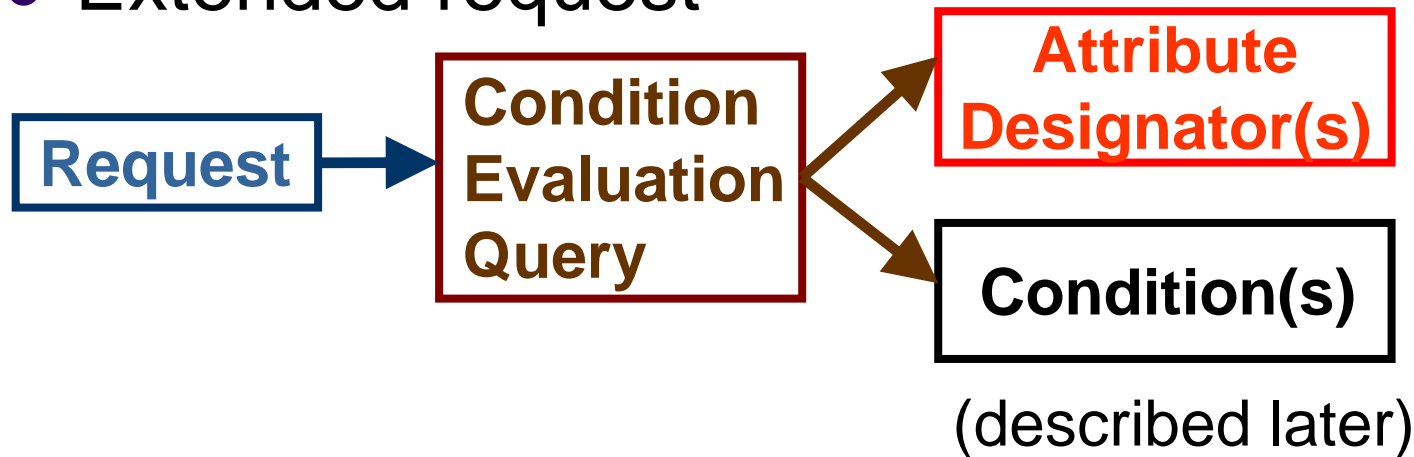
Protocol Message Extension (Request from SPs to IdPs)



- Existing attribute request



- Extended request



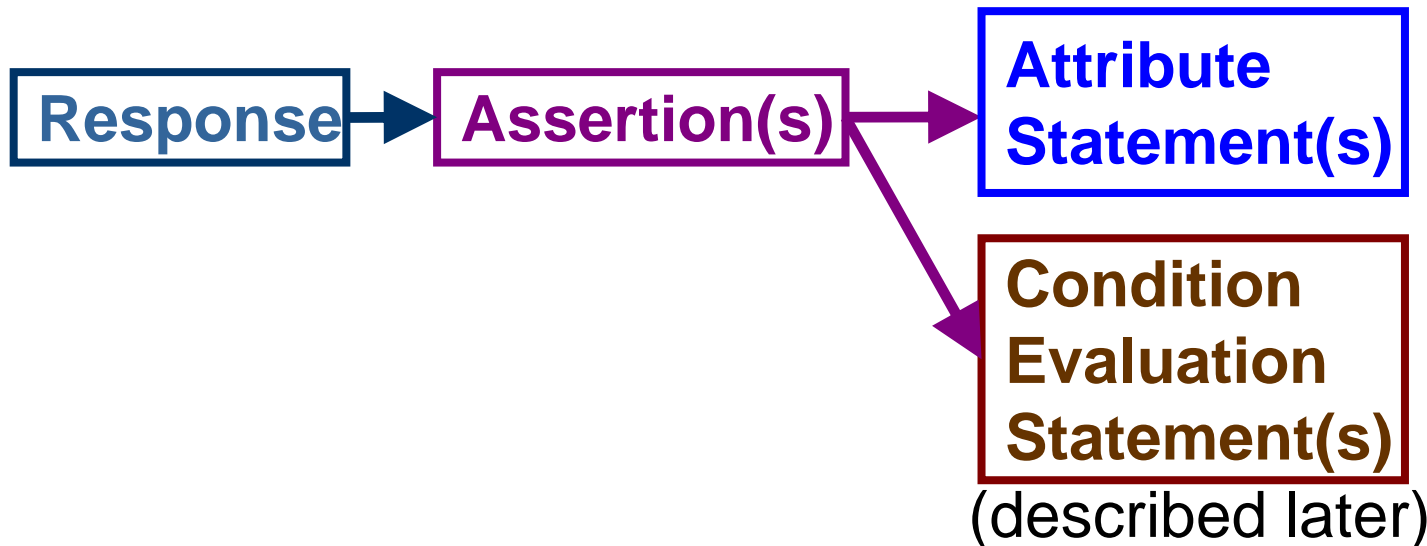
Protocol Message Extension (Response from IdPs to SPs)



