Improvements on Conventional PKI Wisdom

Carl M. Ellison
Sr. Security Architect
Corporate Technology Group
Intel Corporation

1st PKI Workshop: April 24, 2002

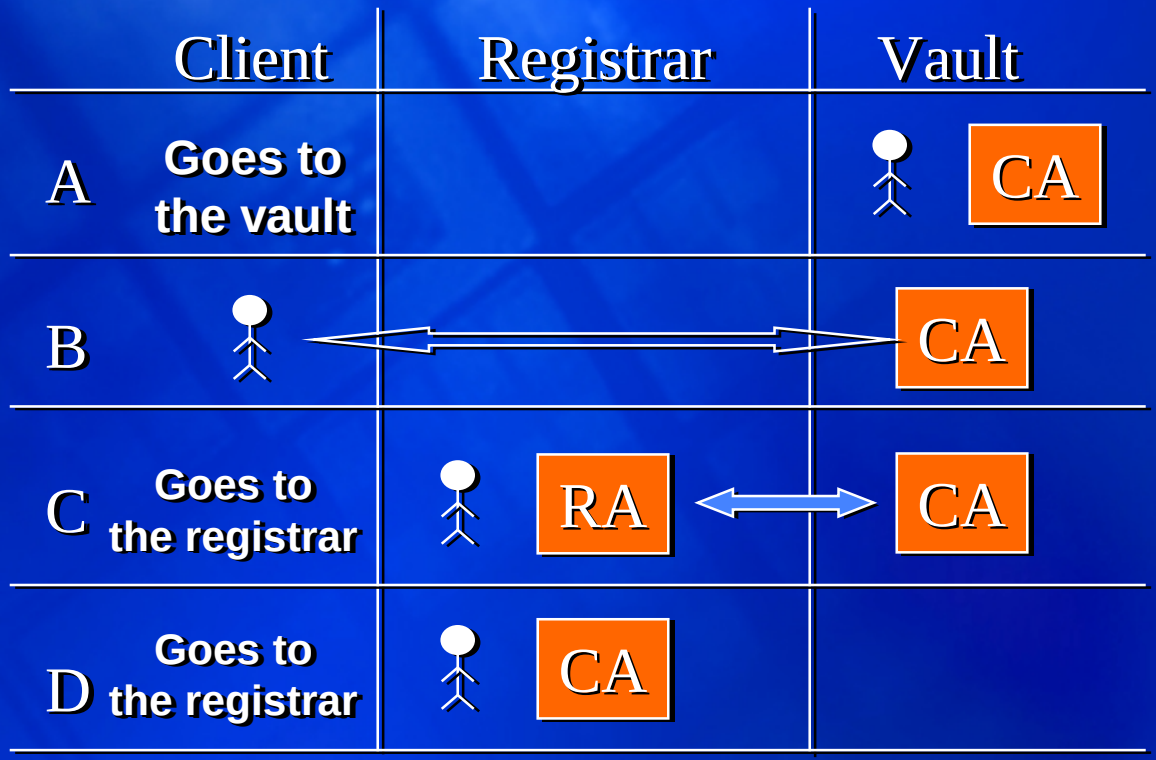
Conventional PKI Wisdom

1. Get and use an acceptable ID certificate for digital signatures.
2. Each certificate should come from a CA with strong key security (a vault).
3. This allows you to know who your transaction partner is.
4. This process gives non-repudiation.

1. ID Certificates

- Which ID should I use and who should certify me?
  - 5 at work: carl.m.ellison; cme; amr/cellison; Ellison, Carl M; <WWID>
  - >12 at home: driver's License number; 4 credit card numbers; 1 ATM card; bank and stock brokerage account numbers; e-mail account names; login names
- So … should we change all existing business practices to use a single ID?

2. CA Security



Too expensive for real use

Grossly insecure

OK, but security can be better

Fewer parts; no network; same key vulnerability

3. Know the other person

- The John Wilson Problem
  - E-mail
  - Bay area trip, August 2001
  - Ann Harrison
- Moral of the story: human beings do not use names the way we computer scientists would like them to.
- So … should we change all humans?

