TÖL303G

Gagnasafnsfræði

Snorri Agnarsson

SQL Aðgangsheimildir

Heimildir, réttindi, aðgangsréttindi, notkunarréttindi
(privileges, permissions, access rights)

GRANT og REVOKE skipanir (GRANT and REVOKE commands)

Heimildanet (Grant Diagrams)

Heimild (Authorization)

- Skráakerfi geymir upplýsingar um notkunarréttindi fyrir þá hluti (skrár) sem það sér um – File systems maintain access right information for those objects (files) that it manages
  - Dæmigerð réttindi eru fyrir lestur, skrift, keyrslu – Typical rights are for reading, writing, executing
- Skráakerfi hefur einnig upplýsingar um notendur og flokka notenda sem geta fengið viðeigandi réttindi – File systems also has information about users and groups of users that can have rights in question
  - Dæmigert er að einhver notandi sé eigandi (owner) og hafi tiltekin réttindi, sumir aðrir notendur séu í skilgreindum hópi (group) og hafi tiltekin réttindi, og að allir aðrir notendur (other) hafi önnur tiltekin réttindi – Typically some user is the owner and has appropriate rights, some other users are members of a group that has appropriate rights, and all other users have some other defined rights
- Sjá t.d./See, e.g.: https://en.wikipedia.org/wiki/File_system_permissions

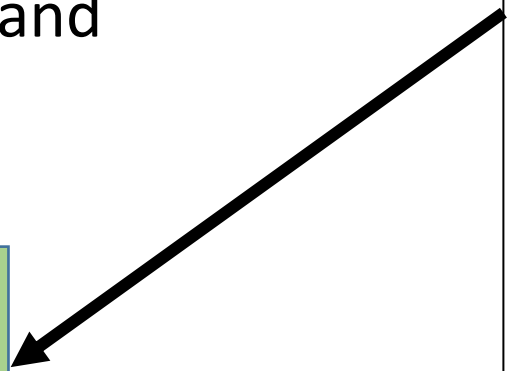
SQL heimildir – SQL Authorizations

- Í SQL eru skilgreind víðtækari gerðir heimilda á hluti (vensl, tafla) en í dæmigerðum skráakerfum – In SQL we have more extensive types of access rights than in typical file systems
- Margar mismunandi gerðir heimilda eru skilgreindar – Many different sorts of access right are defined
  - Dæmi hér/Example here: https://www.postgresql.org/docs/current/sql-grant.html Sumar heimildir má takmarka við staka dálka í töflum – Some access rights can be limited to discrete columns in tables
- Nokkrar mikilvægar gerðir heimilda eru / Some important types of access rights:
  1. SELECT – réttur til að gera fyrirspurn á töflu – the right to query a table
  2. INSERT – réttur til að bæta við n-dum – the right to add tuples
     - Má takmarka við dálk – can be limited to discrete columns
  3. DELETE – réttur til að eyða n-dum – the right to delete tuples/rows
  4. UPDATE – réttur til að uppfæra n-dir – the right to update tuples
     - Má takmarka við dálk – can be limited to discrete columns

Dæmi – Example

- Fyrir eftirfarandi SQL setningu
  For the following SQL command

```
INSERT INTO Beers(name)
   SELECT beer FROM Sells
   WHERE NOT EXISTS
     (SELECT * FROM Beers
      WHERE name=beer);
```



Bjórar sem ekki koma fyrir í Beers töflunni. Við bætum þeim í Beers töfluna með nafni en með NULL gildi fyrir aðra dálka (eða sjálfgefið).

Beers that do not occur in the Beers table. We add them to the Beers table with name but with NULL value for other columns (or default)

- þarf réttindi SELECT á töflurnar Sells og Beers auk INSERT réttinda á Beer eða Beer.name
  We need SELECT rights for the tables Sells and Beers and INSERT rights for Beer or Beer.name

Hlutir í gagnagrunnum – Objects in databases

- Meðal hluta í gagnagrunnum sem geta haft réttindi tengd eru töflur og sýnir – Among the objects in databases that can have access rights are tables and views
- Einnig eru til réttindi til að smíða hluti af tiltekinni gerð, svo sem gikki – Also there are access rights to construct objects of a given type such as triggers
- Sýnir eru mikilvæg tól til að stýra aðgangi – Views are important to control access

Dæmi um notkun sýnar – Example of using a view

- Við viljum e.t.v. ekki gefa SELECT heimild á Emps(name,addr,sal)
  We do not, perhaps, want to allow SELECT on Emps(name,addr,sal)
- En líklegra er að við viljum gefa SELECT heimild á – More likely we want to allow SELECT on
  CREATE VIEW SafeEmps AS SELECT name,addr FROM Emps;
- Fyrirspurnir á SafeEmps þarfnast ekki SELECT heimildar á Emps, aðeins heimildar á SafeEmps – Queries on SafeEmps do not need a SELECT right for Emps, only for SafeEmps

Notendanöfn - Authorization ID‘s

- Notendur eru auðkenndir með notendanöfnum, oft sama og notandanafnið fyrir tölvureikning notandans – Users are identified by authorization ID‘s, often the same userid as the users ID on the computer
- Einnig er til notandanafnið PUBLIC – We also have the authorization ID called PUBLIC
- Heimild sem gefin er til PUBLIC er heimild sem allir notendur fá – An access right given to PUBLIC is a right that all users get

Veiting heimilda – Granting Access Rights

- Þú hefur allar mögulegar heimildir fyrir þá hluti sem þú smíðar, svo sem töflur og sýnir – You have all possible rights for those objects that you create, such as tables and views
- Þú getur einnig veitt öðrum notendum (notendanöfnum) heimildir – You can also grant other users (authorization ID‘s) rights
- Þú getur einnig veitt heimildir með WITH GRANT OPTION, sem gerir þeim sem fær heimildirnar kleift að veita öðrum heimildirnar – You can also grant rights WITH GRANT OPTION, which makes it possible for those receiving the rights to grant those rights to others