- Existing response to attribute request



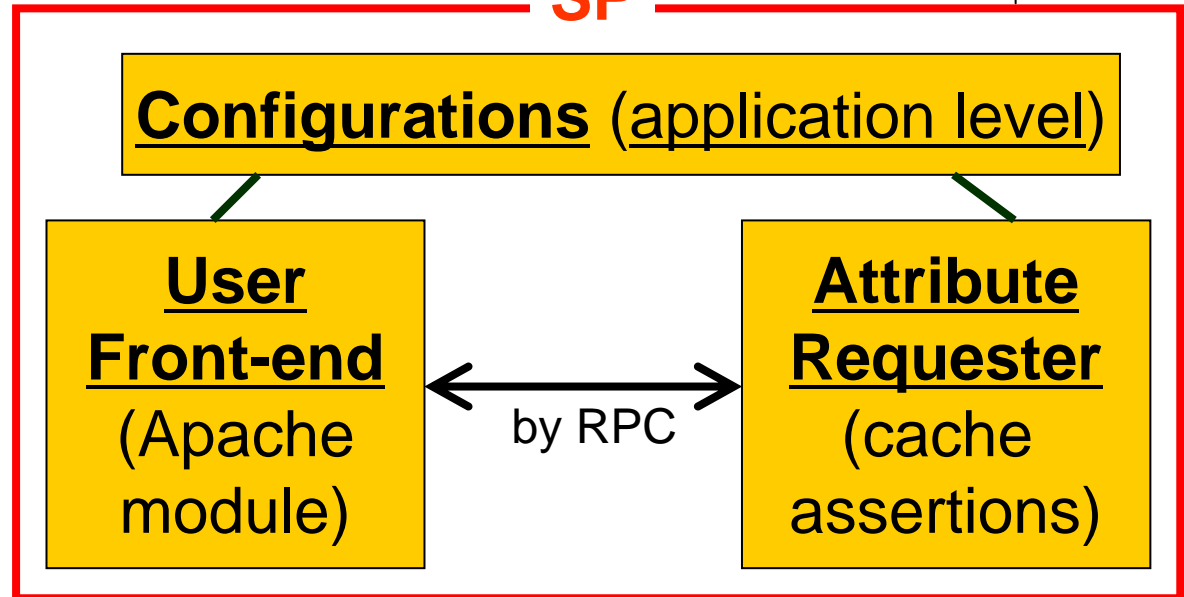
- Extended response





Protocol in detail

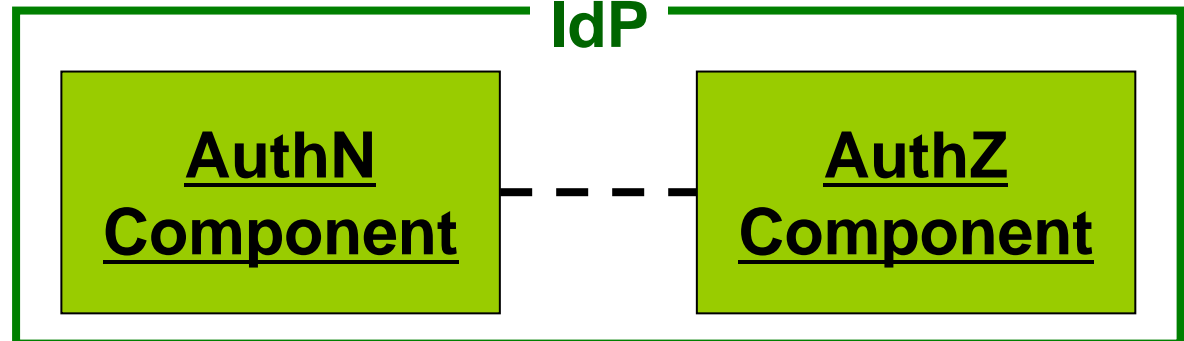
SP



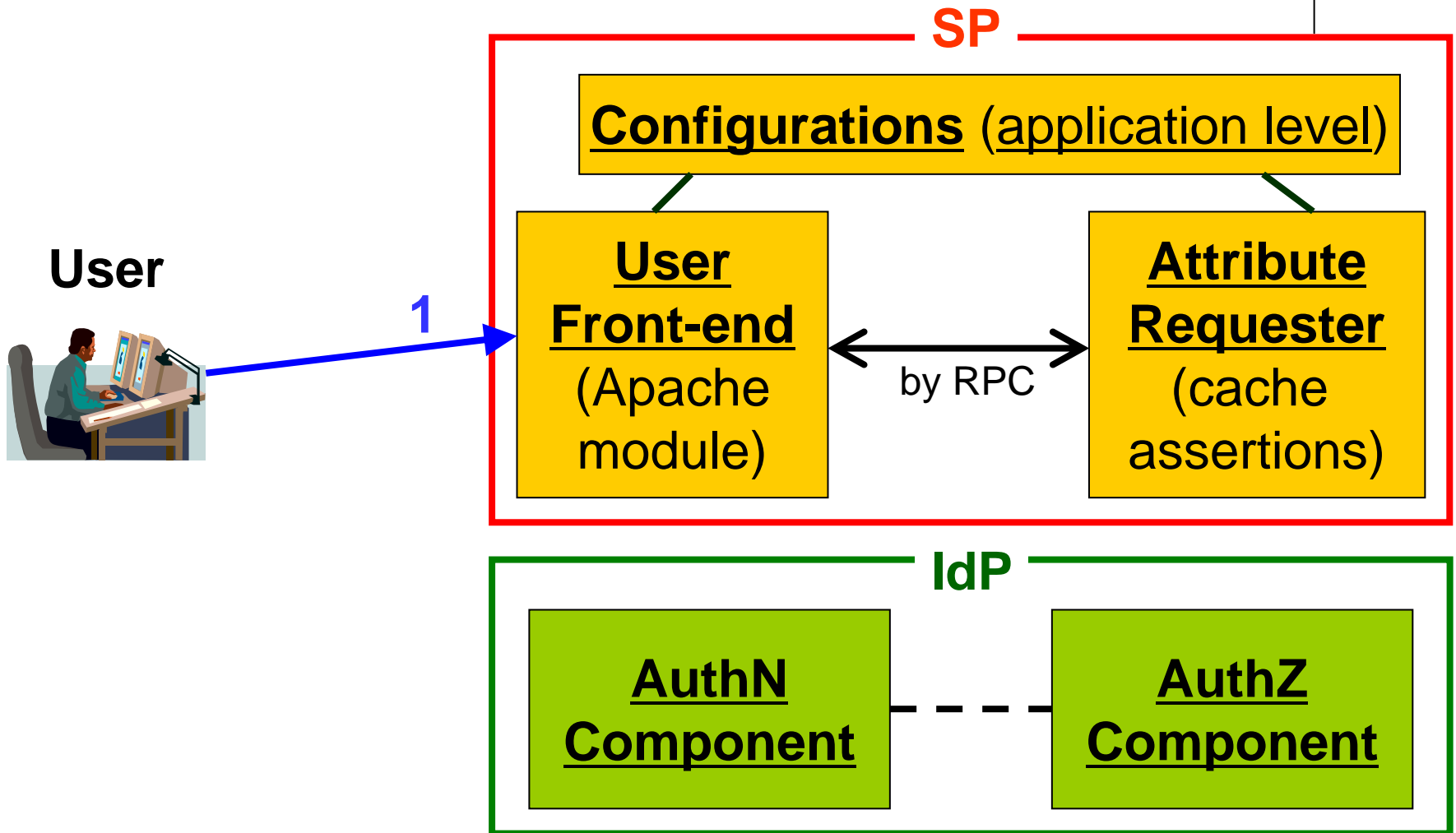
User



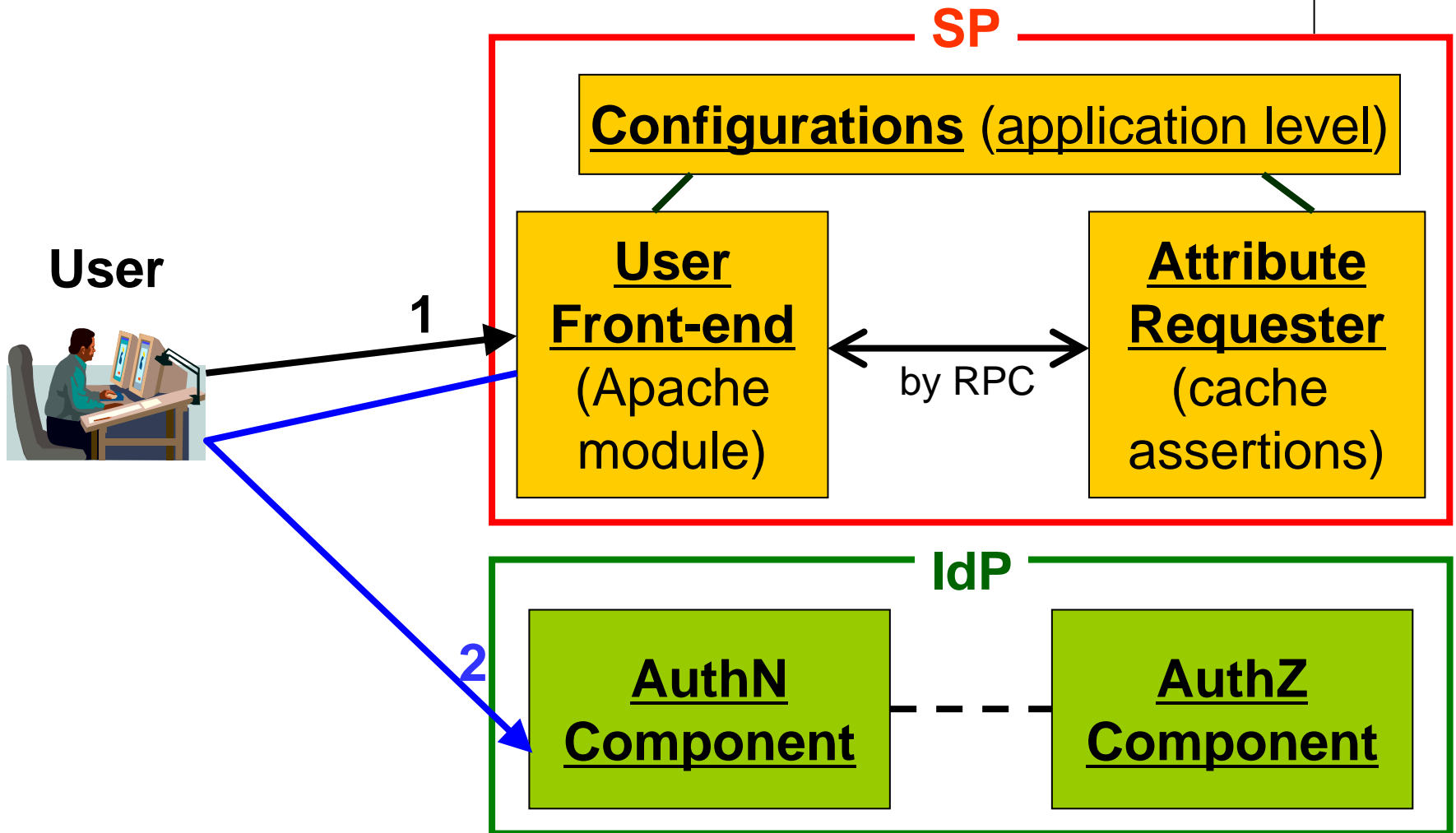
IdP



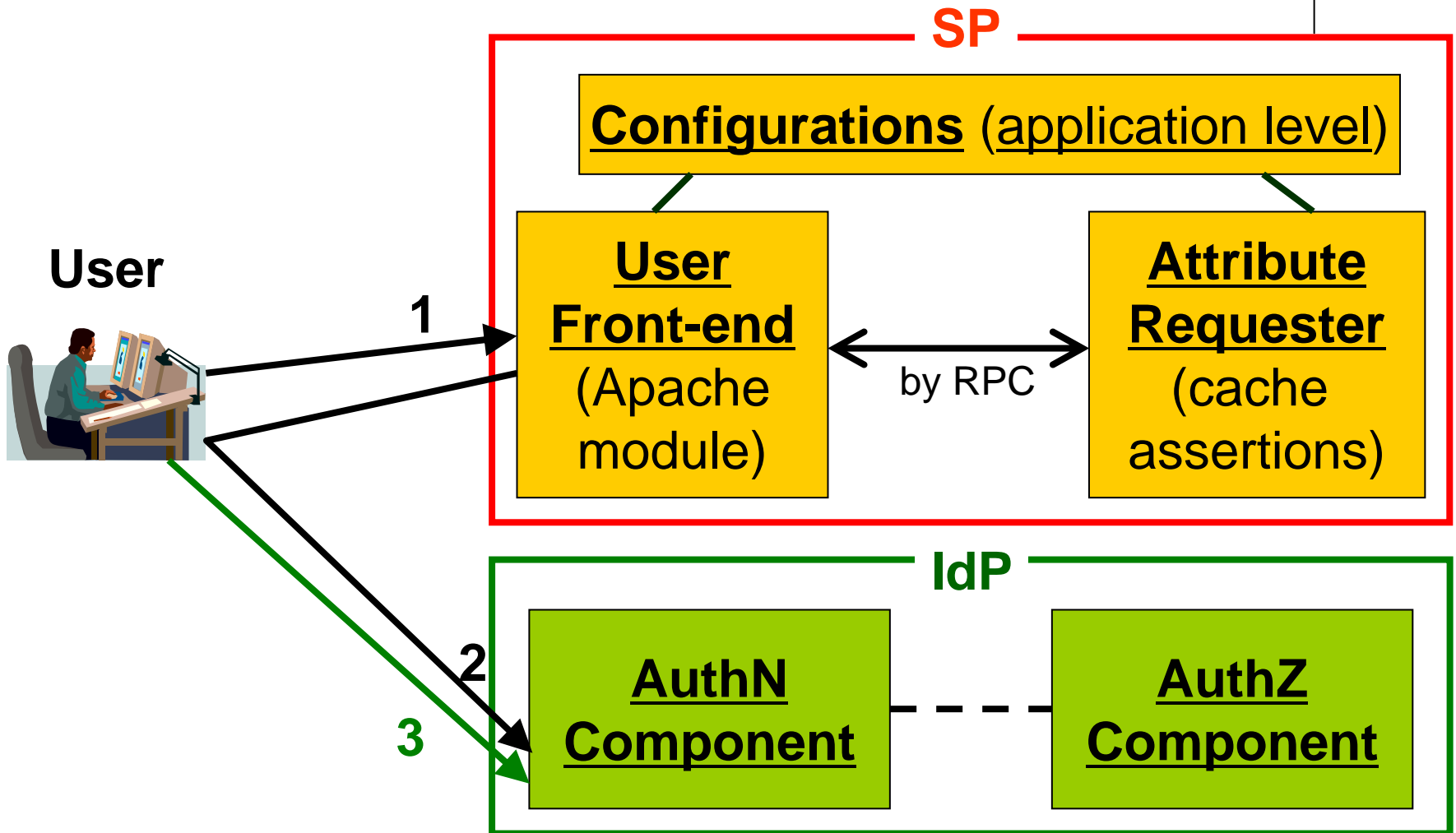
Protocol in detail



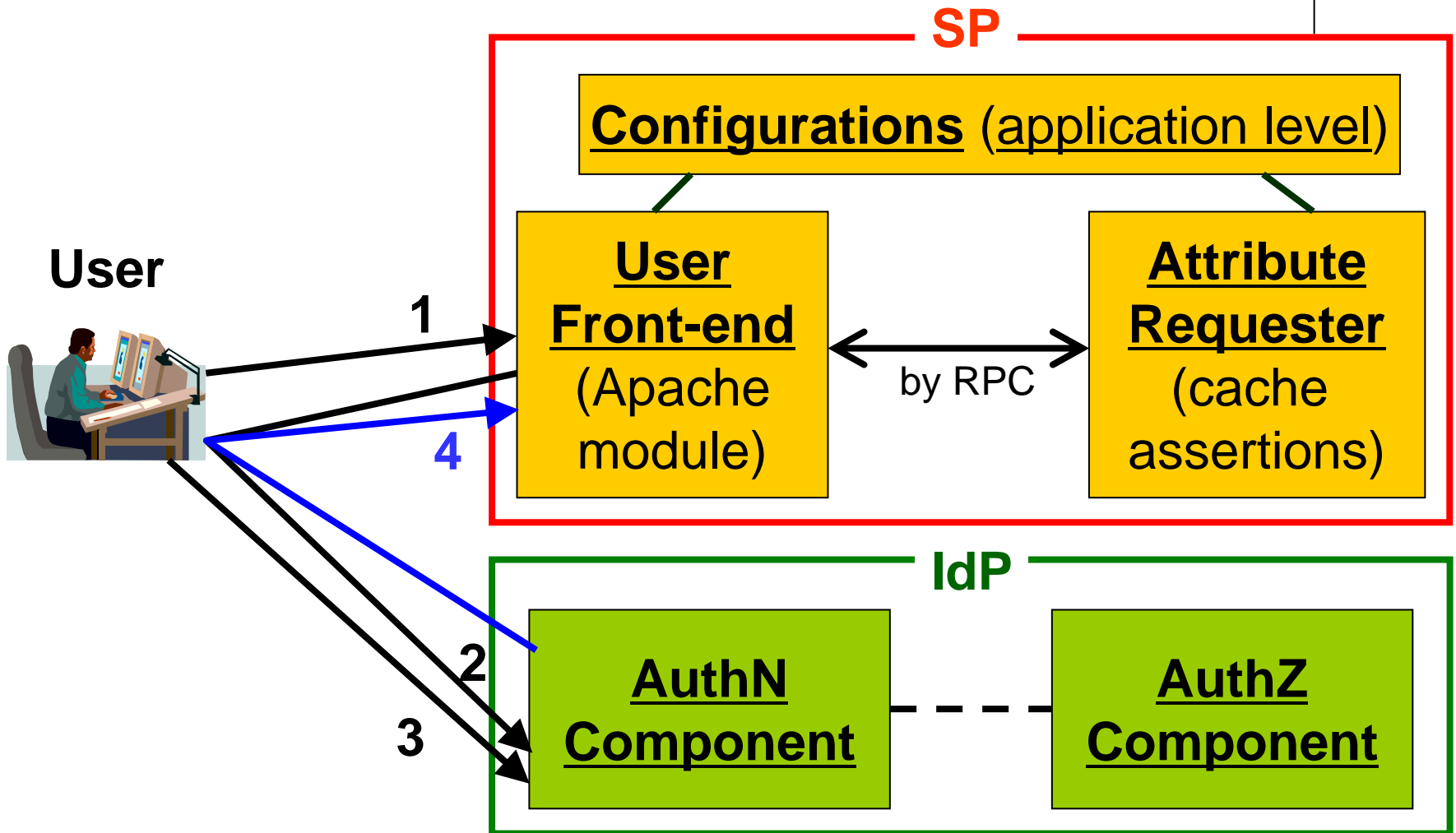
Protocol in detail



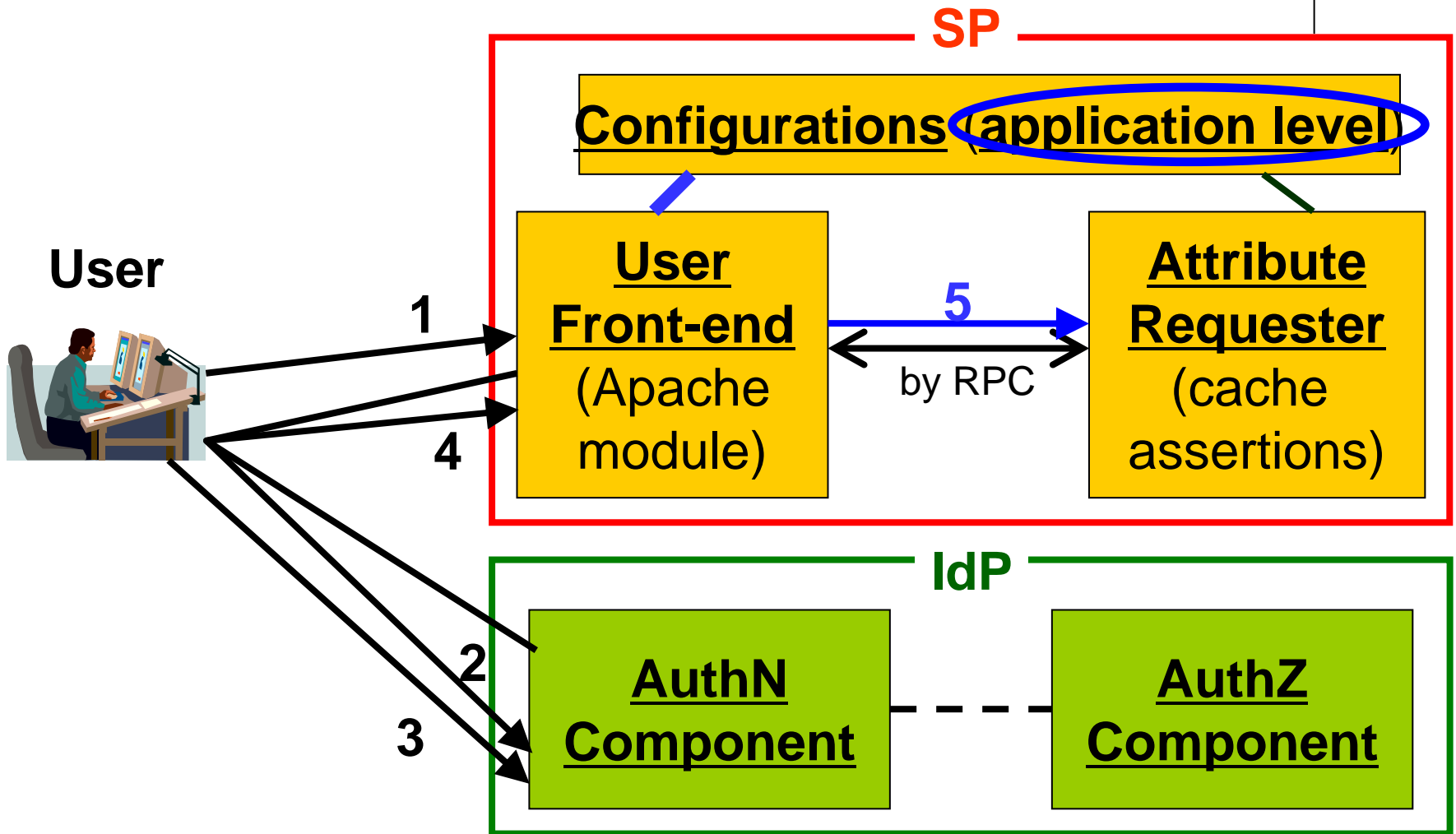
Protocol in detail



Protocol in detail

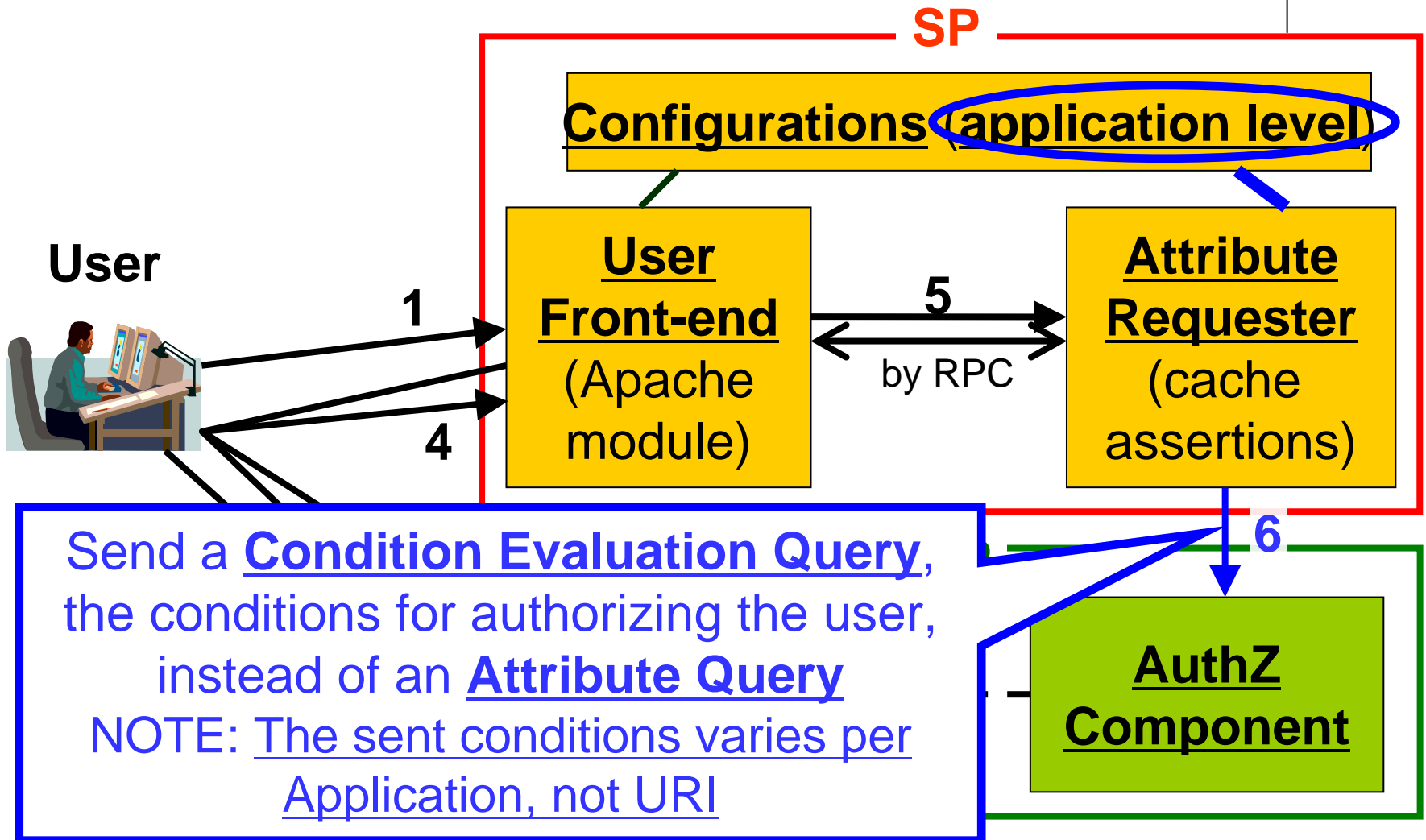


Protocol in detail



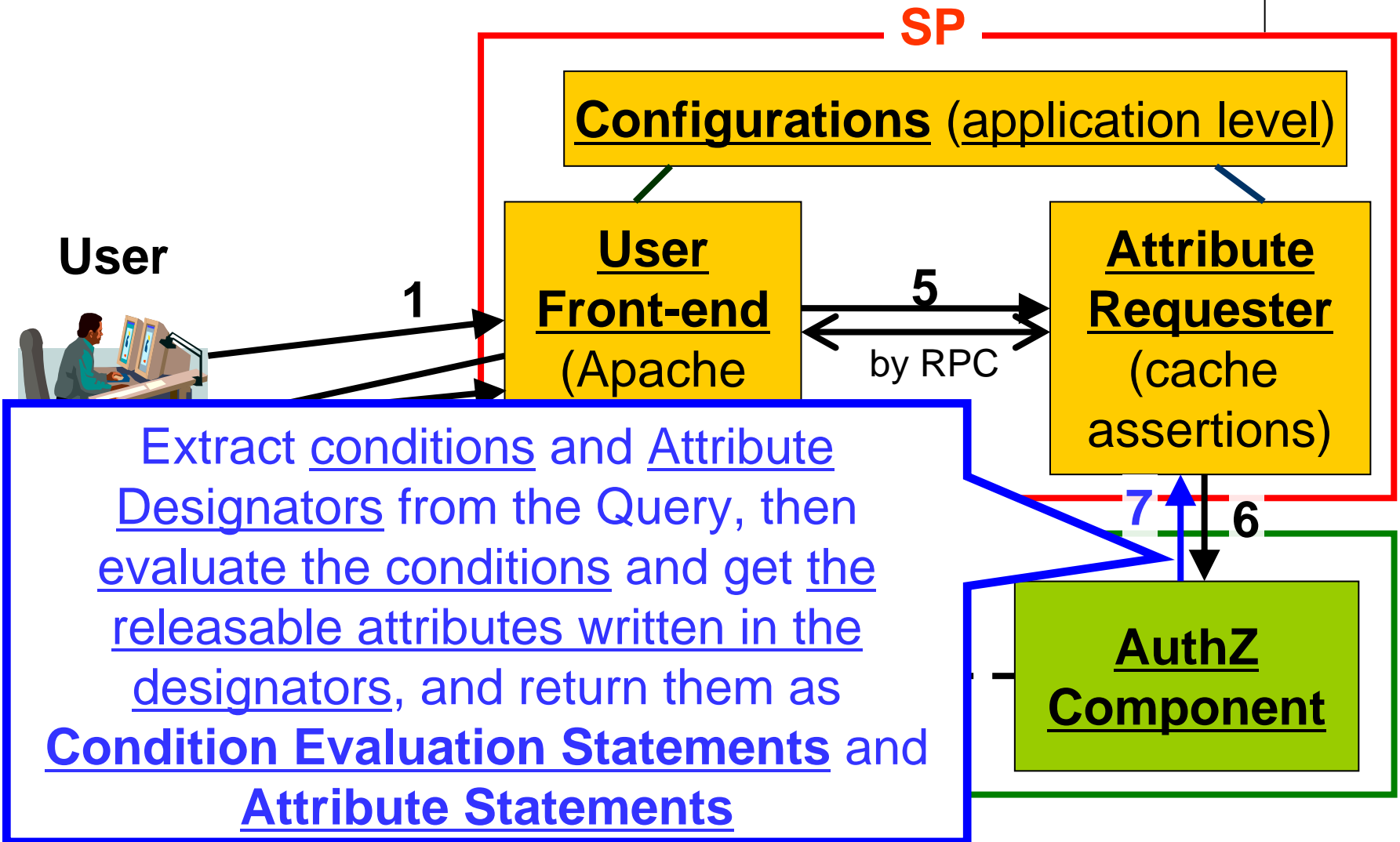


Protocol in detail



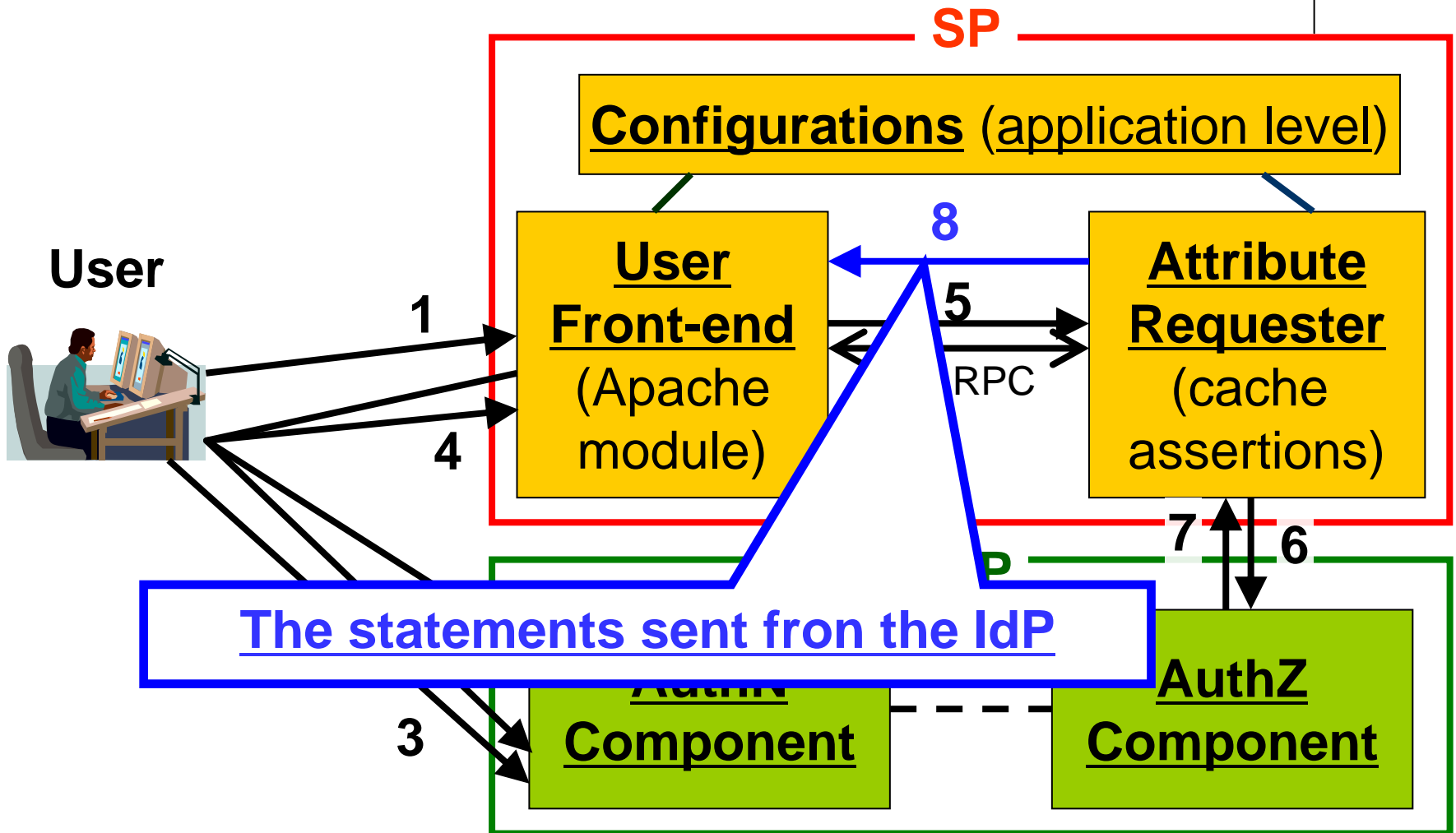


Protocol in detail



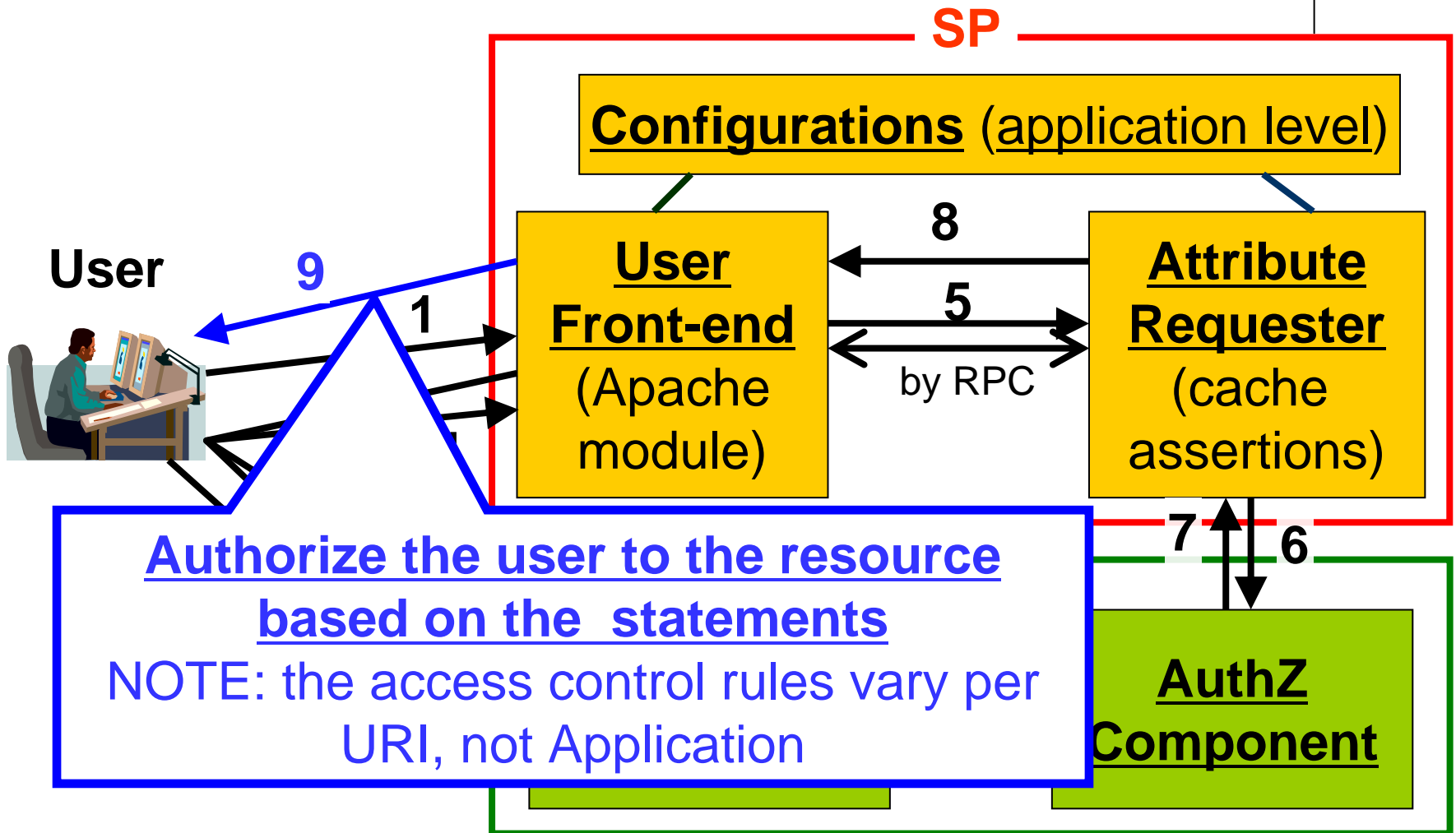


Protocol in detail





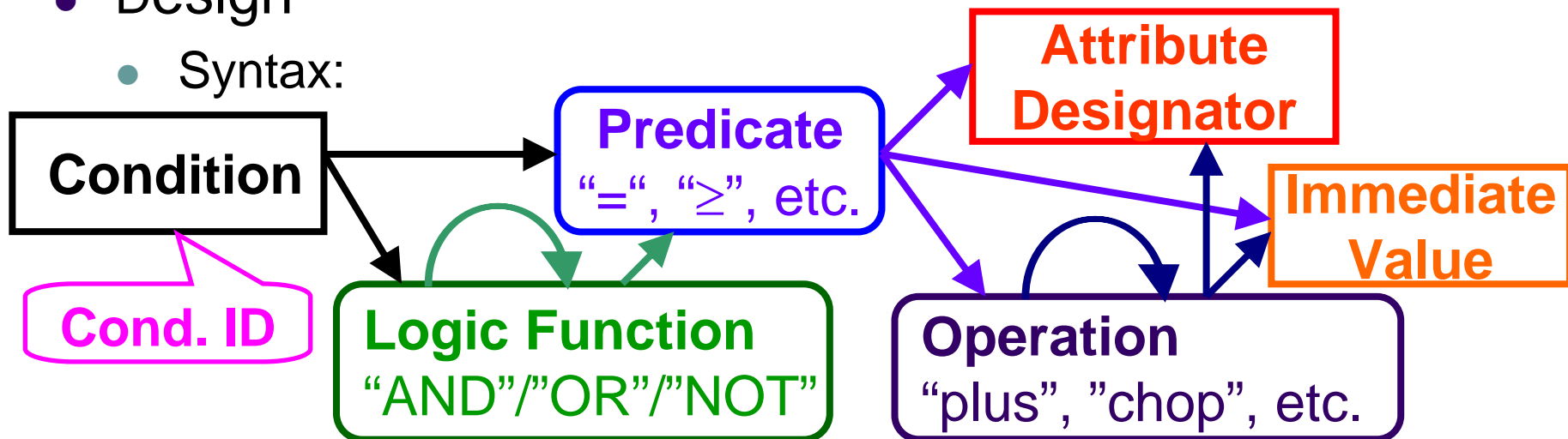