4. Non-repudiation (NR)

- Delayed enforcement: prosecute fraud
- Expensive to track & prosecute
- Valid only if victim can be made whole
  - not for secrets or high value content or lives
- Not possible to implement
  - inadequate protection of keys and S/W
  - inadequate physical security
  - no H/W to witness the signing
- That's OK. If you need legal enforceability, you can use contractual commitment.

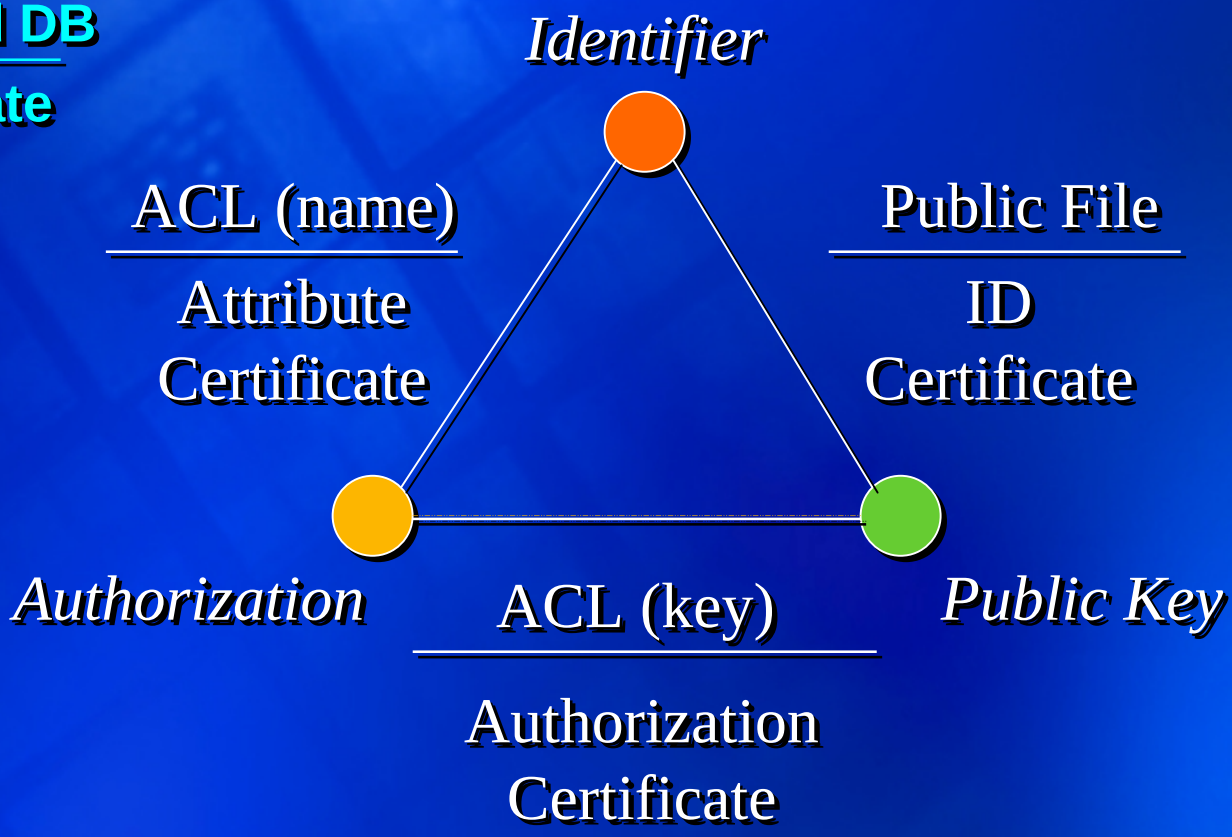
New PKI Wisdom

1. There is no single ID, so a single ID certificate makes no sense.
2. Discard RAs and put CAs on RA desks.
3. Knowing a keyholder's certified name does not tell you who that keyholder is.
4. Non-repudiation is neither adequate for serious problems nor achievable.
5. Do authorization (e.g., access control) up front, instead.