GRANT skipunin – The GRANT command

- Til að veita heimildir er notuð skipun – To grant rights a command is used

  GRANT <listi heimilda/list of right>
  ON <tafla eða annar hlutur/table or other object>
  TO <listi notandanafna/list of authorization ids>;

- Ef þú vilt að móttakendur heimildanna geti gefið öðrum heimildirnar bætir þú við – If you want the receivers to be able to grant the rights to others, you add

  WITH GRANT OPTION

Dæmi um GRANT – Example of GRANT

- Ef þú ert eigandi Sells töflunnar getur þú skrifað – If you are the owner of the Sells table you can write

  ```
  GRANT SELECT, UPDATE(price)
  ON Sells
  TO Nonni;
  ```

- Nú hefur Nonni rétt á gera hvaða fyrirspurn sem er á Sells töfluna og getur aðeins uppfært gildi í price dálkinum – Now Nonni has the right to perform any query on the Sells table and can only update values in the price column

Dæmi um/Example on WITH GRANT OPTION

- Ef við einnig gefum réttindi – If we also grant rights

  GRANT UPDATE ON Sells TO Nonni WITH GRANT OPTION;

- þá getur Nonni nú uppfært hvaða dálk sem er í Sells og getur einnig gefið öðrum heimildina UPDATE á Sells töfluna – Then Nonni can update any column in Sells and can also grant the UPDATE right to others
- Einnig getur Nonni gefið þrengri heimildir svo sem – Nonni could also give a narrower right such as
  - UPDATE(price) ON Sells

Afturköllun heimilda – Revokation of rights

- Skipunin / The command

  REVOKE <listi heimilda/list of rights>
  ON <tafla eða annar hlutur/table or other object>
  FROM <listi notandanafna/list of authorization ids>
  [CASCADE | RESTRICT];

- veldur því að þín heimildaveiting á þessum heimildum til þessara notanda getur ekki lengur verið grundvöllur þess að notendurnir noti þessar heimildir – has the effect that your access right grants of these rights to these users can no longer be the basis for these users to use those rights
  - Það getur samt verið að notendurnir hafi sömu heimildir á grundvelli heimildaveitinga frá öðrum, en ekki ef heimildaveitingin var á grundvelli heimildaveitinga frá þér, beint eða óbeint – It is however possible that the users have the same rights on the basis of access grants from others, but not if the grant was based on a grant from you, directly or indirectly

REVOKE valkostir – REVOKE options

- Aftast í REVOKE skipuninni má vera annað hvort – At the end of the REVOKE command we may have either

1. CASCADE: Heimildir sem sá notandi sem er að missa heimildir hefur veitt öðrum á grundvelli þeirra, beint eða óbeint, á viðkomandi hluti, eru einnig afturkallaðar – Rights that the user that is losing its rights has granted to others on their basis, directly or indirectly, are also revoked
2. RESTRICT: Ef notandinn sem á að missa heimildir hefur veitt öðrum heimildir á grundvelli þeirra þá er engin heimild afturkölluð frá neinum og í stað þess kemur villa, sem er aðvörun um að eitthvað annað þurfi að gera til að elta uppi heimildirnar og bregðast við á viðeigandi hátt – If the user that is to lose rights has granted rights to others on their basis then no rights are revoked and instead an error occurs, which is a warning that something should be done to chase up those rights and respond in an appropriate way

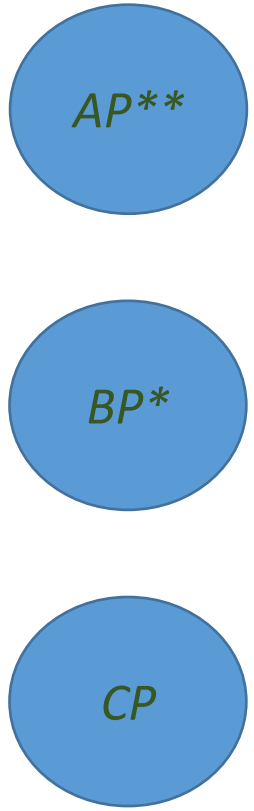
- Sleppa má valkostinum, sem hefur þá sömu merkingu og RESTRICT – Both may be omitted, which has the same effect as RESTRICT

Heimildanet – Grant Diagrams

- Heimildanet eru notuð til að skrá og staðfesta heimildir – Grant disgrams are used to record and confirm rights
- Heimildanet eru stefnd net – Grant diagrams are directed graphs
- Hnútar í heimildaneti samsvara heimild og notanda, ásamt upplýsingum um hvort heimildin innifeli GRANT OPTION og hvort notandinn er eigandi hlutarins – Nodes in a grant diagram correspond to a right and a user along with information whether the user has a GRANT OPTION and whether the user is the owner of the object
- Stika $X \rightarrow Y$ þýðir að hnútur X var notaður til að veita heimildirnar í hnúti Y – An arc $X \rightarrow Y$ means that node X was used as a source of the rights in node Y
- Tilgangurinn er að skrá veittar heimildir og uppsprettur þeirra heimilda og að gera breytingar vel skilgreindar og auðveldar – The purpose is to record granted rights and their sources and make changes well defined and easy

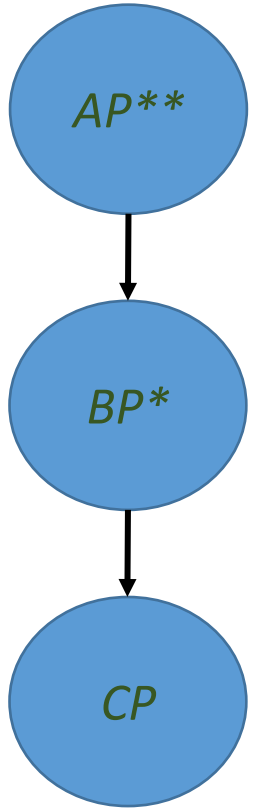
Heimildanet – Grant Diagrams

- Látum hnút vera merktan með rithættinum AP til að tákna að notandi A hafi heimild P – Let a node be marked with the notation AP to denote that user A has right P
- $P*$ er heimild með GRANT OPTION
  $P*$ is a right with GRANT OPTION
- $P**$ er frumuppspretta heimildar P
  $P**$ is the original source of right P
  - A er þá eigandi þess hlutar sem heimildin er fyrir
    A is then the owner of the object that the right is for
  - Óhjákvæmilega fylgir GRANT OPTION með **
    Unavoidably a GRANT OPTION goes with **