Protocol in detail



Language for Describing the Conditions



- Points
 - What to describe: AuthZ conditions about attributes
 - Compactness: XACML is too complicated
- Design
 - Syntax:

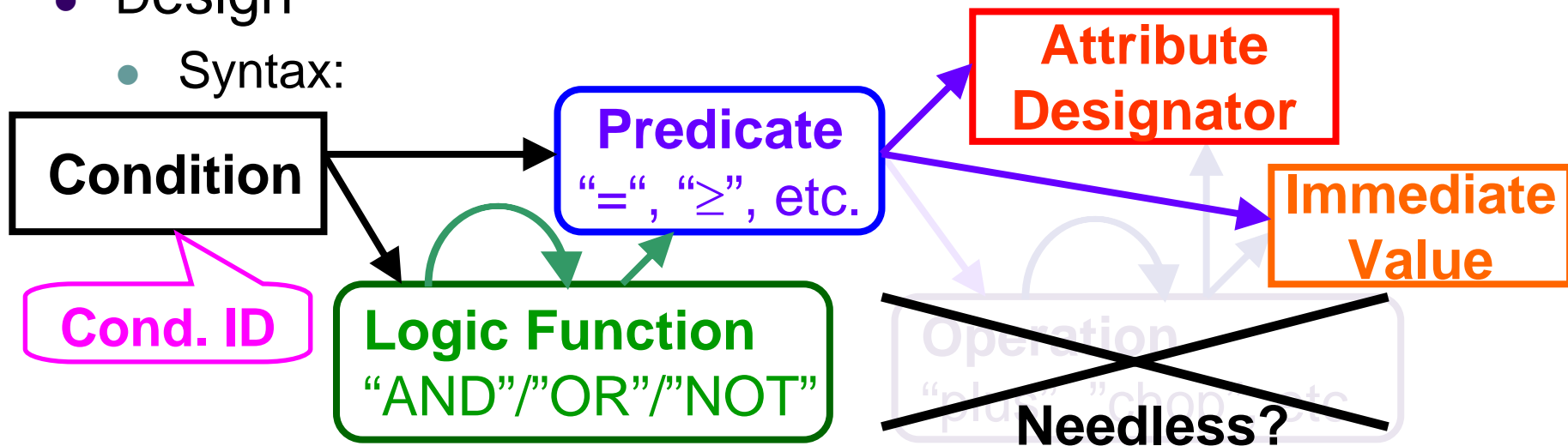


- Data types: string and long integer only

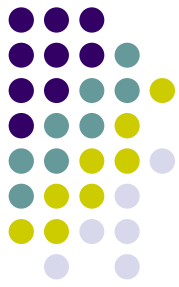
Language for Describing the Conditions



- Points
 - What to describe: AuthZ conditions about attributes
 - Compactness: XACML is too complicated
- Design
 - Syntax:



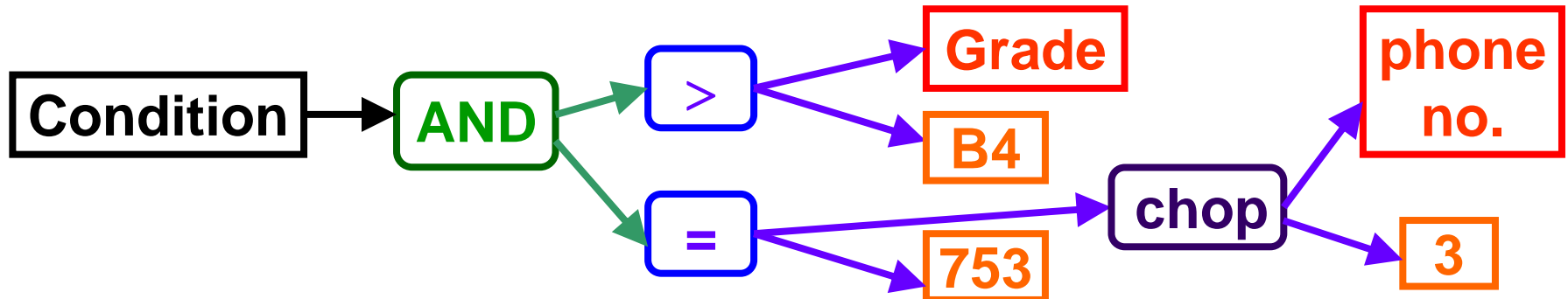
- Data types: string and long integer only



Evaluation and its Result

- Evaluation: at IdPs

Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”



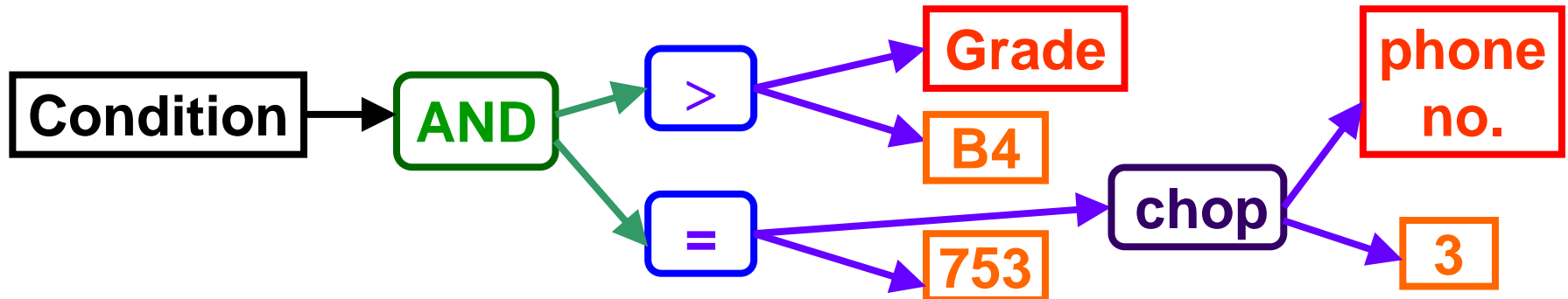


Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.

Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

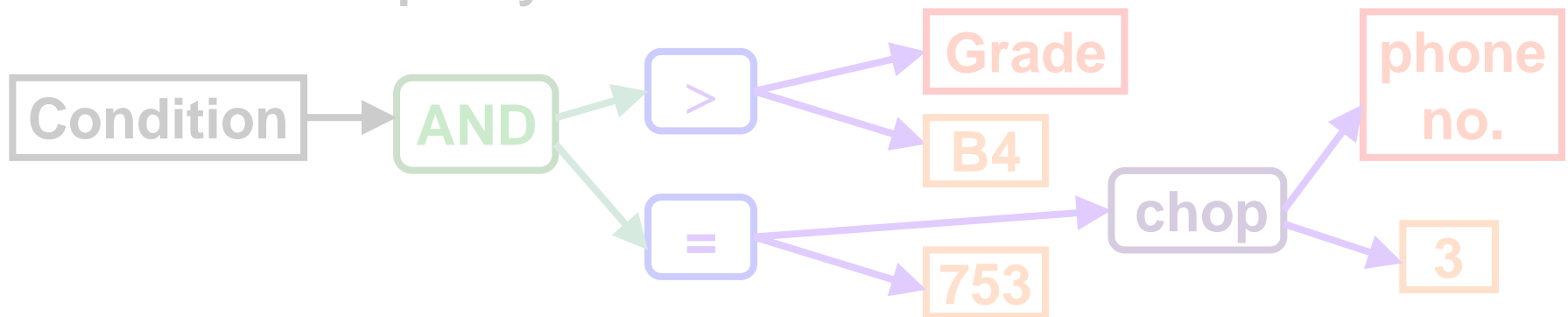




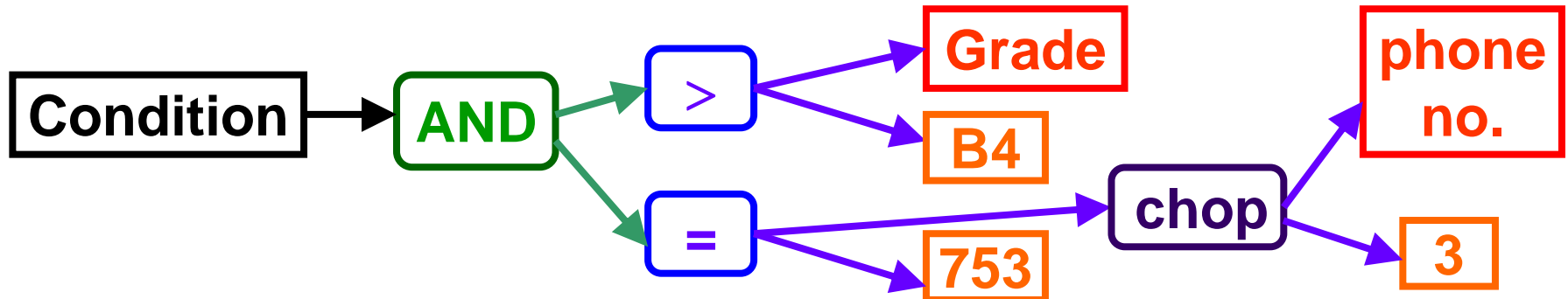
Evaluation and its Result

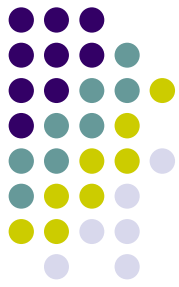
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

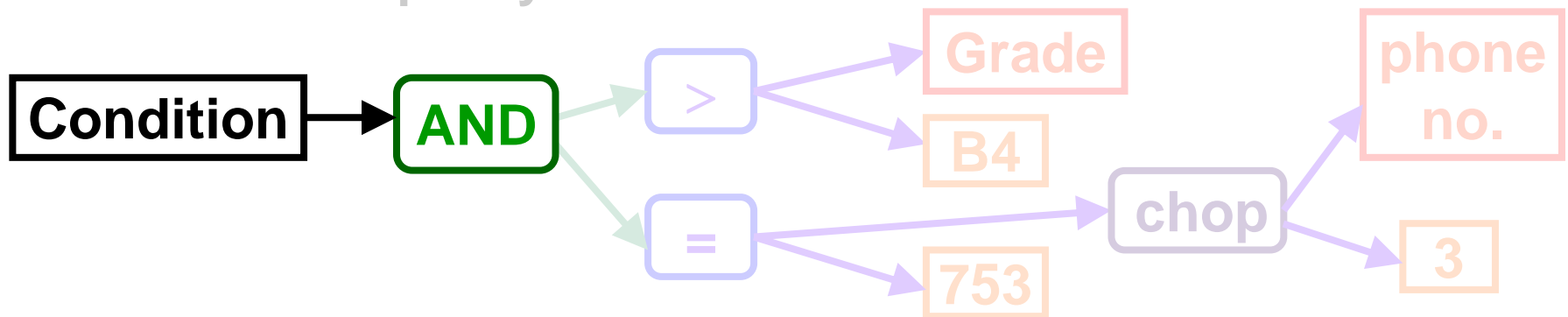




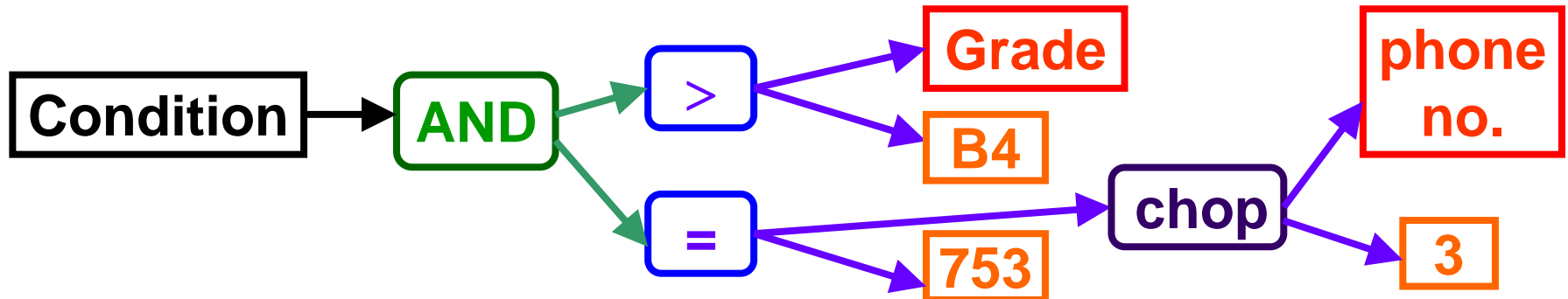
Evaluation and its Result

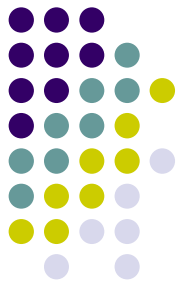
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

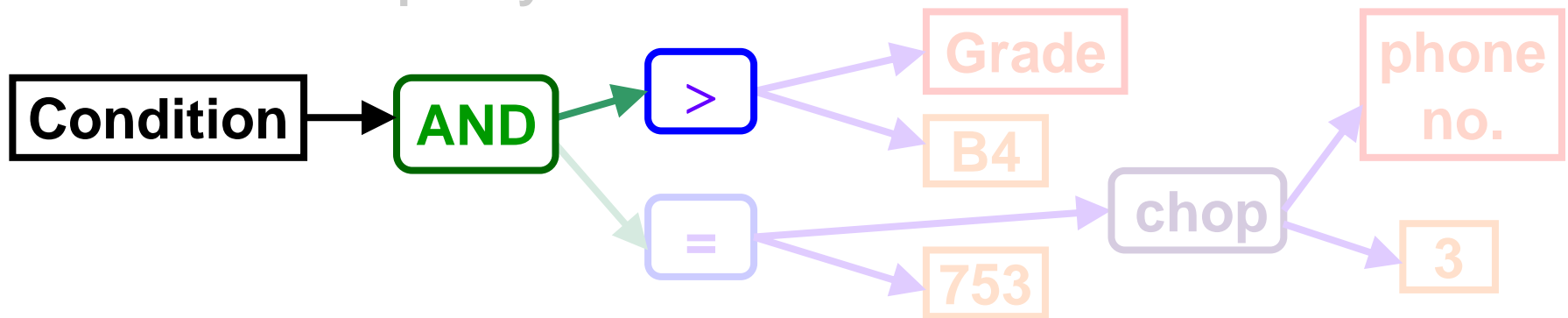




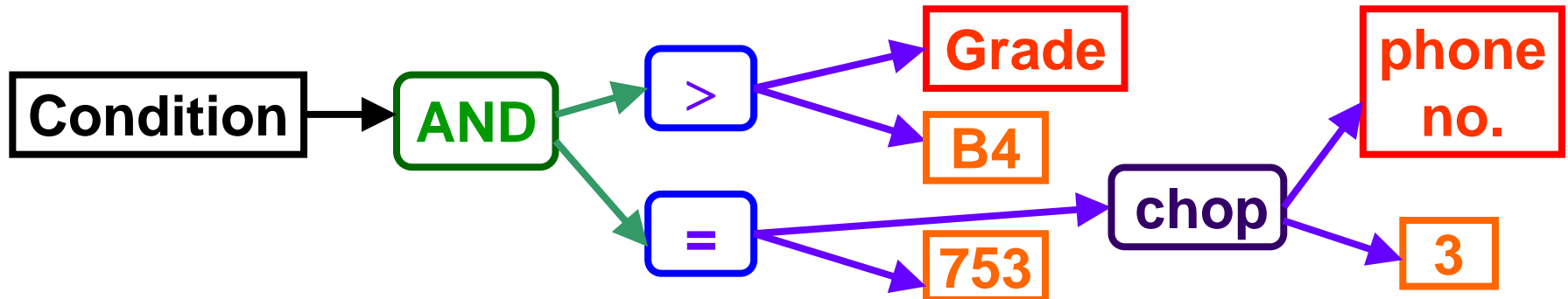
Evaluation and its Result

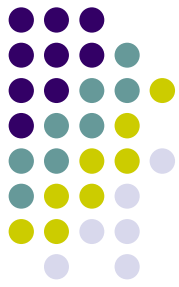
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

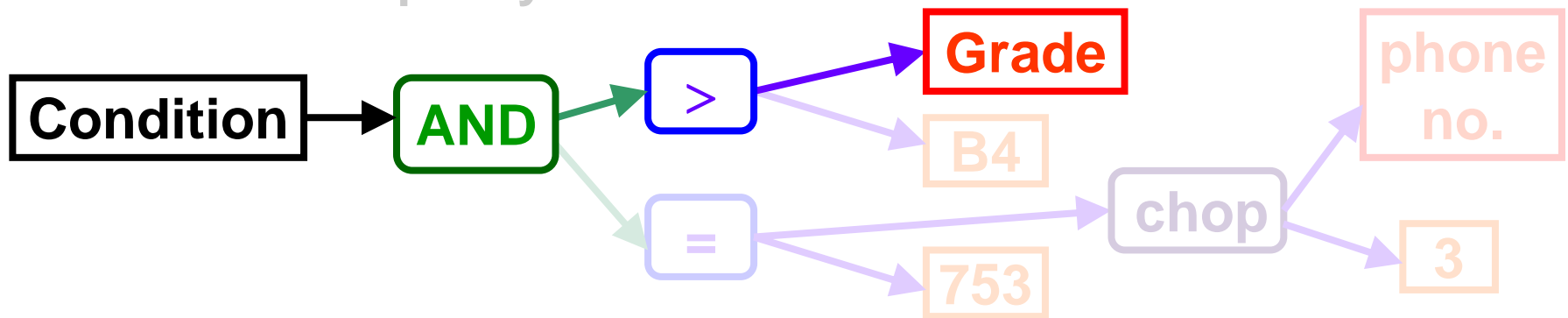




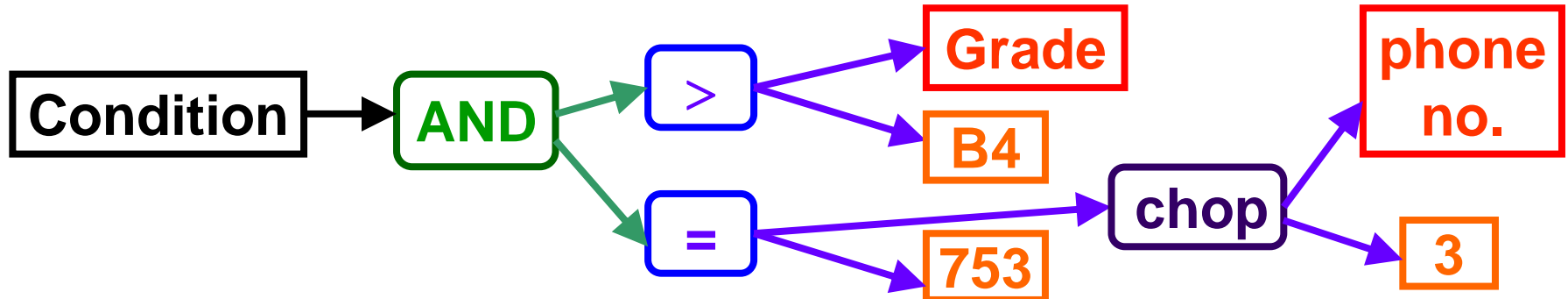
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

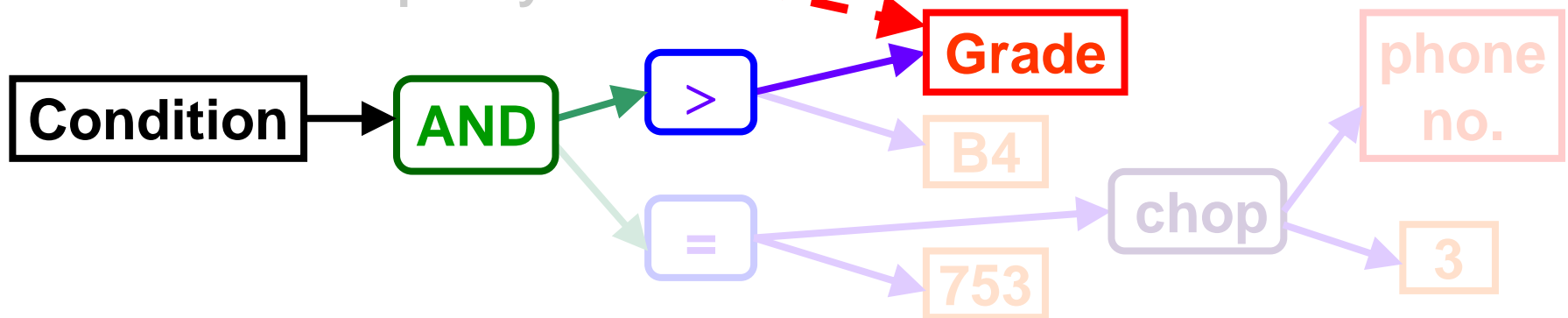




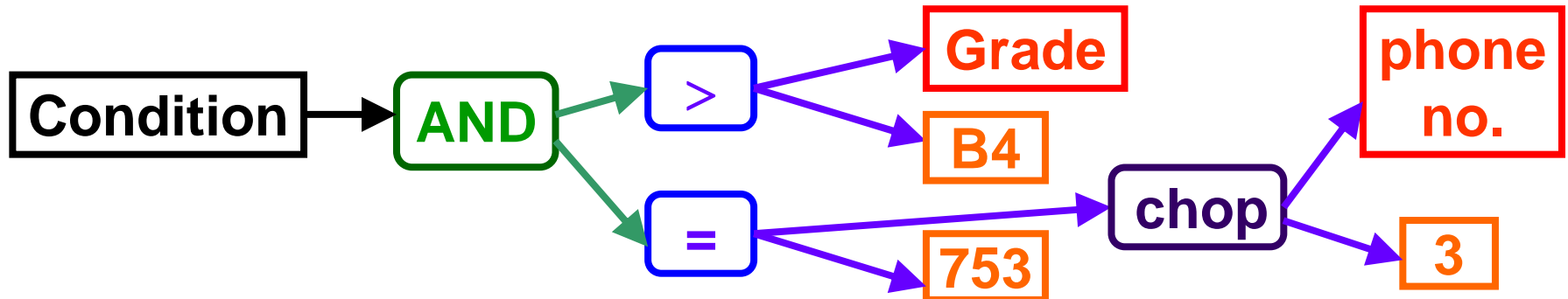
Evaluation and its Result

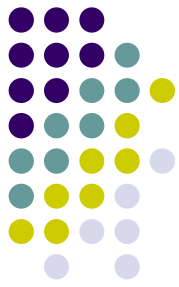
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

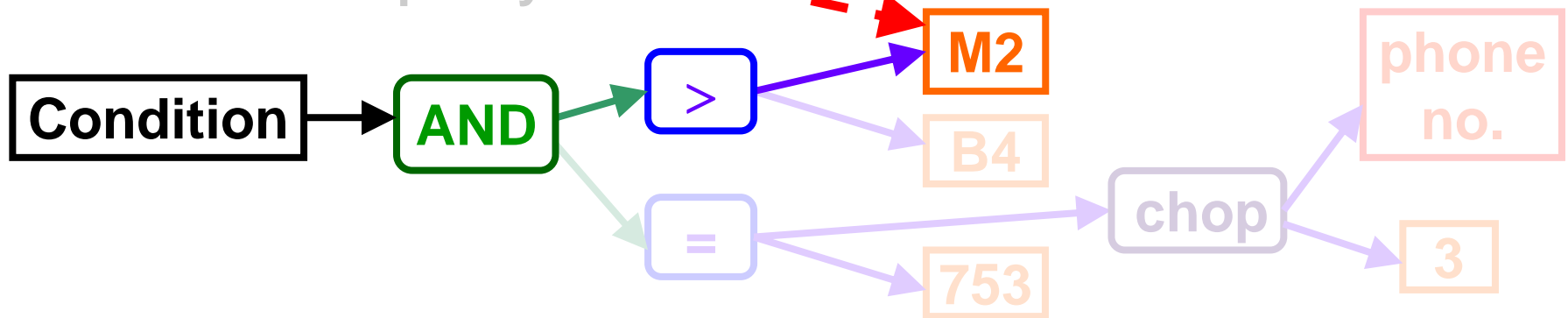




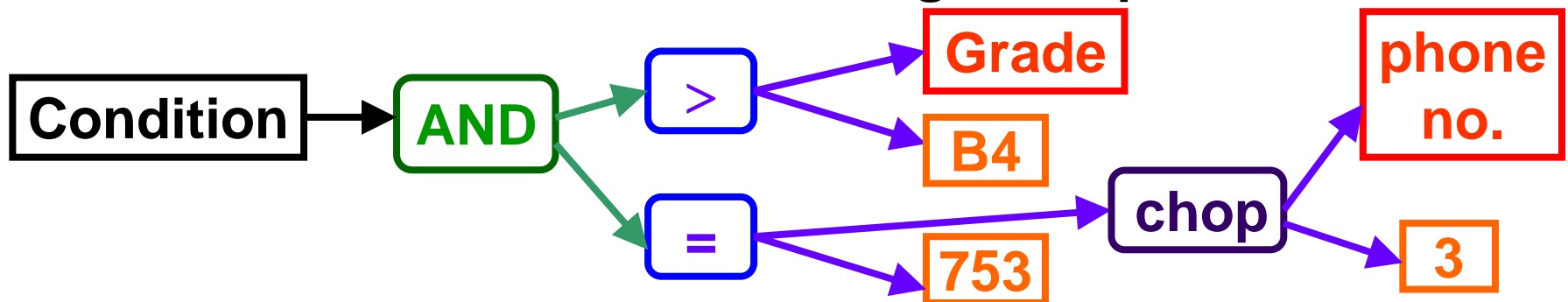
Evaluation and its Result

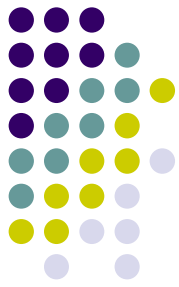
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