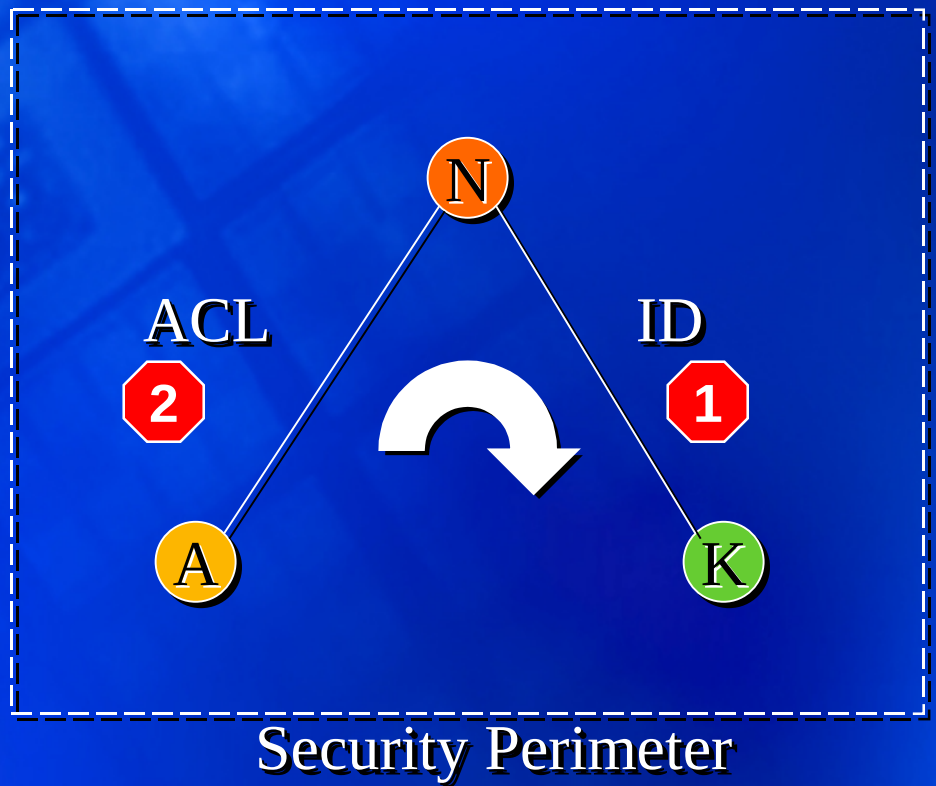
Credential Classes

Protected DB

Certificate

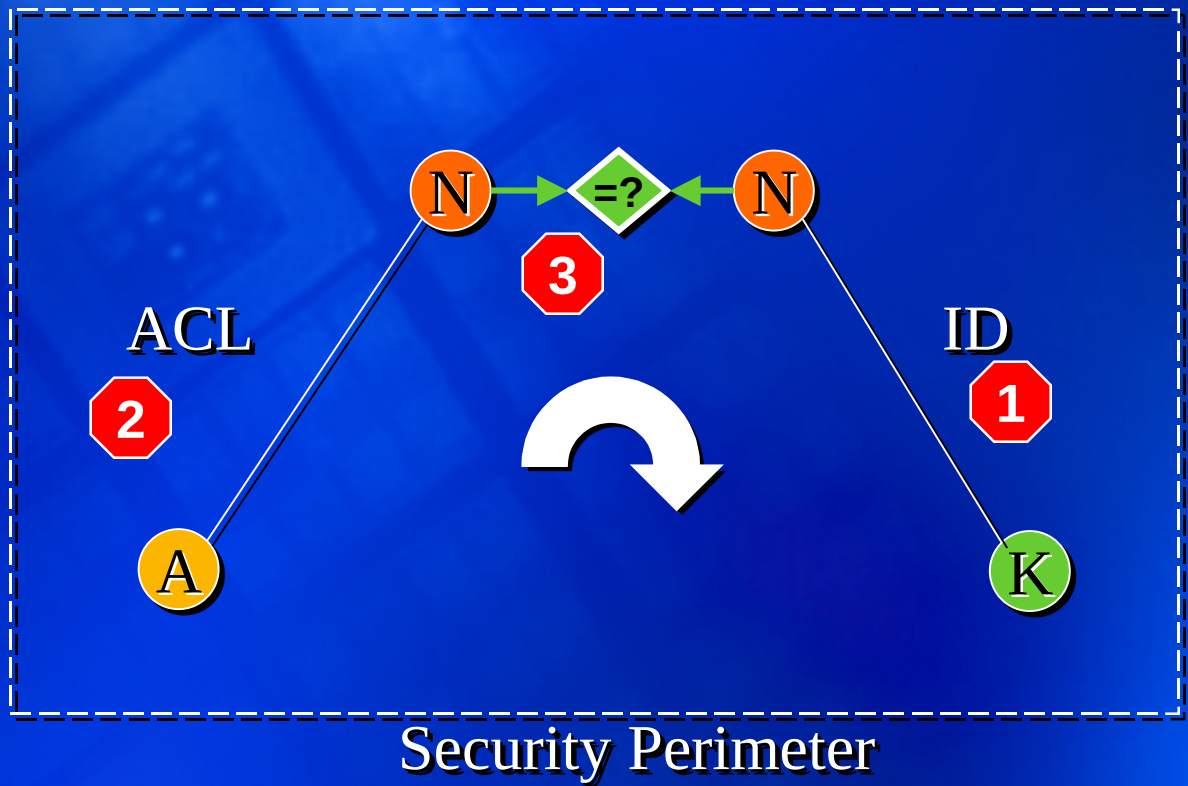


Authorization (1)



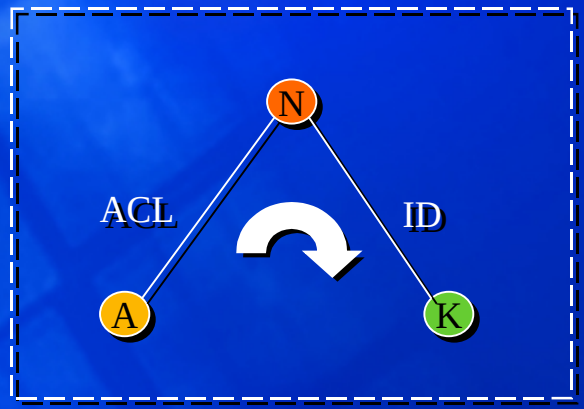
3 points of attack

Authorization (1)