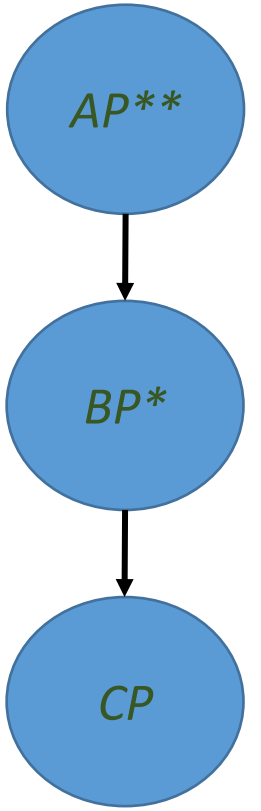
Stikur í heimildaneti – Arcs in a Grant Diagram (1/3)

- Þegar A gefur heimild P til B táknum við það með stiku frá $AP*$ eða $AP**$ til BP
  When A grants permission P to B we denote this with an arc from $AP*$ or $AP**$ to BP
  - Eða til $BP*$ ef heimildin er með GRANT OPTION
    Or to $BP*$ if the permission is with GRANT OPTION
- Ef heimildin er undirheimild Q á heimild P
  If the permission is a subpermission Q on permission P
  - til dæmis „UPDATE(a) ON R“ þar sem P er „UPDATE ON R“
    for example “UPDATE(a) ON R“ where P is “UPDATE ON R“
- þá fer stikan til BQ eða $BQ*$ í staðinn
  then the arc goes to BQ or $BQ*$ instead



Stikur í heimildaneti – Arcs in a Grant Diagram (2/3)

- Grundvallarregla / Foundational Rule:
- Notandi C hefur heimild Q þá og því aðeins að það sé vegur frá $XP{*}{*}$ til CQ, $CQ{*}$ eða $CQ{*}{*}$ og P sé yfirheimild Q
  User C has right Q if and only if there is a path from $XP{*}{*}$ to CQ, $CQ{*}$ or $CQ{*}{*}$ and P is a subpermission of Q
  - Munum að P gæti verið Q og X gæti verið C
    Remember that P might be Q and X might be C
  - Ef X er ekki C þá er $CQ{*}{*}$ ekki möguleiki því aðeins einn eigandi getur verið til staðar
    If X is not C then $CQ{*}{*}$ is not a possibility because there can only be one owner
- Staðfesting heimildar / Verifying a permission
  1. Er notandinn eigandi hlutarins? – Is the user the owner of the object?
  2. Er hluturinn PUBLIC? – Is the object public
  3. Hefur notanda verið veittur aðgangur að hlutnum í heimildaneti?
     Has the user received permission to the object in a grant diagram?