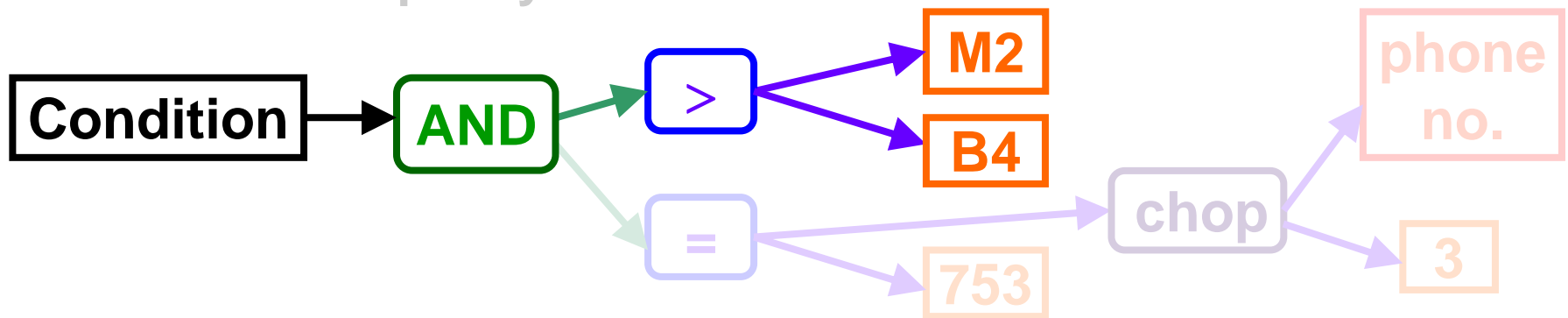




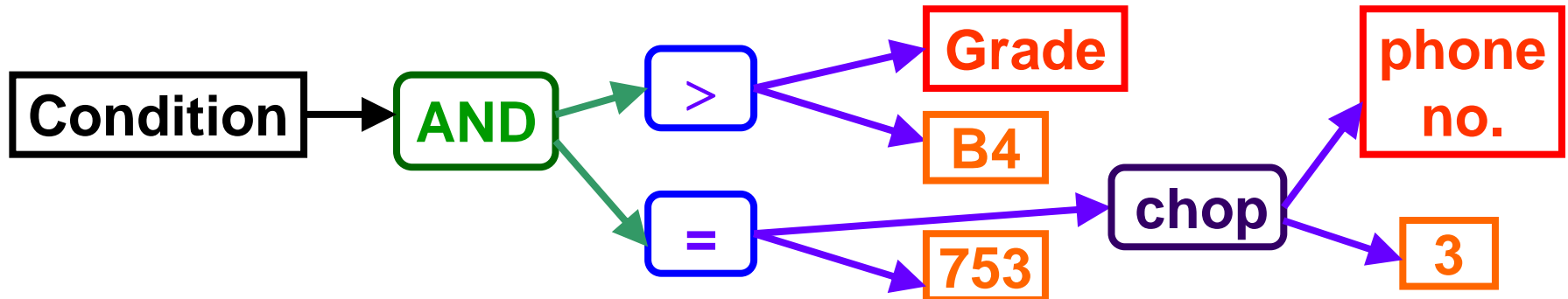
Evaluation and its Result

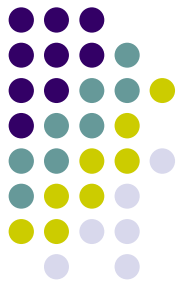
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

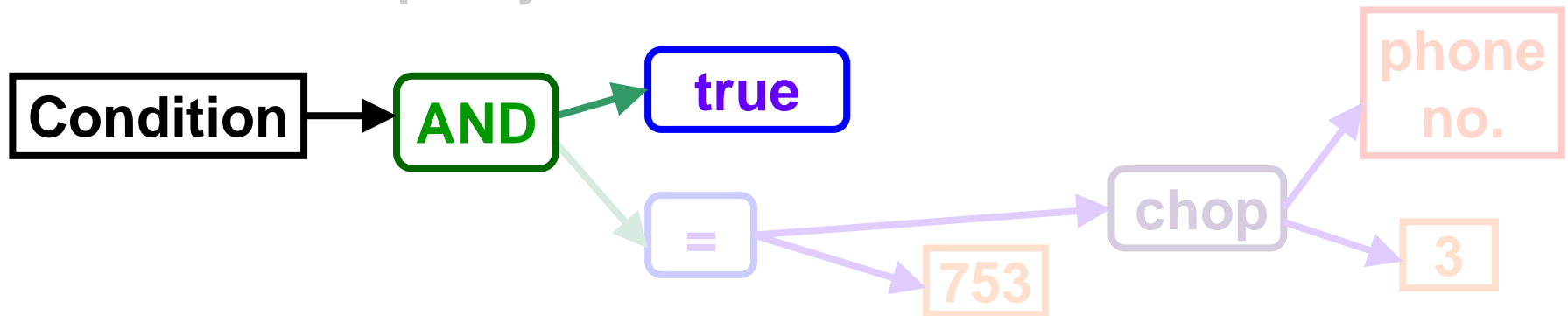




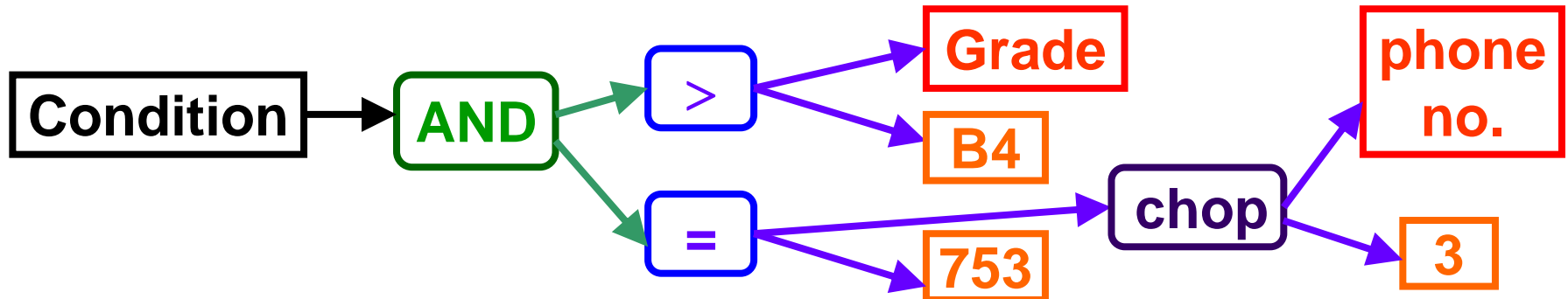
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

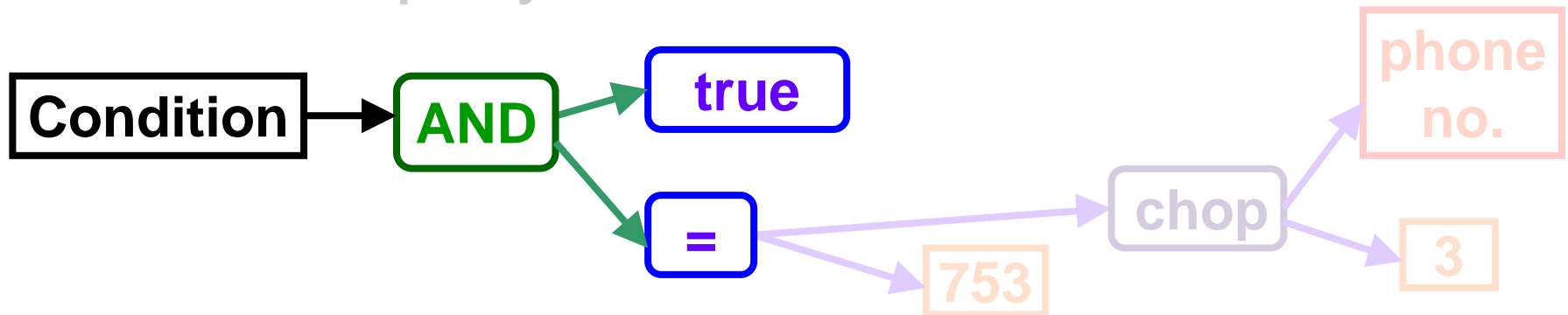




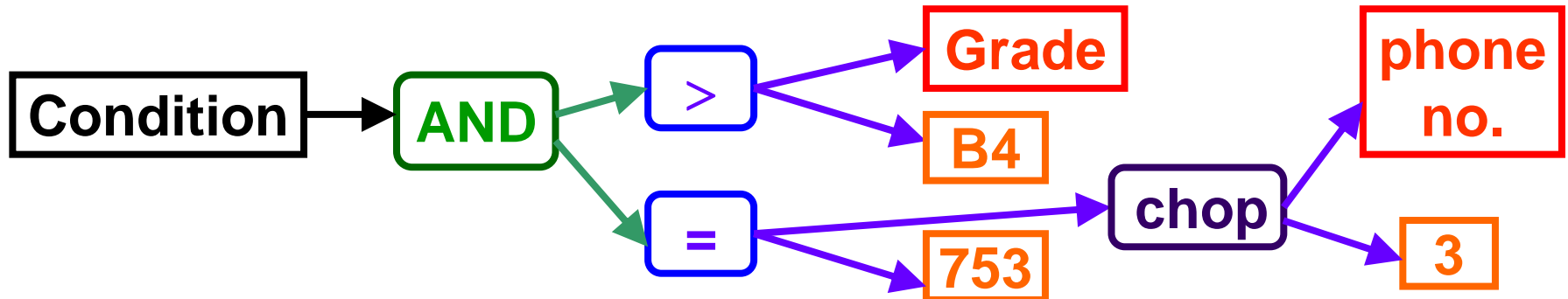
Evaluation and its Result

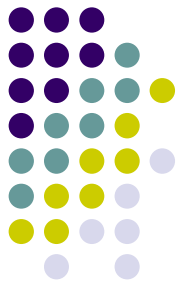
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

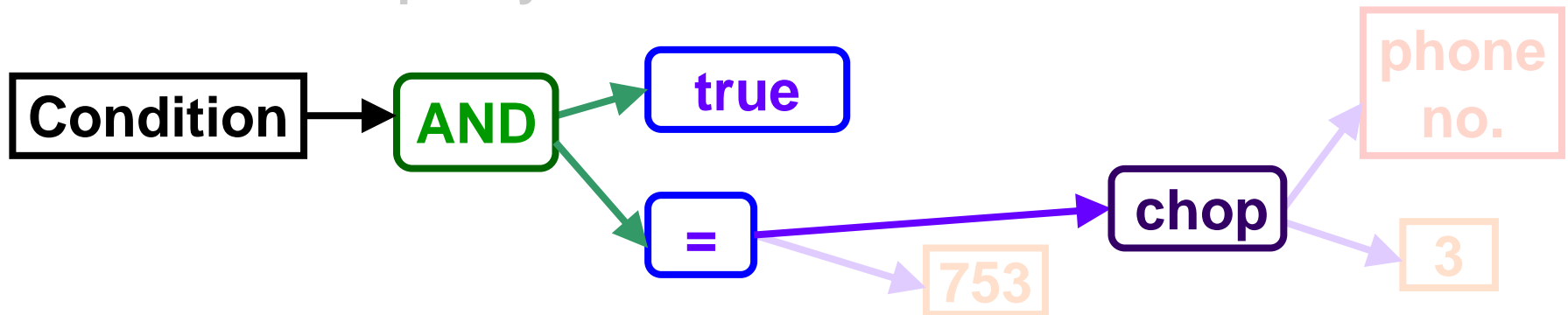




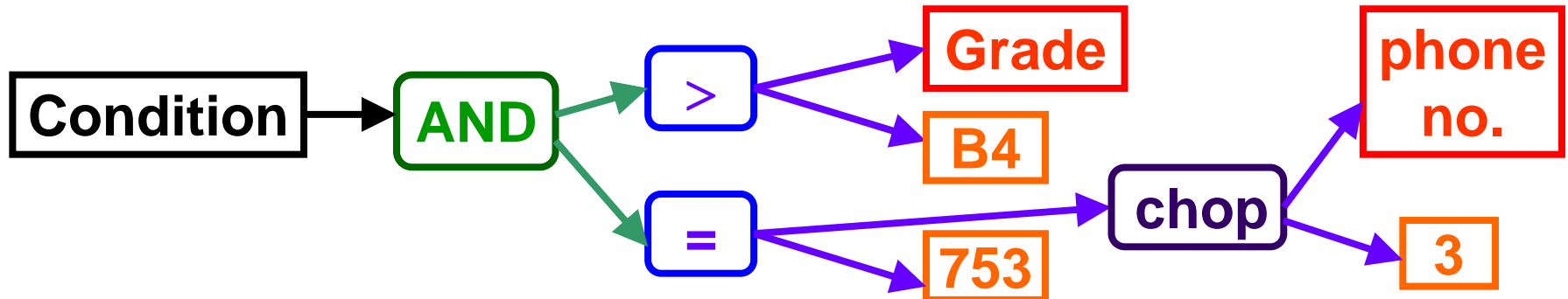
Evaluation and its Result

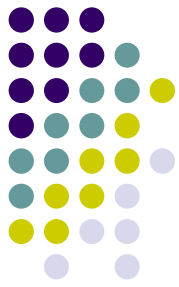
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

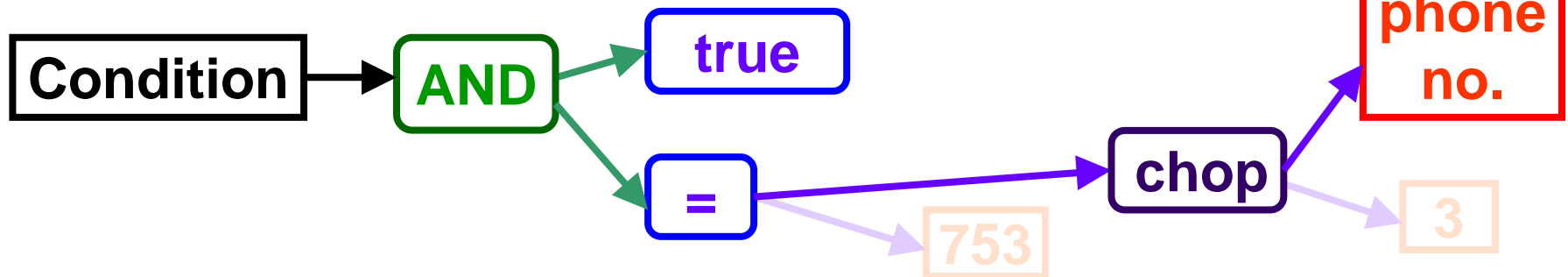




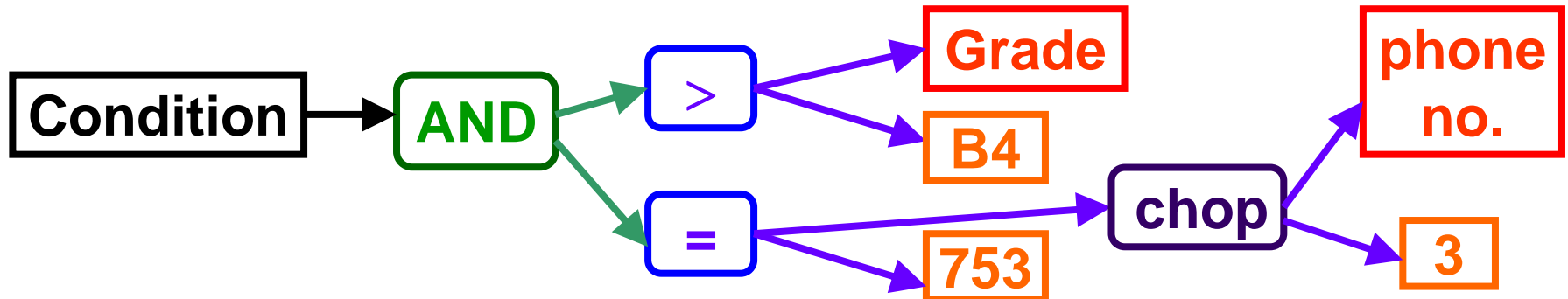
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