3 points of attack

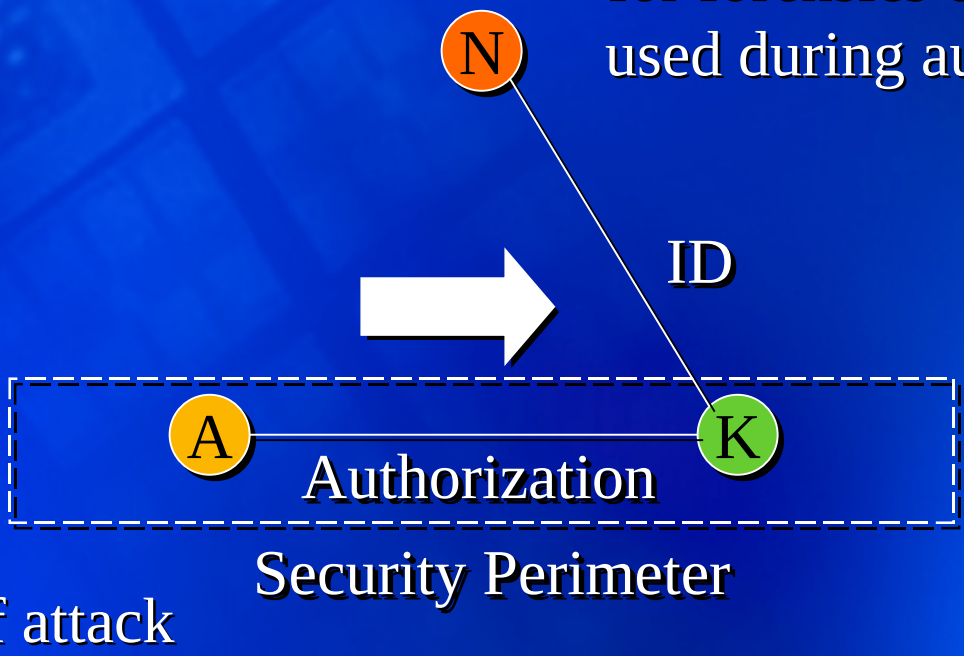
Authorization DB Example



- Large centralized ACL (authorization DB)
  - 6 million users
  - If each user changes status every 2 years, that is one change in the ACL every 2.5 seconds of a standard work day. Each must be investigated.
  - How many people must staff the ACL office?
  - What makes them authorities? …trusted?
  - Is there only one office?

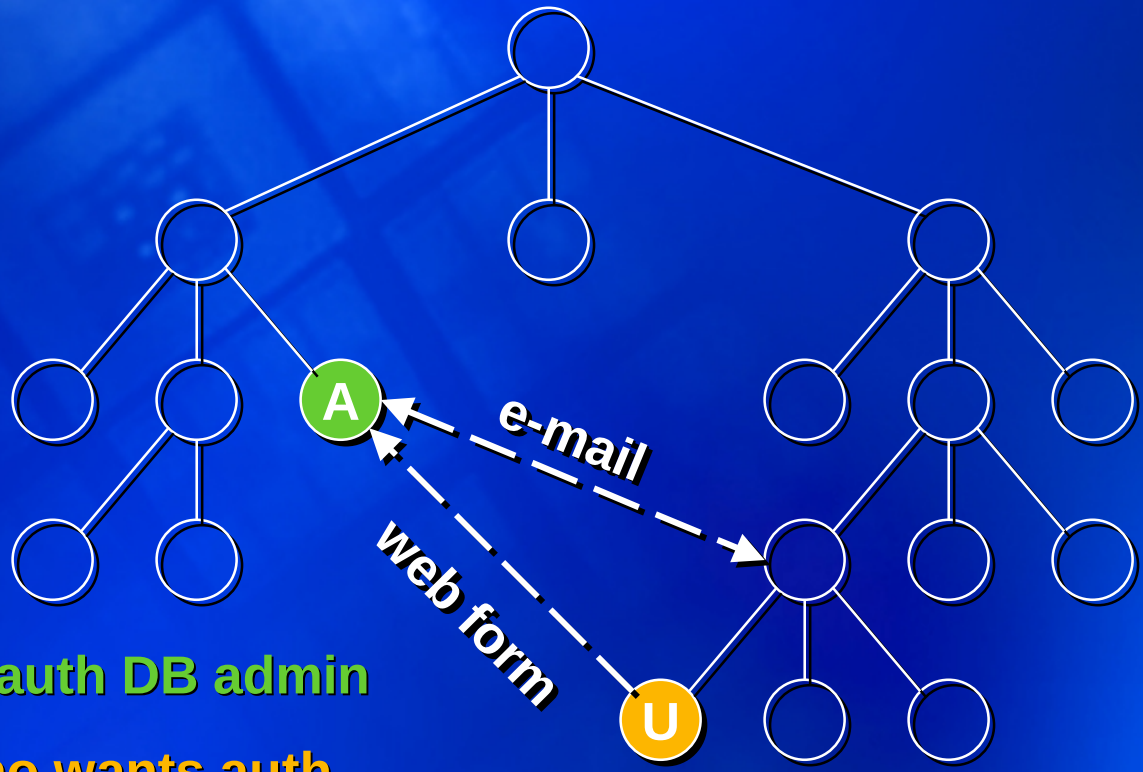
Authorization (2)

ID or locator information for forensics only, not used during authorization.