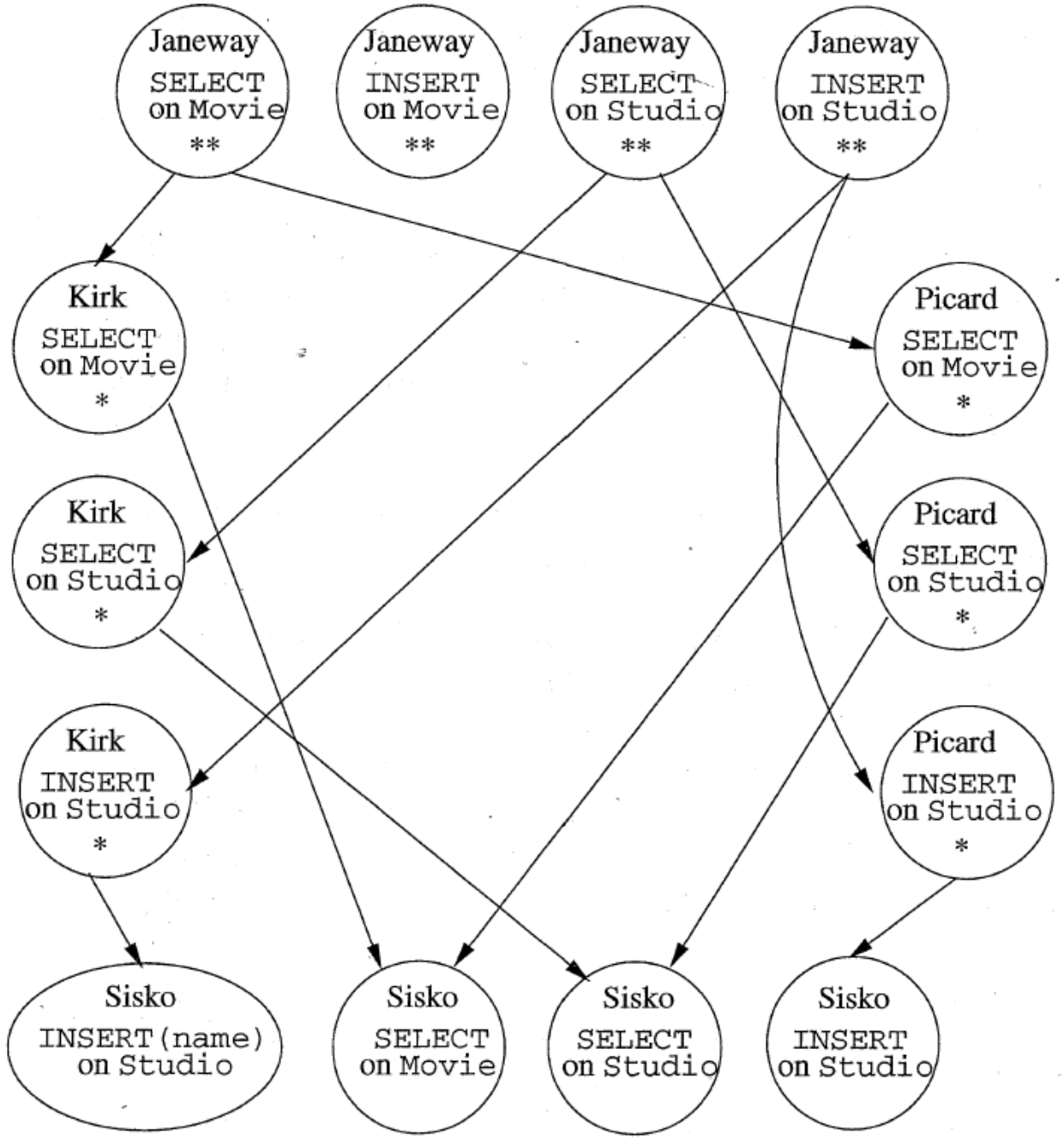


Stikur í heimildaneti – Arcs in a Grant Diagram (3/3)

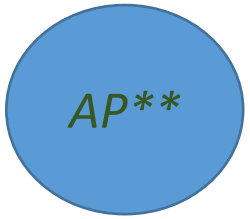
- Ef A afturkallar heimild P frá B með CASCADE þá eyðum við öllum stikum $\rightarrow BP$ sem koma frá hnúti sem hefur fengið sína heimild,
  beint eða óbeint, frá A
  If A revokes a permission P from B with CASCADE then we delete all arcs $\rightarrow BP$ that come from a node that got its permission, directly or indirectly, from A
- Hins vegar ef A afturkallar heimild P frá B með RESTRICT og til er stika $BP \rightarrow CP$ þá er afturköllunninni hafnað með villumeldingu og engin breyting er gerð á netinu
  On the other hand if A revokes permission P from B with RESTRICT and there exists an arc $BP \rightarrow CP$ then the revokation is rejected with an error message and no change is made to the diagram
- Eftir að stiku er eytt þarf að staðfesta að til allra hnúta í netinu sé til vegur frá ** hnúti (sem samsvarar þá eiganda hlutarins og er því uppspretta slíkra heimilda á hlutinn)
  After an arc is deleted we need to verify that there is a path to all nodes in the diagram from a ** node (that then corresponds to the owner of the object and is therefore the primary source of all such permissions)
- Ef hnútur hefur ekki slíkan veg þá stendur hnúturinn fyrir afturkallaða heimild og hnútnum er þá eytt úr netinu
  Is the node has no such path then the node stands for a revoked permission and is then deleted from the diagram

Dæmi – Example

- Látum notanda Janeway framkvæma
  Let user Janeway execute
  CREATE TABLE Movies(...);
  CREATE TABLE Studio(...);
  GRANT SELECT, INSERT ON Studio TO Kirk, Picard WITH GRANT OPTION;
  GRANT SELECT ON Movies TO Kirk, Picard WITH GRANT OPTION;
- Látum síðan Picard framkvæma
  Then let Picard execute
  GRANT SELECT, INSERT ON Studio TO Sisko;
  GRANT SELECT ON Movies TO Sisko;
- Og látum Kirk framkvæma
  And let Kirk execute
  GRANT SELECT, INSERT(name) ON Studio TO Sisko;
  GRANT SELECT ON Movies TO Sisko;

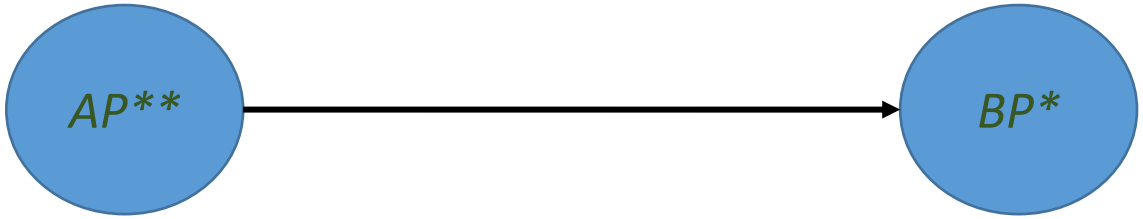


Dæmi um heimildanet
Example of grant diagram



A er eigandi hlutar, P er heimild á hlutnum
A is the owner of an object, P is a permission on the object

Dæmi um heimildanet
Example of grant diagram

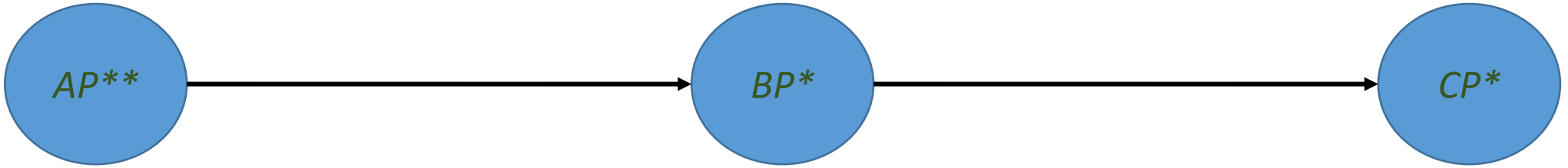


A er eigandi hlutar, P er heimild á hlutnum
A is the owner of an object, P is a permission on the object