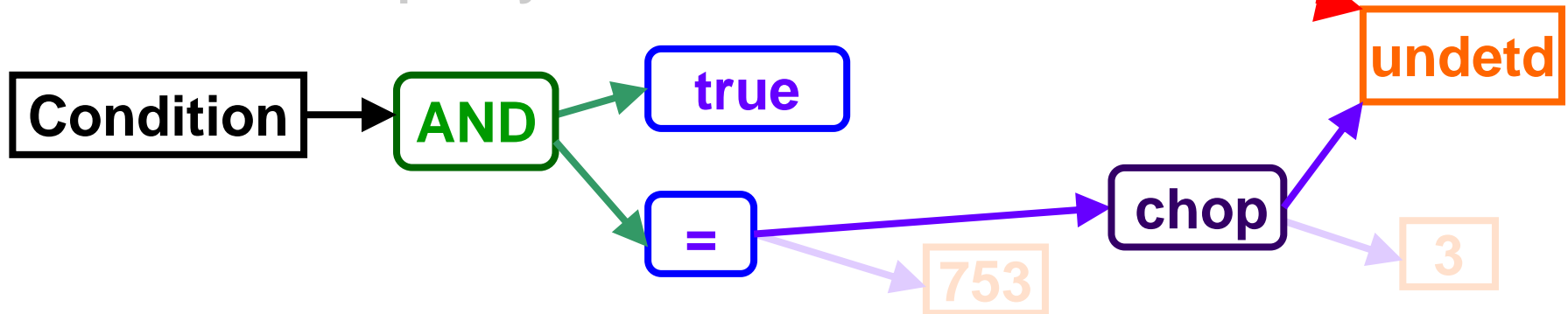




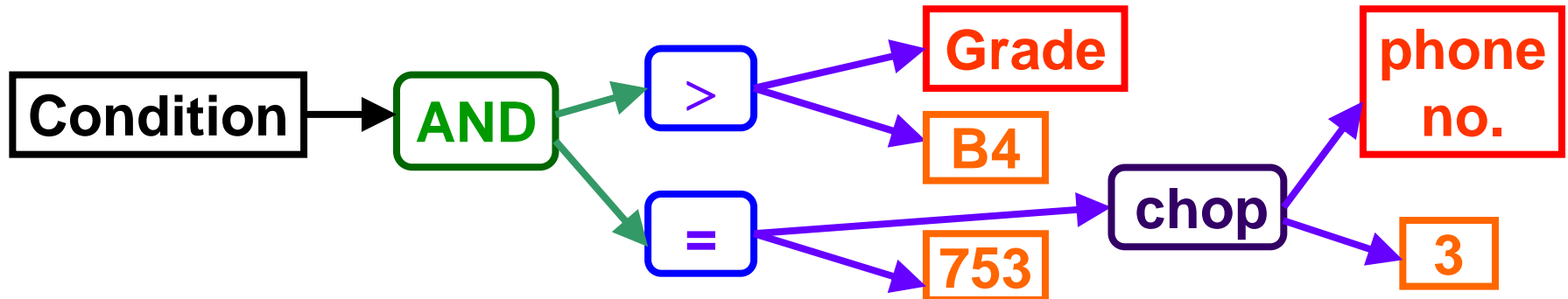
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

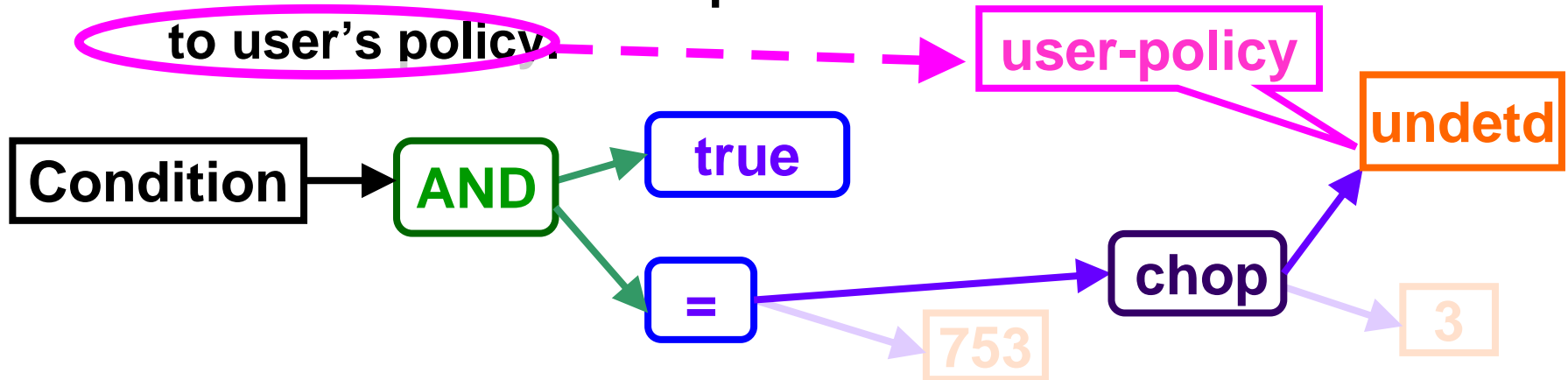




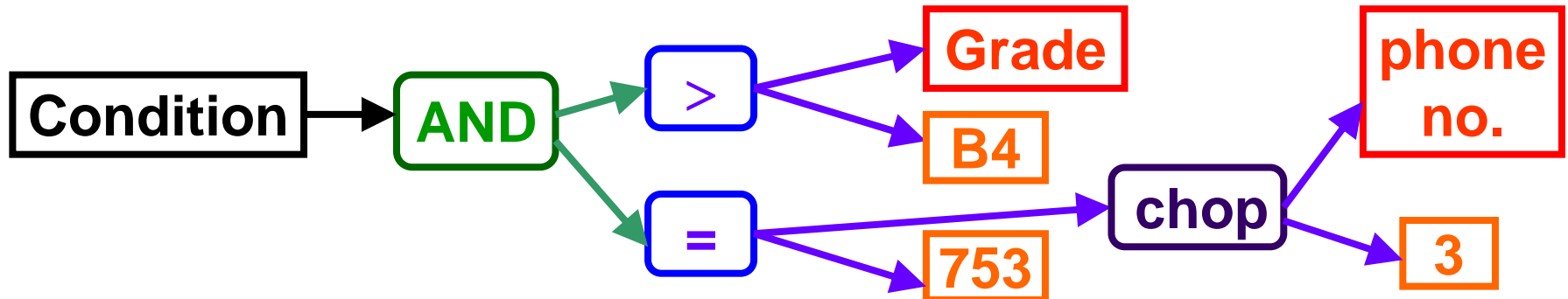
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

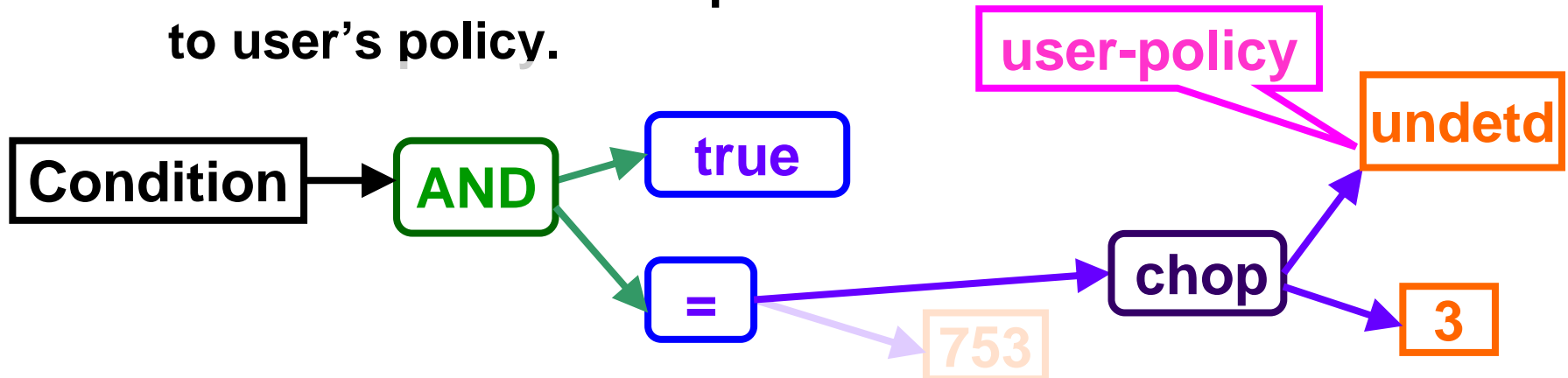




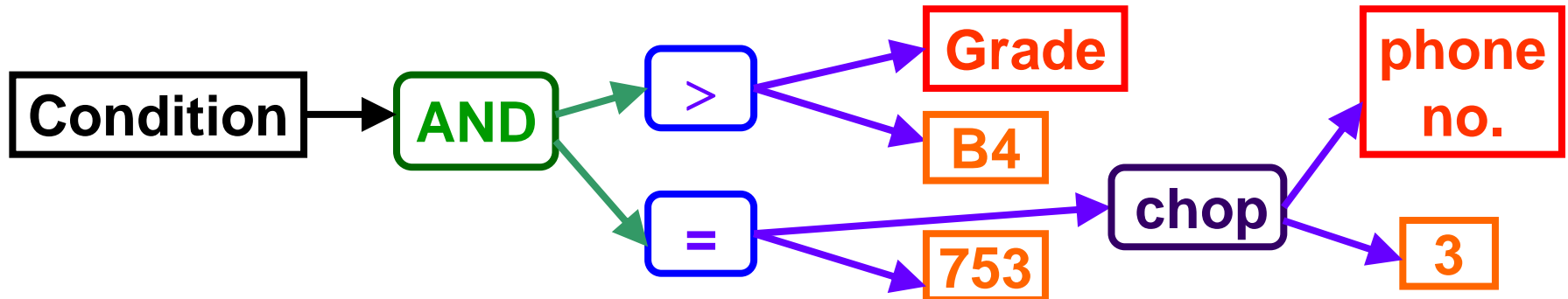
Evaluation and its Result

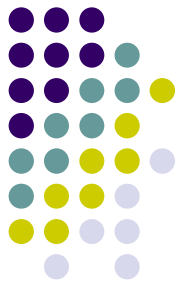
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

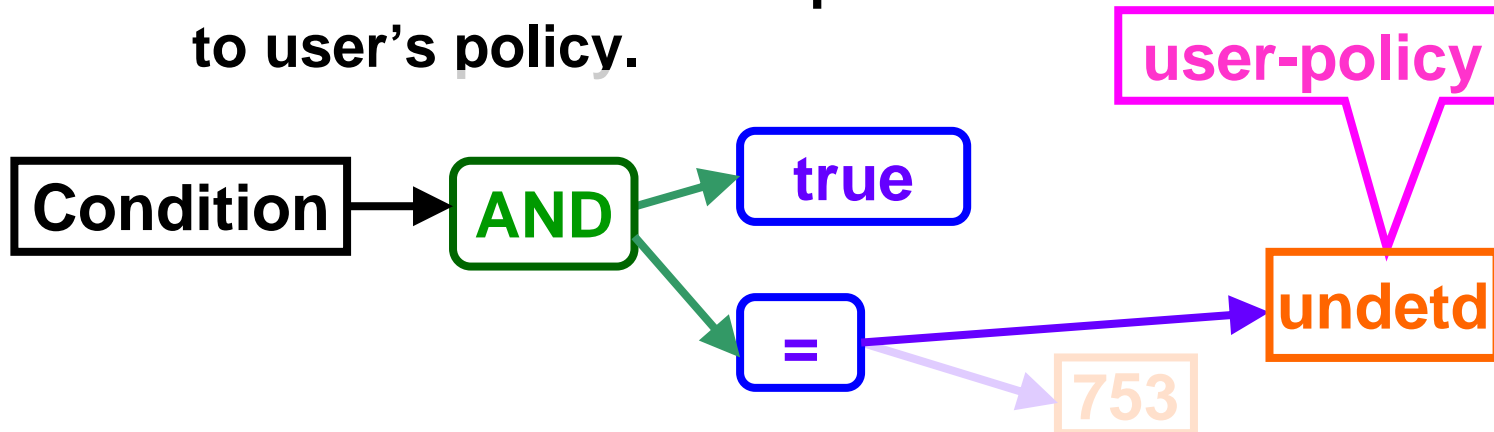




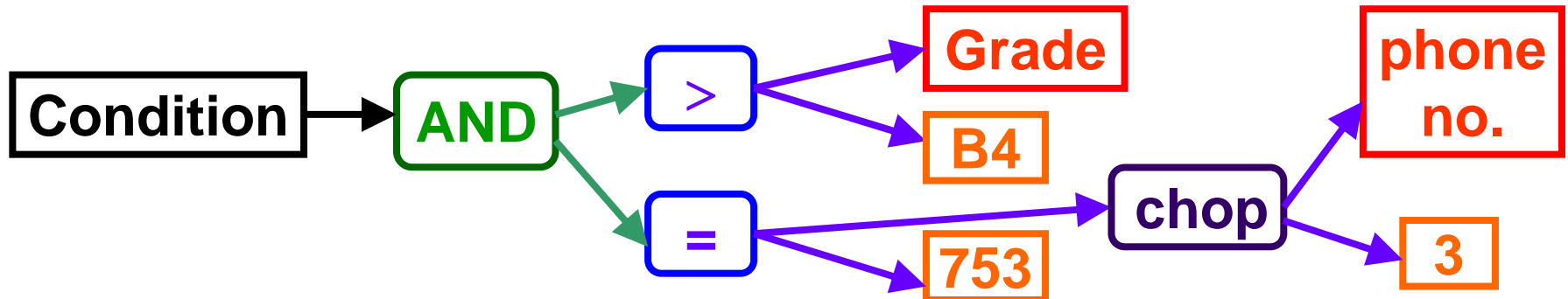
Evaluation and its Result

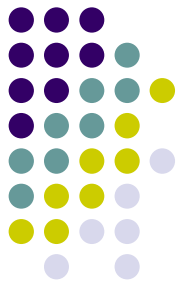
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

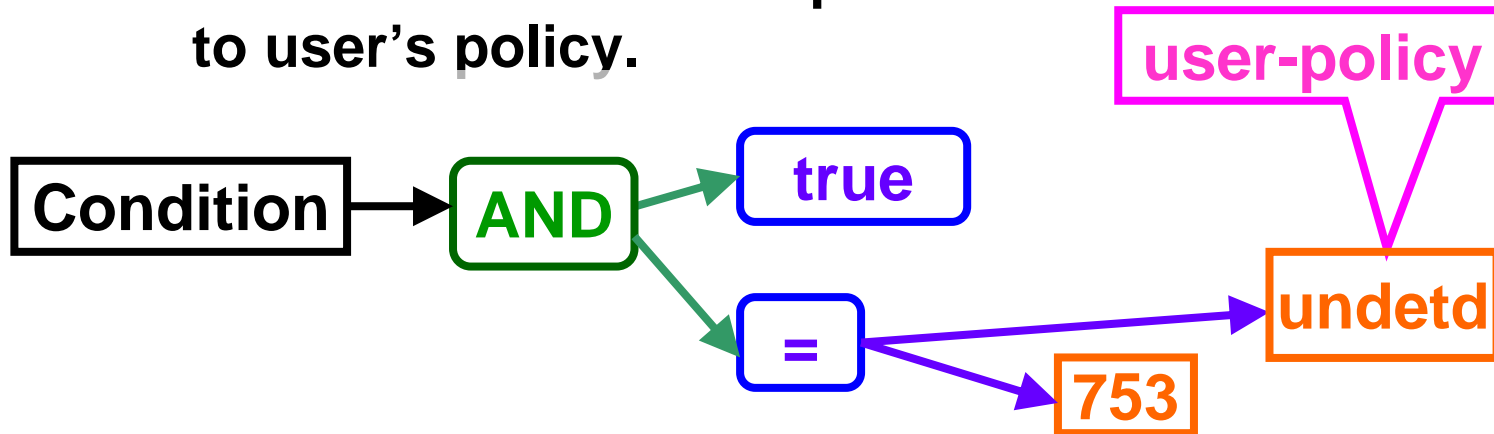




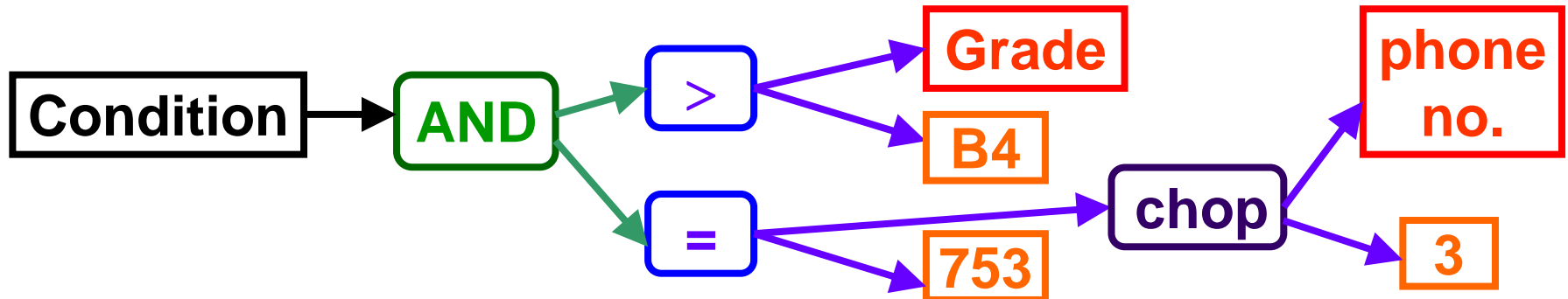
Evaluation and its Result

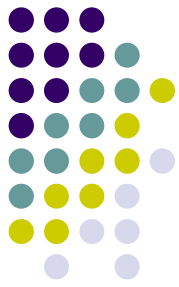
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