1 point of attack

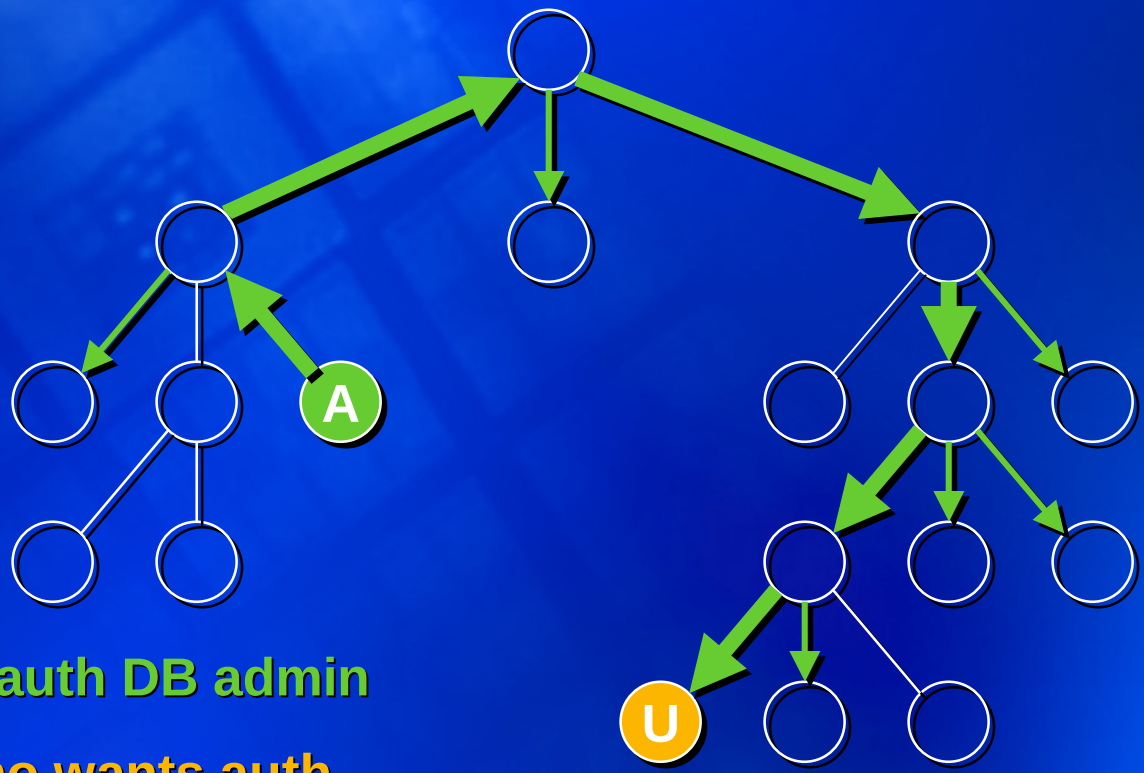
Authorization Example (1)