A gerir – A executes:
GRANT P TO B WITH GRANT OPTION

Dæmi um heimildanet
Example of grant diagram

B gerir – B executes:
GRANT P TO C WITH GRANT OPTION

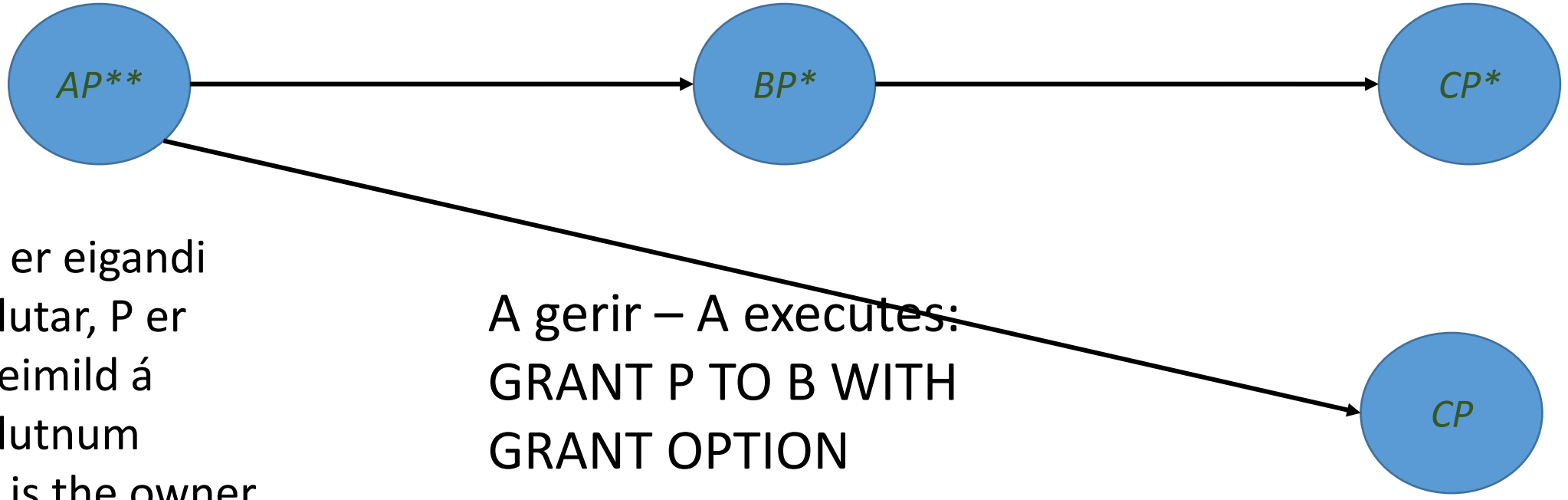


A er eigandi hlutar, P er heimild á hlutnum
A is the owner of an object, P is a permission on the object

A gerir – A executes:
GRANT P TO B WITH GRANT OPTION

Dæmi um heimildanet
Example of grant diagram

B gerir – B executes:
GRANT P TO C WITH GRANT OPTION

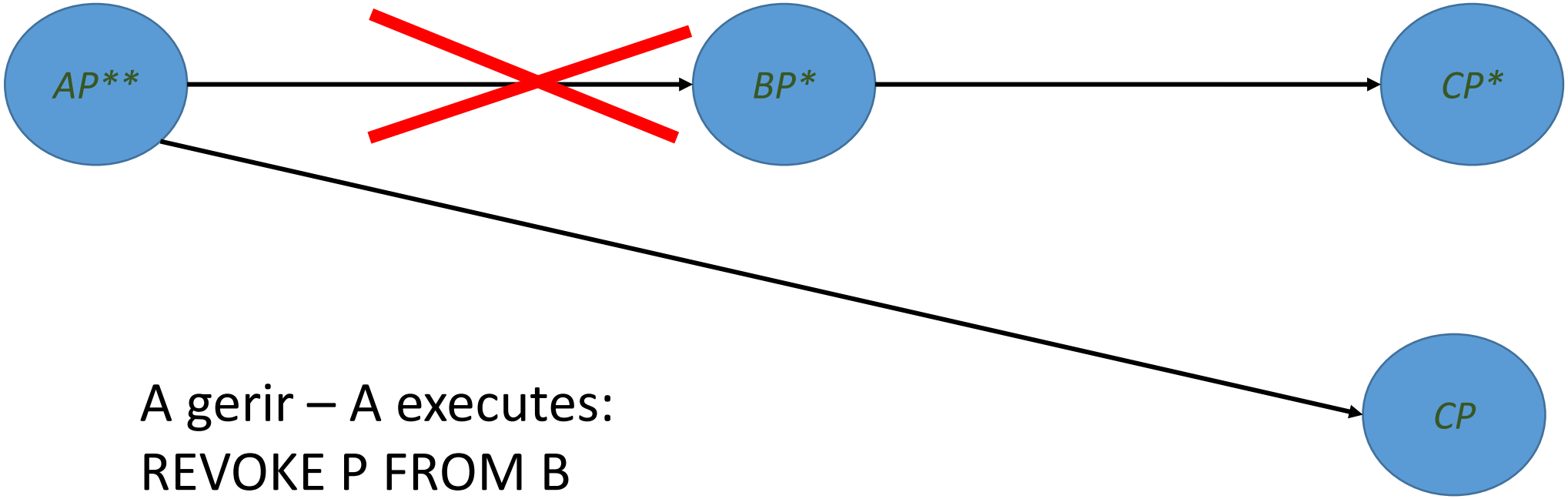


A er eigandi hlutar, P er heimild á hlutnum
A is the owner of an object, P is a permission on the object