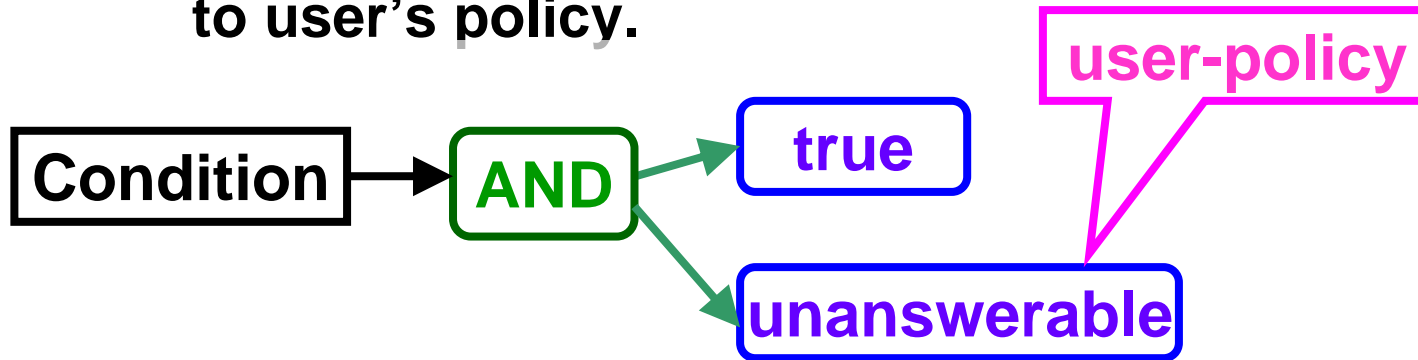




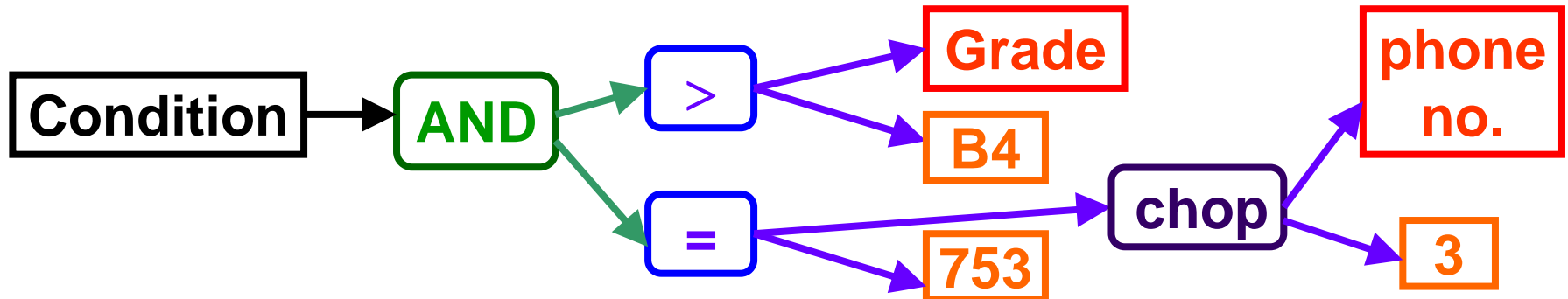
Evaluation and its Result

- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”

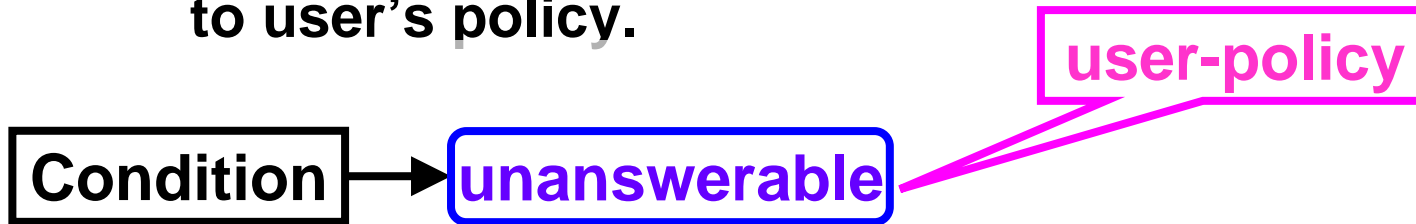




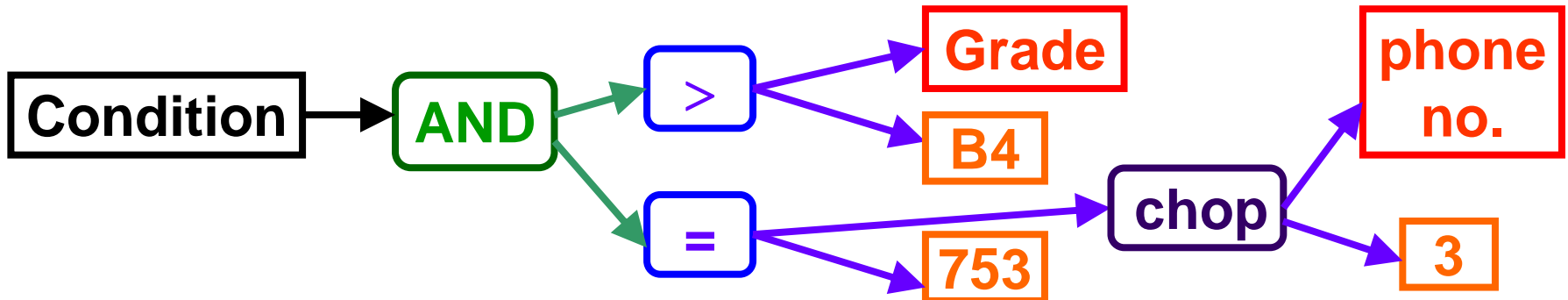
Evaluation and its Result

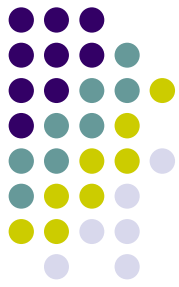
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.



Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”





Evaluation and its Result

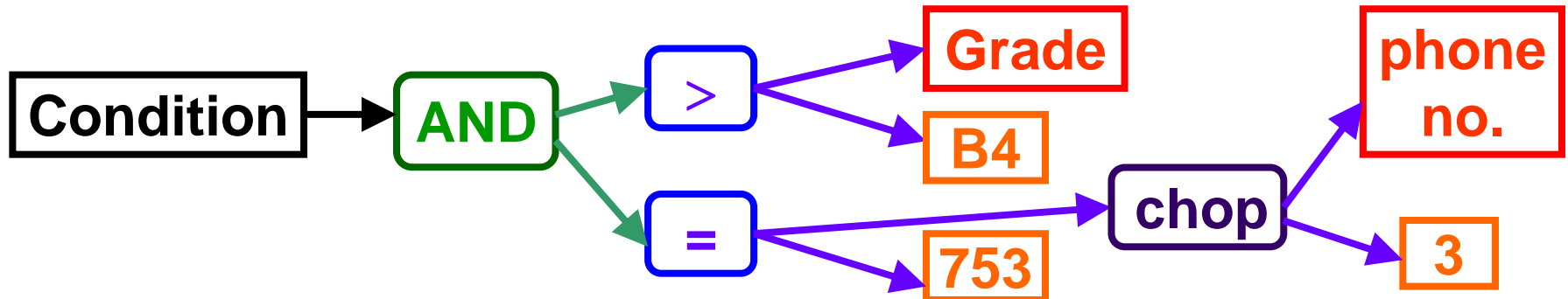
- Evaluation: at IdPs

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.

user-policy

unanswerable

Condition: “Grade” > “B4” & first 3 digits of “phone no.” = “753”





Evaluation and its Result

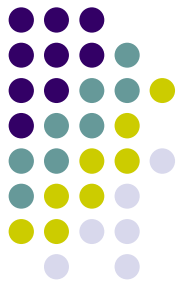
- Evaluation

- “Grade” is “M2” and “phone no.” is not released due to user’s policy.

user-policy

unanswerable

- Result



Evaluation and its Result

- Evaluation

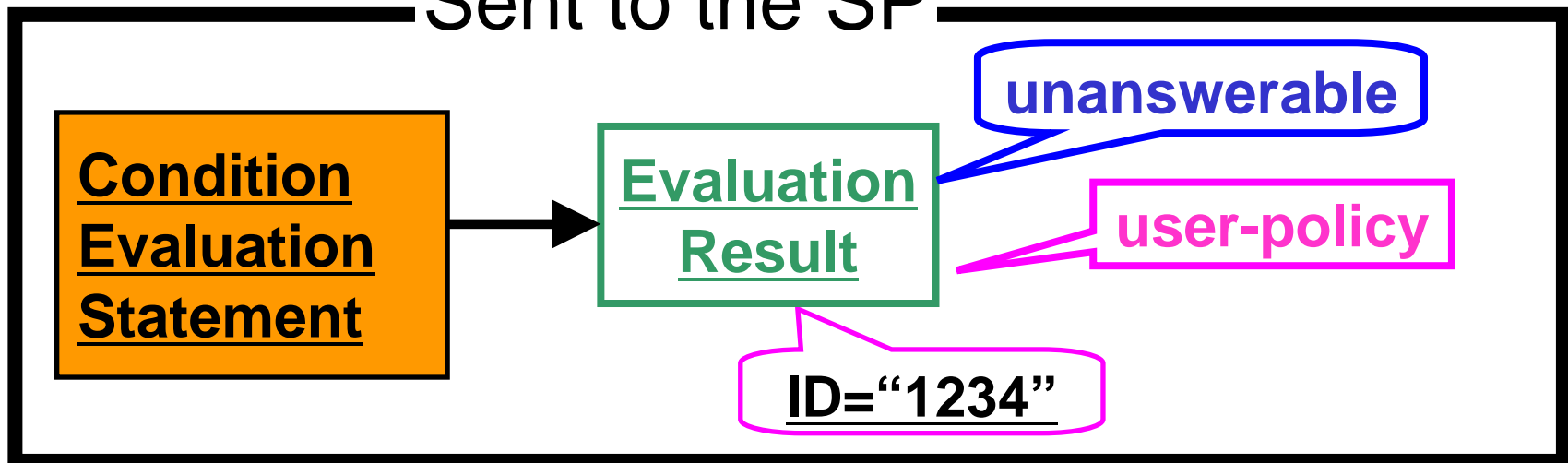
- “Grade” is “M2” and “phone no.” is not released due to user’s policy.

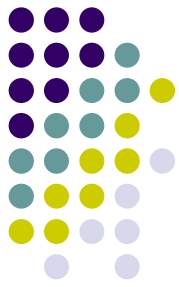
user-policy

unanswerable

- Result

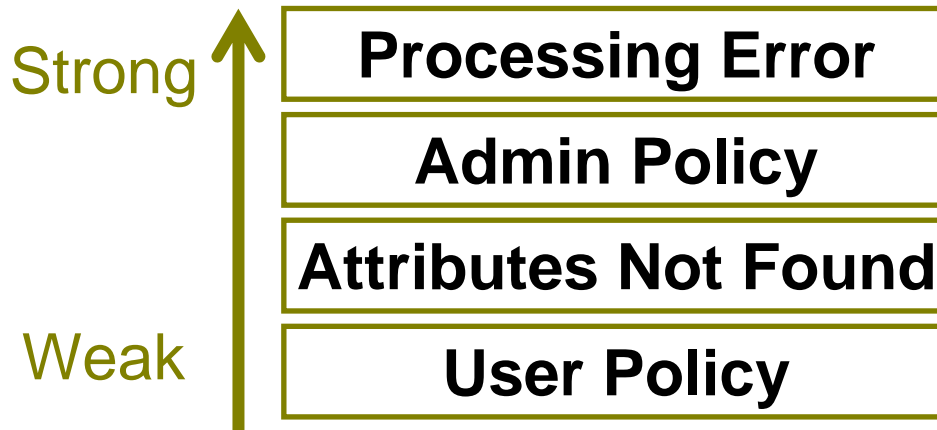
Sent to the SP



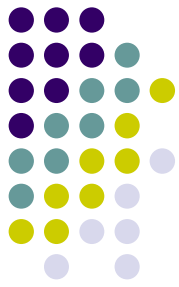


“Reasons” of “Unanswerable”

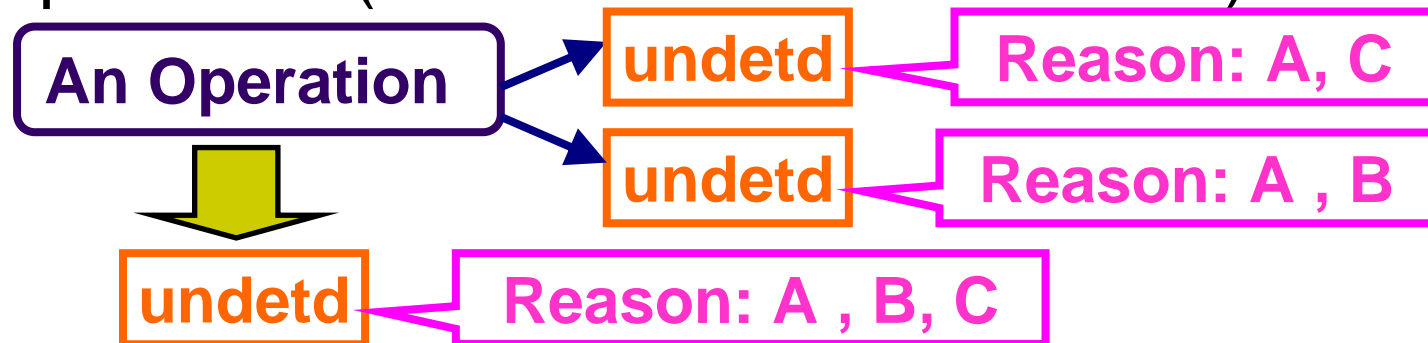
- To be ‘polite’ to users
- An IdP attaches just one “reason” to a evaluation result of “unanswerable”
- 4 Kinds of “reasons” of “unanswerable”



Calculation of “Reasons” @IdP

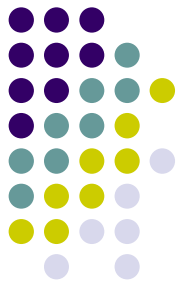


- Immediate Value: has no reasons
- Attribute Designator: calculates reasons based on ARPs actually applied for filtering if no values are obtained.
- Operation: (in case of “undetermined”)

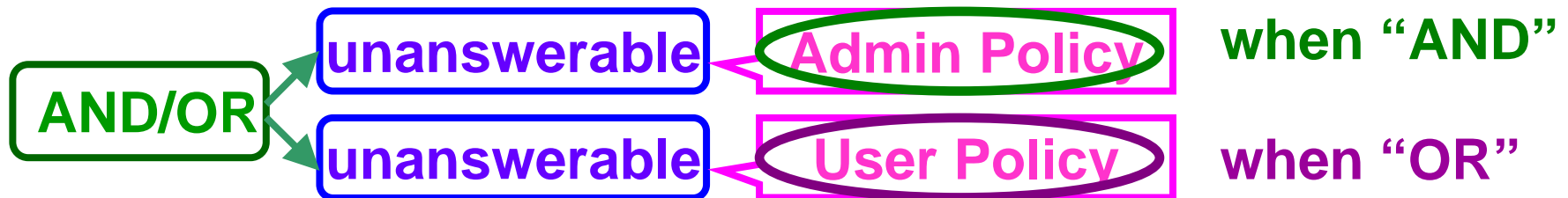


- Predicate: (in case of “unanswerable”)
 - As well as the case of “Operation”

Calculation of “Reasons” @IdP

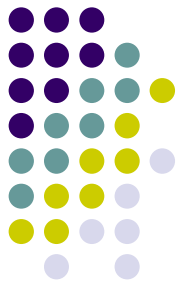


- Logic Function (in case of “unanswerable”)
 - AND: “the strongest reason” in its operands
 - OR: “the weakest reason” in its operands
 - NOT: reasons of its operand