A: Central auth DB admin

U: User who wants auth

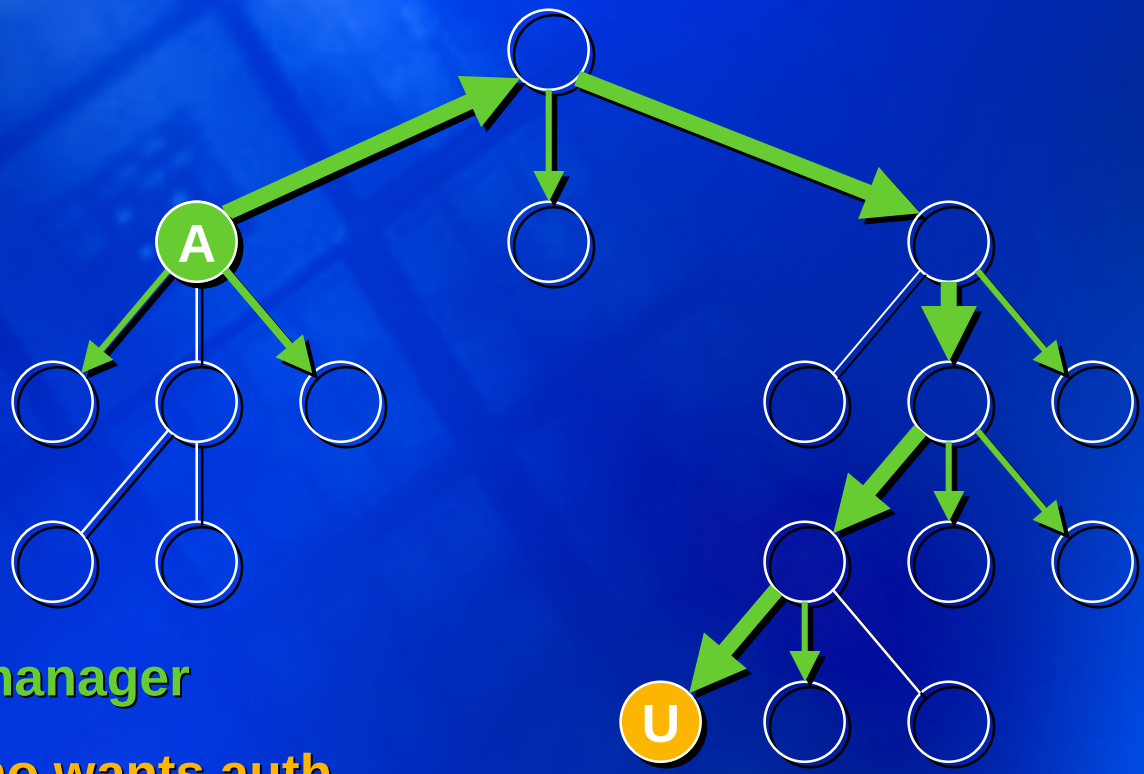
Authorization Example (2)



A: Central auth DB admin

U: User who wants auth

Authorization Example (2)