A gerir – A executes:
GRANT P TO B WITH GRANT OPTION

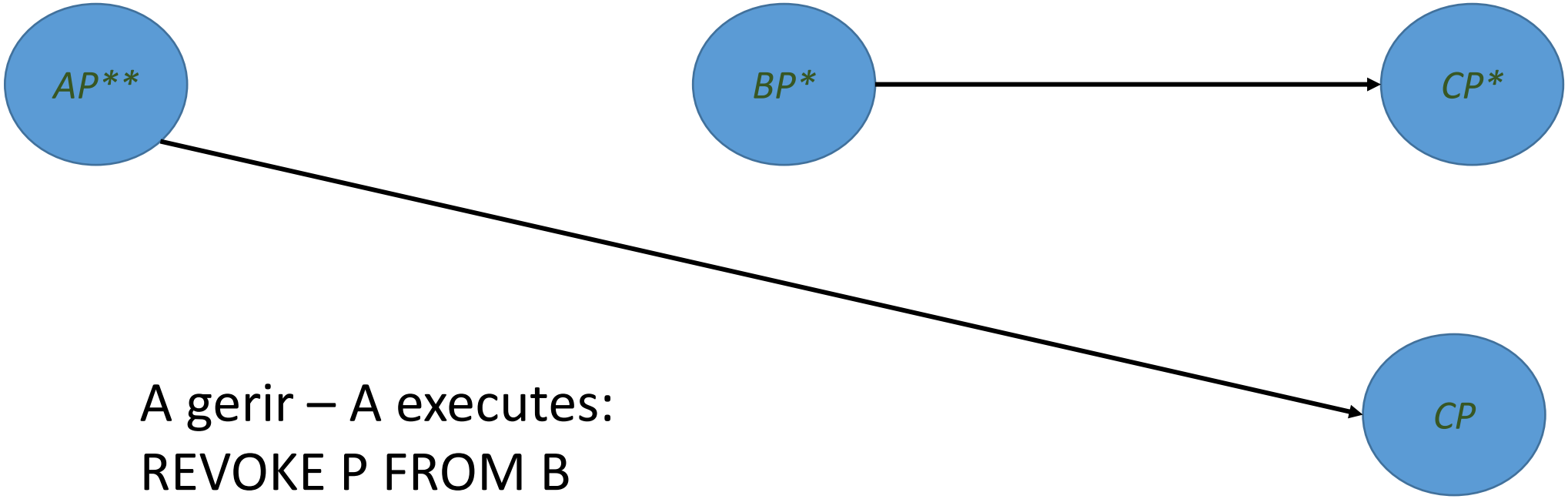
A gerir – A executes:
GRANT P TO C

Dæmi um heimildanet
Example of grant diagram



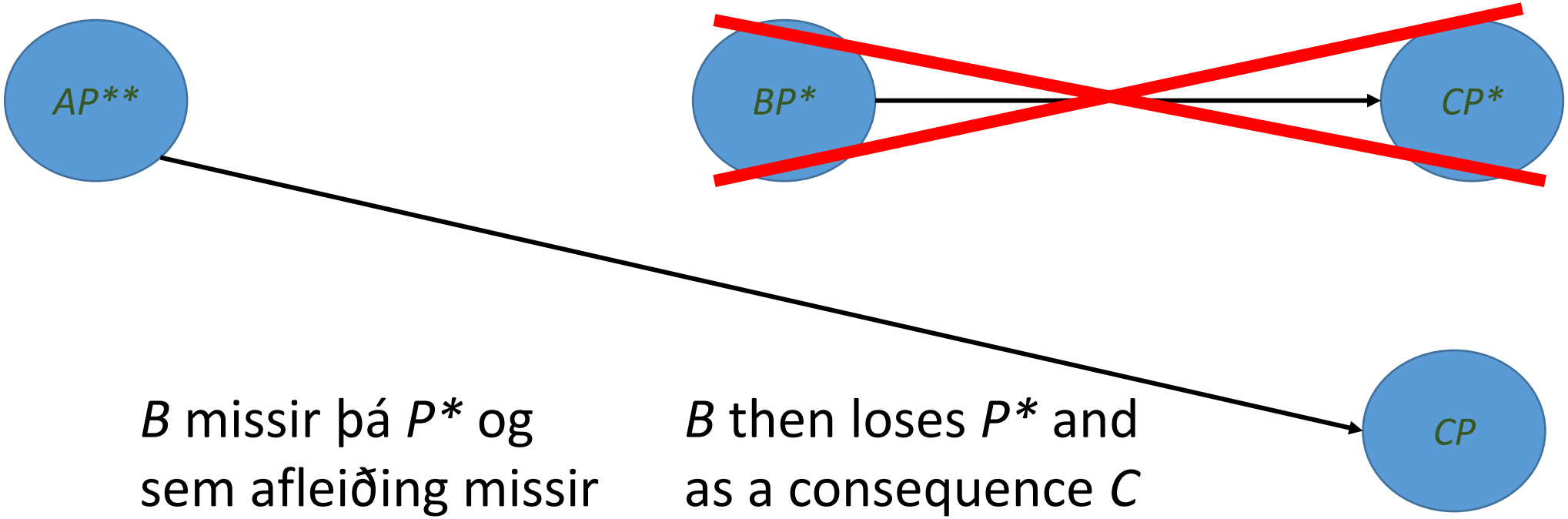
A gerir – A executes:
REVOKE P FROM B
CASCADE

Dæmi um heimildanet
Example of grant diagram



A gerir – A executes:
REVOKE P FROM B
CASCADE

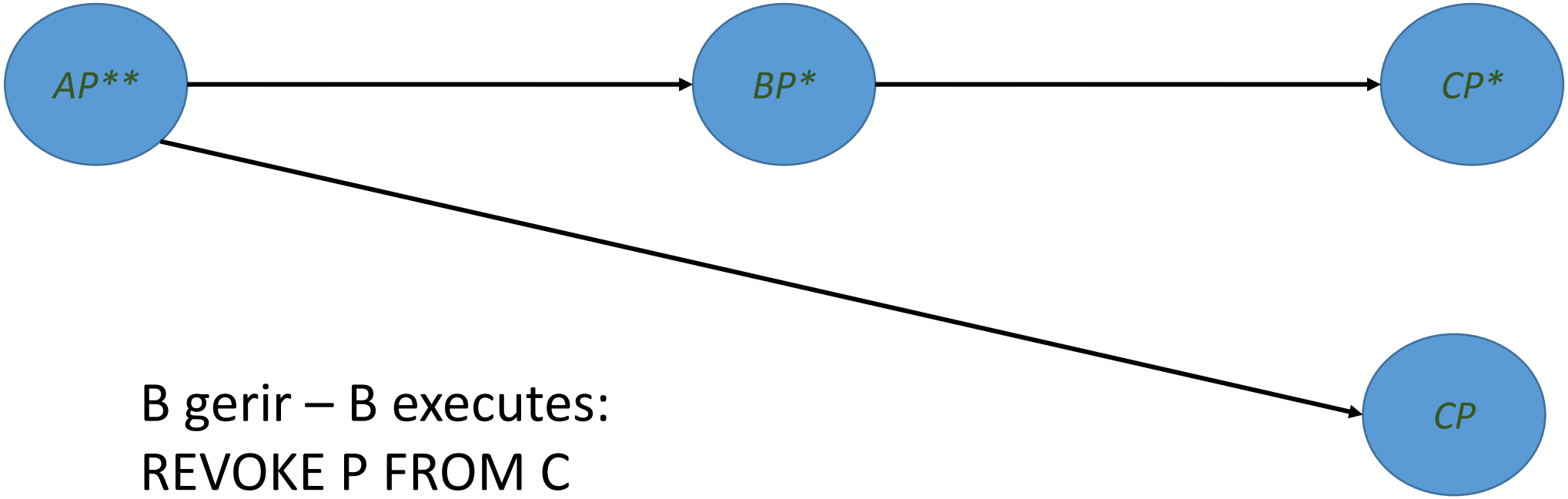
Dæmi um heimildanet
Example of grant diagram