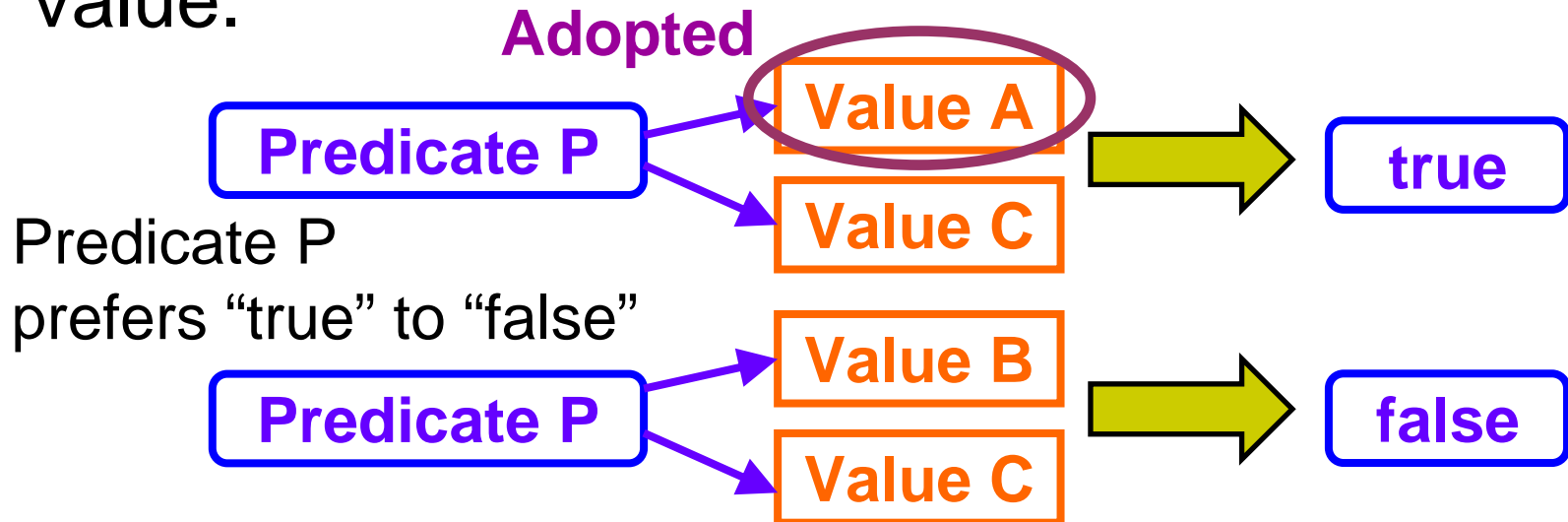


- Condition (in case of “unanswerable”): “the strongest reason” among its child node

Coping with Multivalued Attributes (to be implemented)



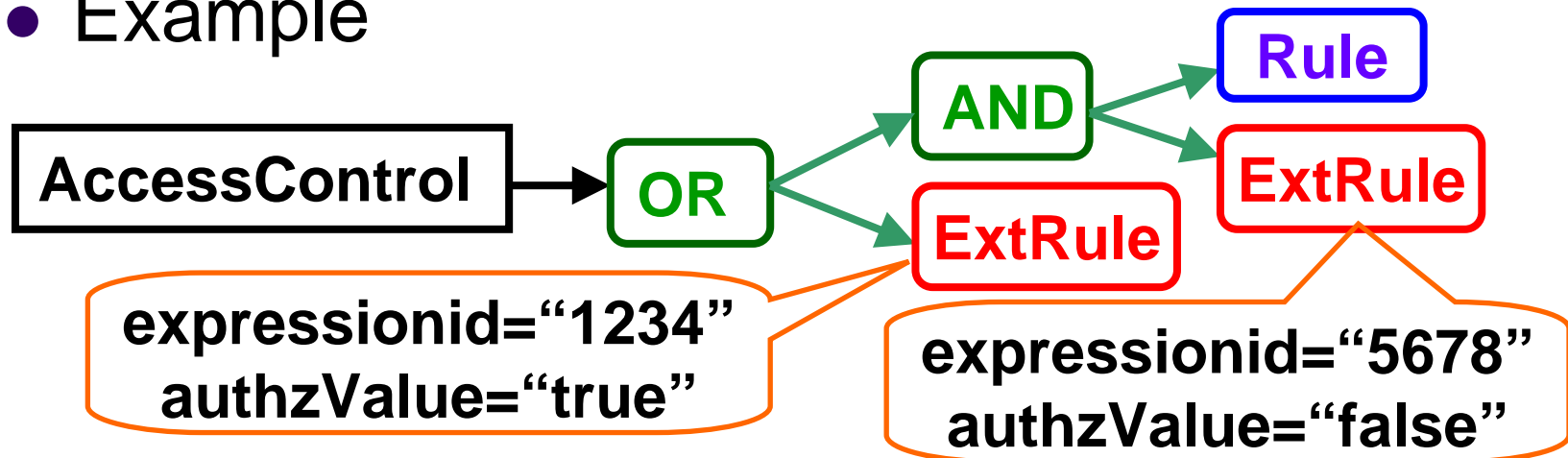
- Specify preference of each “Predicate” as to “true/false”
- Adopt the attribute value with which the predicate is evaluated as the most desirable value.



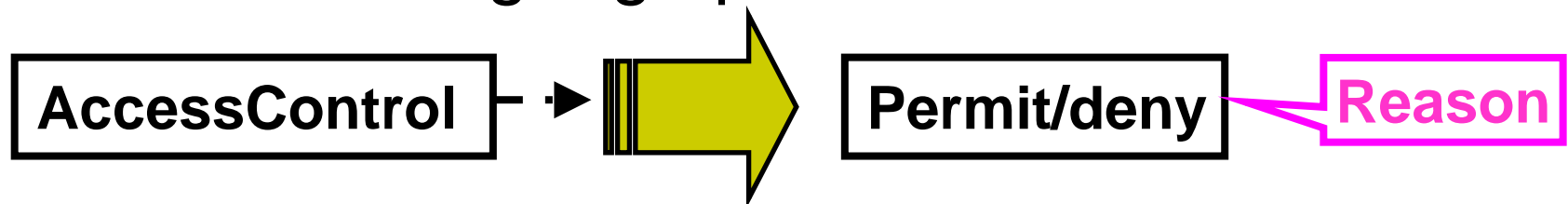


Access Control @SP

- Example

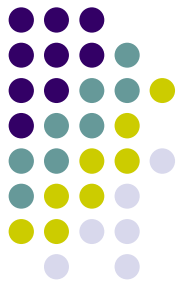


- Processing: in a similar way by which the condition language processed at IdPs



“unanswerable” with its reason → “deny” with the reason

Handling “unanswerable” (“deny”) According to “reason”



Shibboleth

Authorization Failed

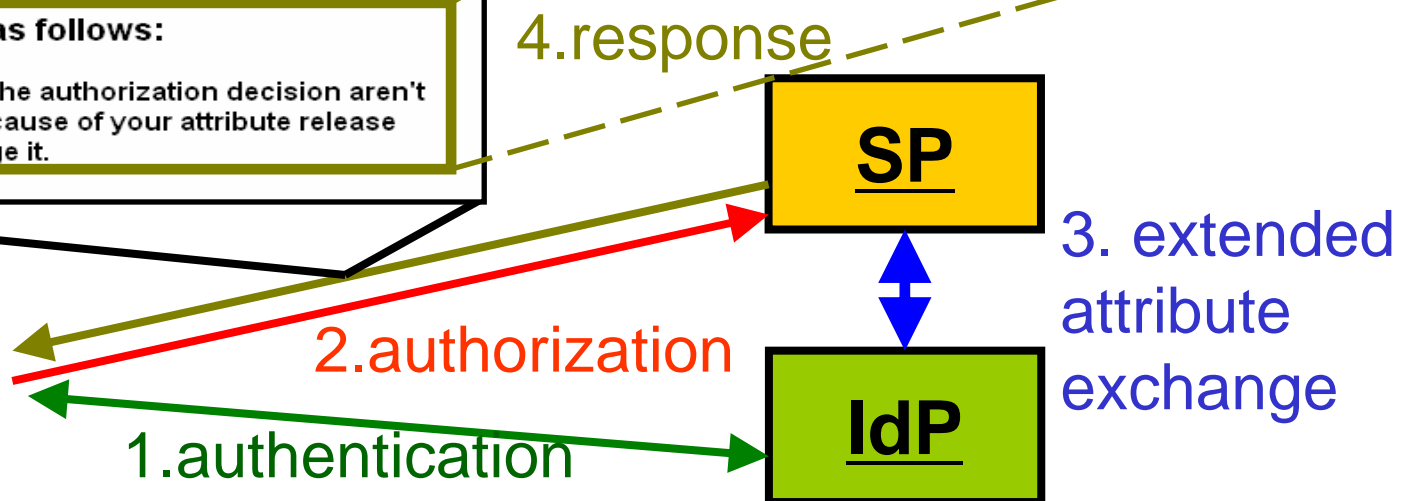
Based on the information about you, you are not authorized to access the resource at "https://s...". Please contact the administrator of this service or application if you believe this to be an error.

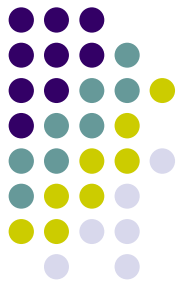
The reason of denial is as follows:

Some attributes required for the authorization decision aren't released to us, and this is because of your attribute release policy. So, you need to change it.

The reason of denial is as follows:

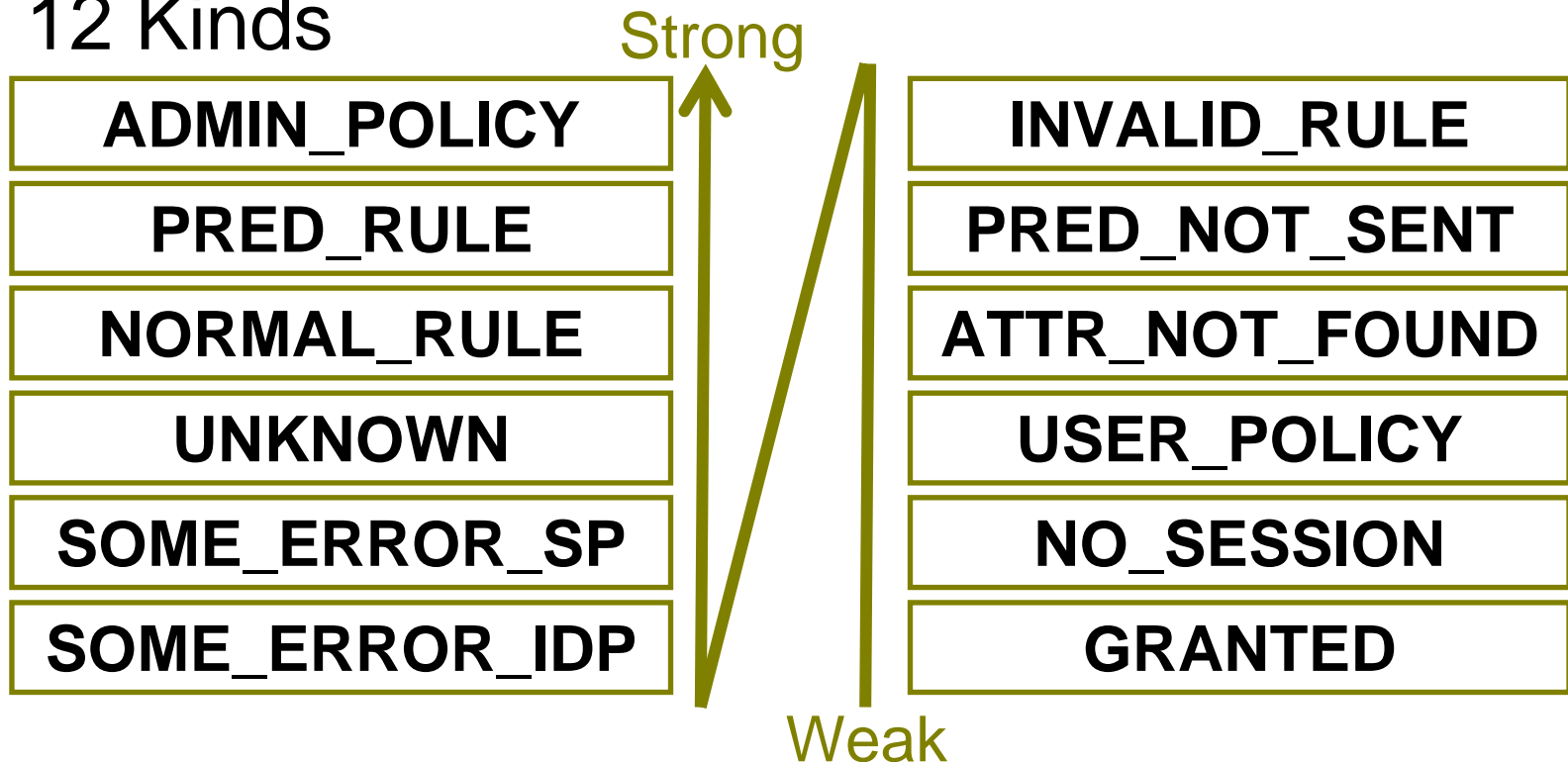
Some attributes required for the authorization decision aren't released to us, and this is because of your attribute release policy. So, you need to change it.



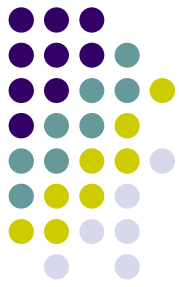


“Reasons” of “Deny” @SP

- 12 Kinds

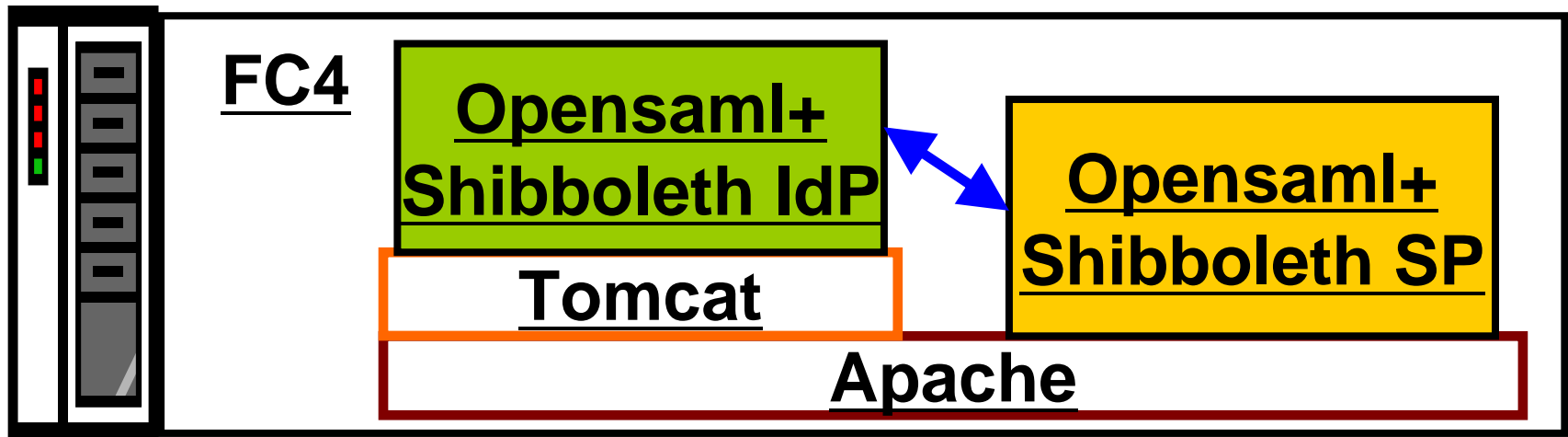


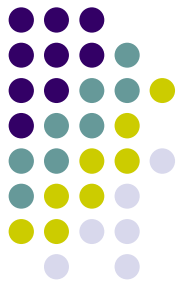
- IdP > SP > user (-side reasons)
- Definite “deny” > error > any shortages



Implementation

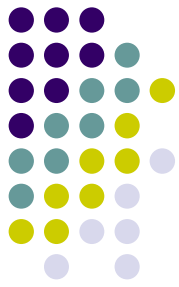
- Platform: Apache 2.0.58/Tomcat 5.5.20/
Java 2 SDK 1.5.0 on Fedora Core 4
- IdP: Opensaml 1.1b, Shibboleth 1.3c
- SP: Opensaml 1.1a, Shibboleth 1.3f (C++,
source code build)





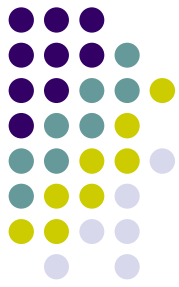
Demonstration

- A user m1 tries to access a DEMO book rental service at an SP
 - AuthZ condition: user's grade \geq B4
- 1st trial: denied due to one of the user's policies
 - ↓ change the policy
- 2nd trial: successfully authorized



Agenda

- Outline of our work: extending attribute exchange to enhance privacy in Shibboleth
- Design and implementation
- **Summary and future works** ←



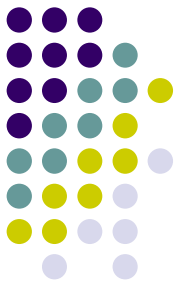
Summary

- An Extended protocol of attribute exchange in shibboleth to enhance user's privacy
 - An SP to an IdP: conditions for authorization
 - The IdP to the SP: their evaluation result with reasons why the IdP evaluated so
- How to control access requests
 - Utilizing reasons of “unanswerable” and “deny”
- Implementation and Demo.



Future Works

- Policy filtering
- Application to Shibboleth 2.0
- Verification of practicality
- Blend of the existing strategy of attribute release at IdPs and that of our extension



Thank you for your attention !
Questions ?