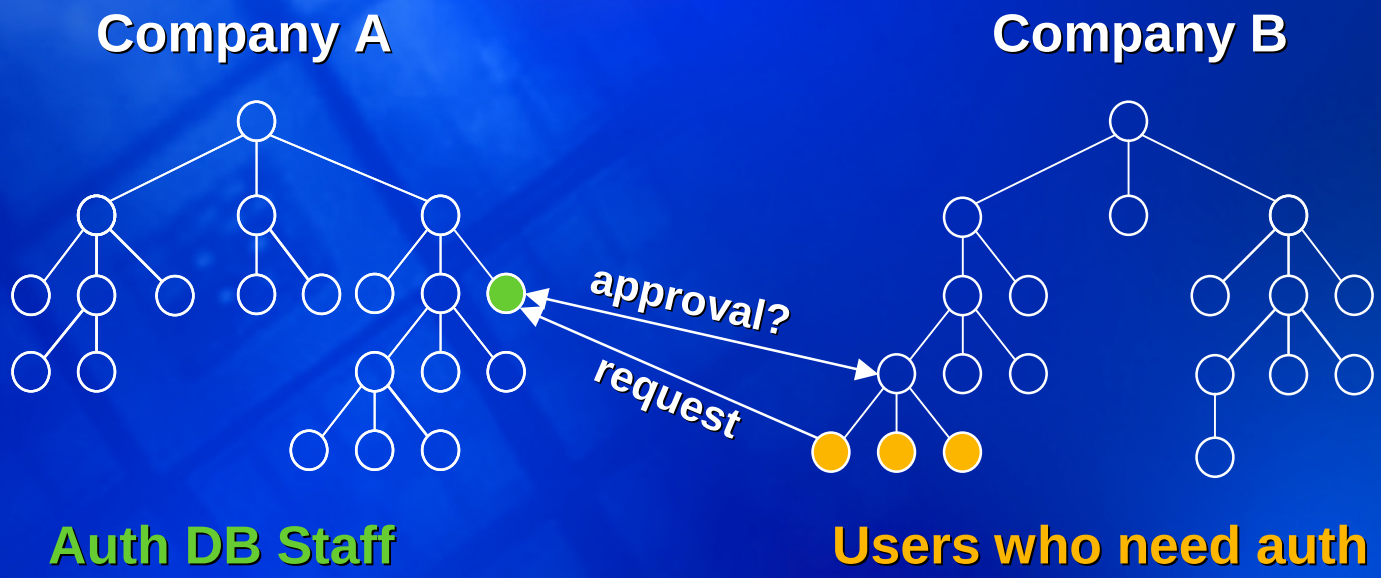


A: Policy manager

U: User who wants auth

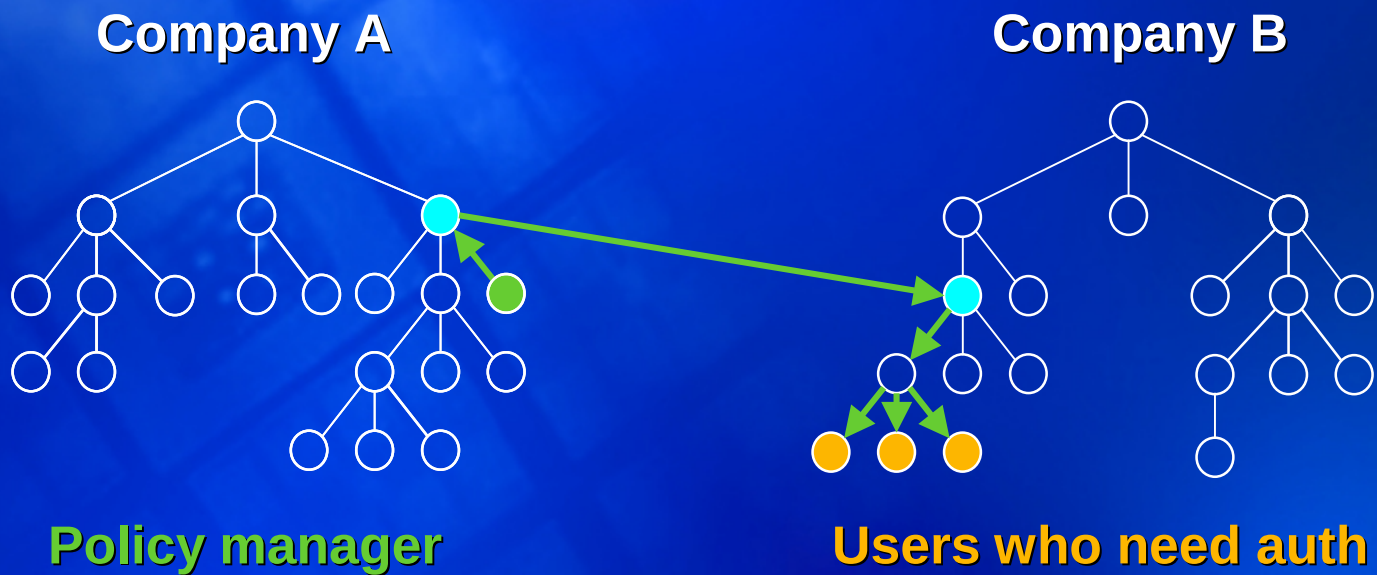
Side-effect: No central DB to maintain so staff not needed for DB administration, saving money while improving security.

Cross-company (1)



- Bridge two PKIs ⇒ The John Wilson problem gets *MUCH* worse.
  - There are suddenly more John Wilsons than there were before.
  - There is no central naming authority with control over all PKIs.
- Access by A to B's confidential information? (org chart; names)
- If A keeps a copy of a subset of B's info, that's dynamic & requires its own auth DB at A for updaters ⇒ design recursion.
- If A accesses B data in place, that requires an auth DB at B. (ditto)

Cross-company (2)



Bridged by executives who sign the B2B relationship contract

- No bridging of ID PKIs
- No names used, so no John Wilson problem
- No access to the other company's employee data
- Improved security

References

- Dohrmann and Ellison, “Public Key Support for Collaborative Groups”, Internet2 PKI Workshop, April 2002.
- Ellison, “Establishing Identity Without Certification Authorities”, 6th USENIX Security Symposium, 1996.
- http://developer.intel.com/ial/security/
- http://world.std.com/~cme/html/spki.html