B missir þá *P** og sem afleiðing missir *C* einnig *P**.
Eyðum því hnútum *BP** og *CP**.

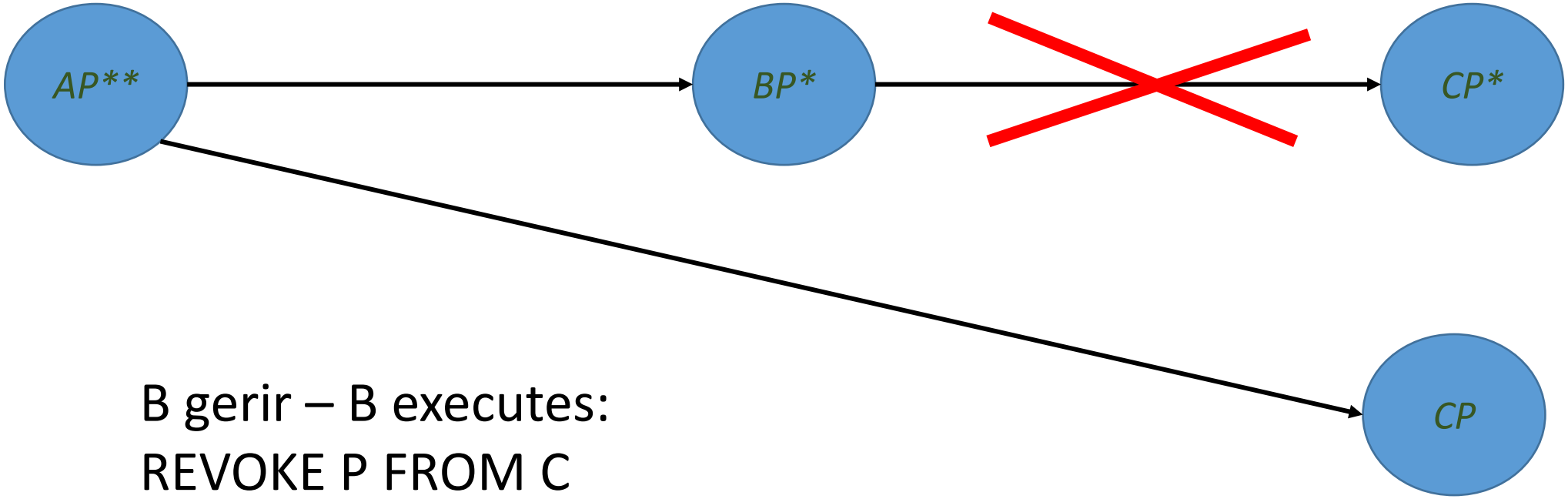
B then loses *P** and as a consequence *C* also loses *P**.
Therefore delete the nodes *BP** and *CP**.

Dæmi um heimildanet
Example of grant diagram



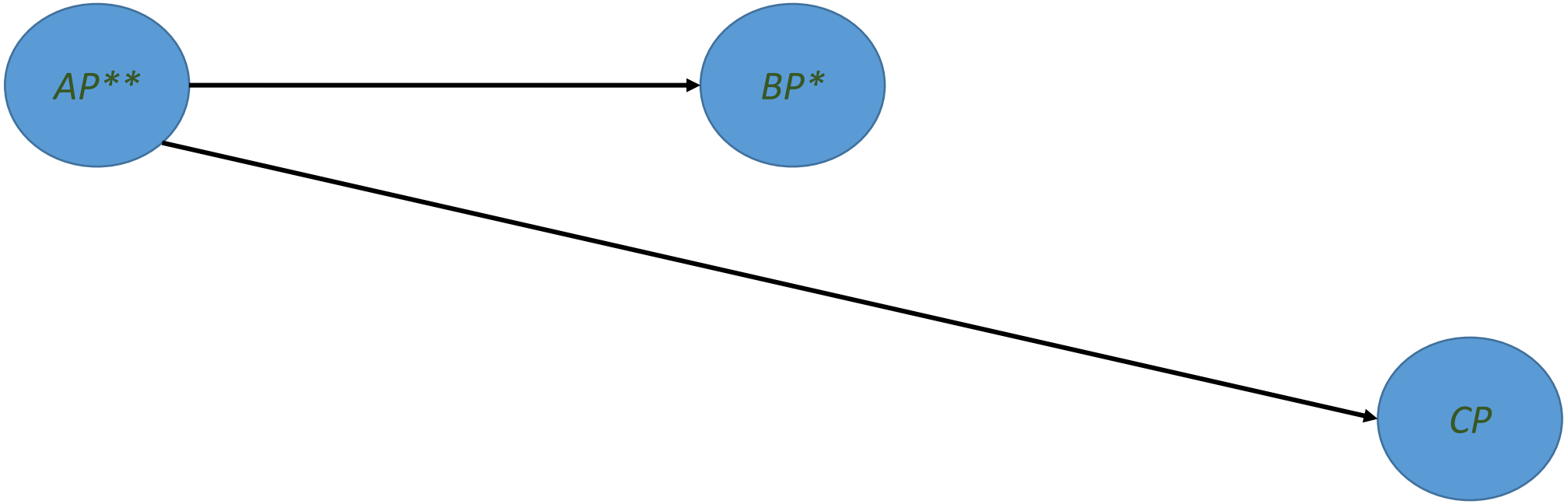
B gerir – B executes:
REVOKE P FROM C

Dæmi um heimildanet
Example of grant diagram

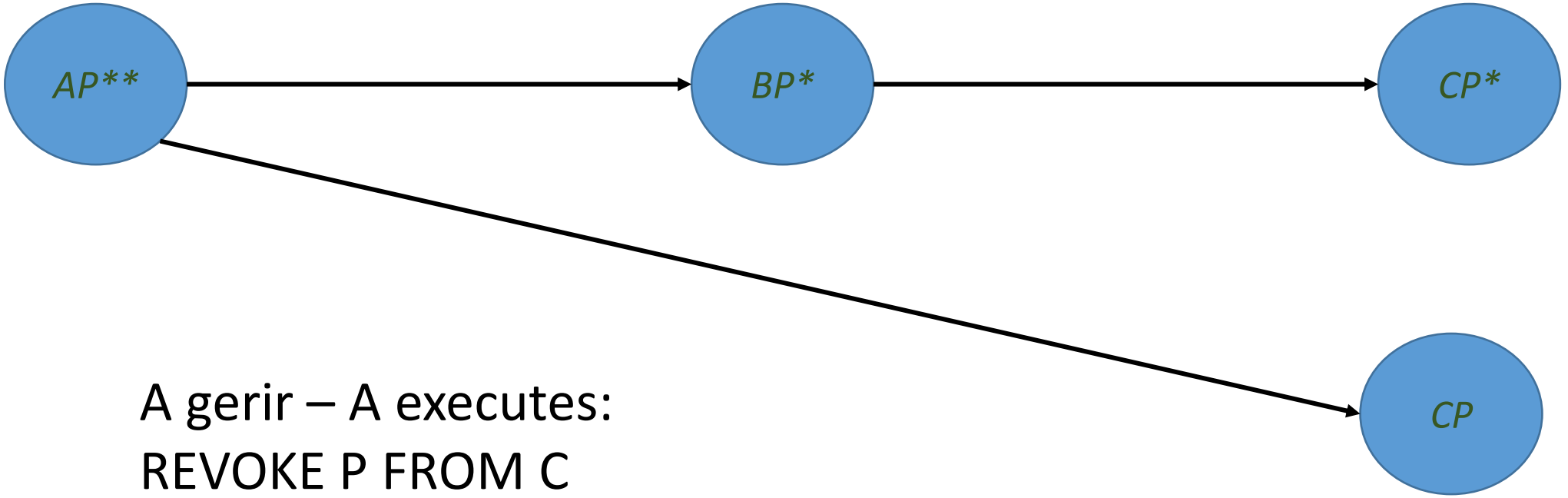


B gerir – B executes:
REVOKE P FROM C

Dæmi um heimildanet
Example of grant diagram

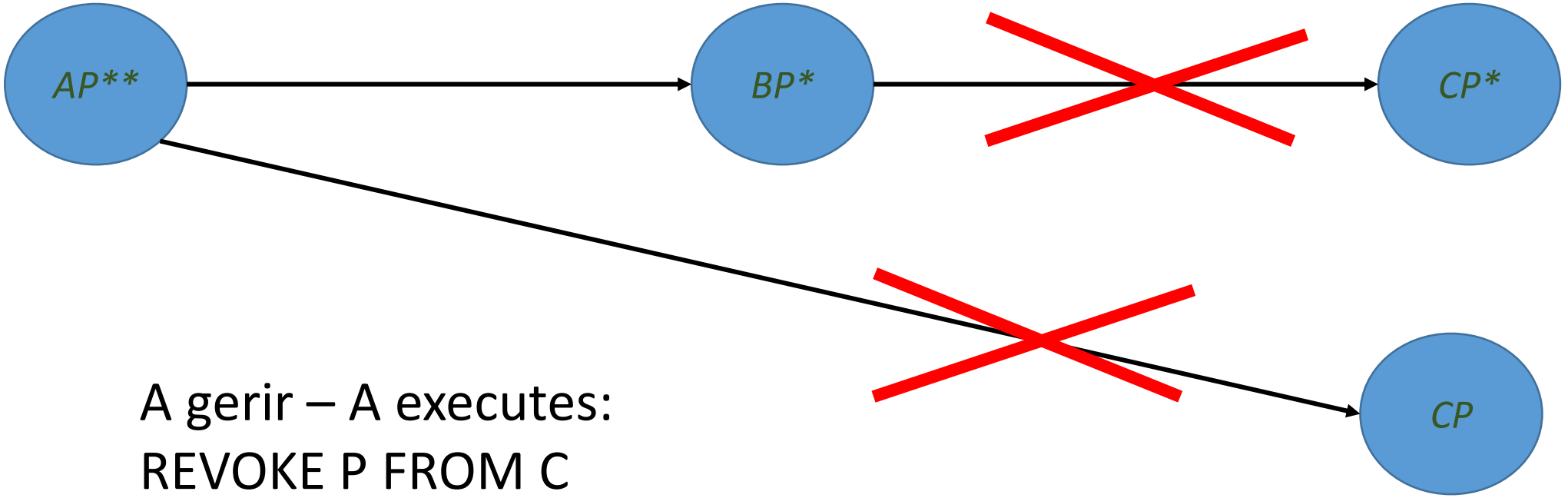


Dæmi um heimildanet
Example of grant diagram



A gerir – A executes:
REVOKE P FROM C

Dæmi um heimildanet
Example of grant diagram



A gerir – A executes:
REVOKE P FROM C

Dæmi um heimildanet
Example of grant diagram