CPSC 457/557 // Exam 1 // October 15, 2013

Answer all of the questions. Please remember to write your name, the course number, and today's date on all blue books that you submit.

You need not justify your answers to True-False or multiple-choice questions.

This is a closed-book exam; please do not refer to any books or notes, and please do not talk to any of the other students.

Question 1 (18 points):

The context for this question is Microsoft's differential pricing of Windows – specifically, its creation of a simplified-Chinese version of Windows that is sold only in China at a price that Chinese consumers can afford.

a) (8 points) What is the *reimportation problem* faced by US companies that use differential pricing to sell products in developing countries?

b) (6 points) How has Microsoft solved (or at least partially solved) this problem in the case of Windows?

c) (4 points) The solution in part (b) does not work for all products made by US companies and sold more cheaply in developing countries than they are sold in the US. Give an example of a product for which it does not work.

Question 2 (10 points):

a) (6 points) For two points each, give three situations in which circumvention of effective technological-protection measures *is* allowed under the Digital Millennium Copyright Act.

b) (2 points) True or False: In order to be guilty of violating the Digital Millennium Copyright Act, one must be guilty of copyright infringement.

c) (2 points) True or False: In the US, private, noncommercial copying is always fair use.

Question 3 (15 points):

a) (6 points) What does Solove mean by the "secrecy paradigm," and why is its relevance to privacy norms increasing as computers and networks become more prevalent in daily life?

b) (6 points) What does Solove mean by "increased accessibility," and what is its relevance to courts' and other government agencies' placing public records online?

c) (3 points) Which element of Solove's 16-part taxonomy is most directly related to "tagging" of people in pictures that are posted on Facebook?

Question 4 (30 points):

a) (6 points) For 3 points each, define the terms *issuer* and *subject* as they are used in the literature on public-key certificates.

b) (6 points) In the SSL/TLS protocol for securing web traffic, what is the main potential problem that is avoided by the use of public-key certificates?

c) (6 points) In Figure 1, which two signatures must Alice verify before she believes that PK_B is really Bob's public key?

d) (6 points) In Figure 2, which three signatures must Bob verify before he believes that

PK_A is really Alice's public key?
e) (6 points) Suppose that, in Figure 3, Dave has just discovered that CA_1's public-key certificate is on a certificate-revocation list. Which set of signatures should Dave verify before believing that PK_H is Harry's public key?

Question 5 (7 points):
In the physical world, Alice's signatures on two different paper documents are (ideally) identical. By contrast, in the digital world, Alice's signatures on two different digital documents are different. Why is this property of digital signatures necessary for their security?

Question 6 (20 points):
For 4 points each, answer True or False for each of parts a) through e).

a) When you download a webpage, all of its constituent packets must follow the same route from the server to your machine.

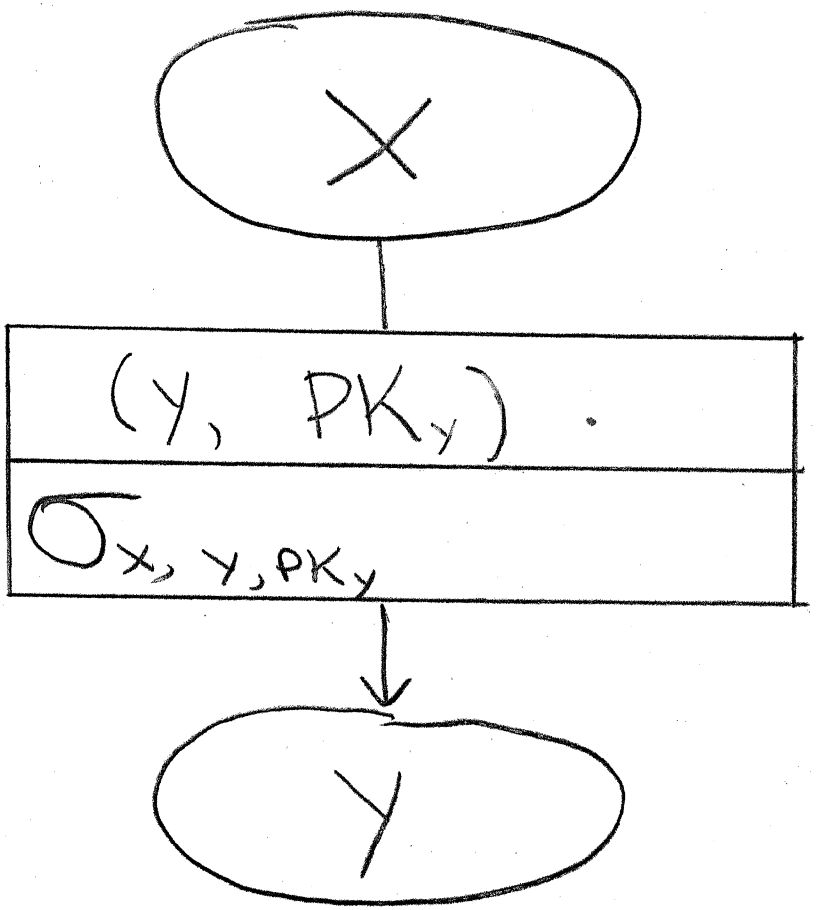
b) If your machine is part of the yale.edu domain, then it must send a query to a DNS server every time you visit a website not hosted by Yale.

c) If a packet is routed along a faulty path and cannot reach its destination, its TTL ("time-to-live") IP-header field can be used to prevent it from looping forever.

d) For any Internet topology and ASes' choices of routing policies, BGP is guaranteed to converge.

e) UDP is a transport-layer protocol that is used by applications that do not require completely reliable packet delivery (*e.g.*, multimedia applications).

In Figures 1, 2, and 3



means that X gives Y a certificate that binds the name Y to the key PK_Y.

σ_{X, Y, PK_Y} is X's signature on the cert.

Figure 1

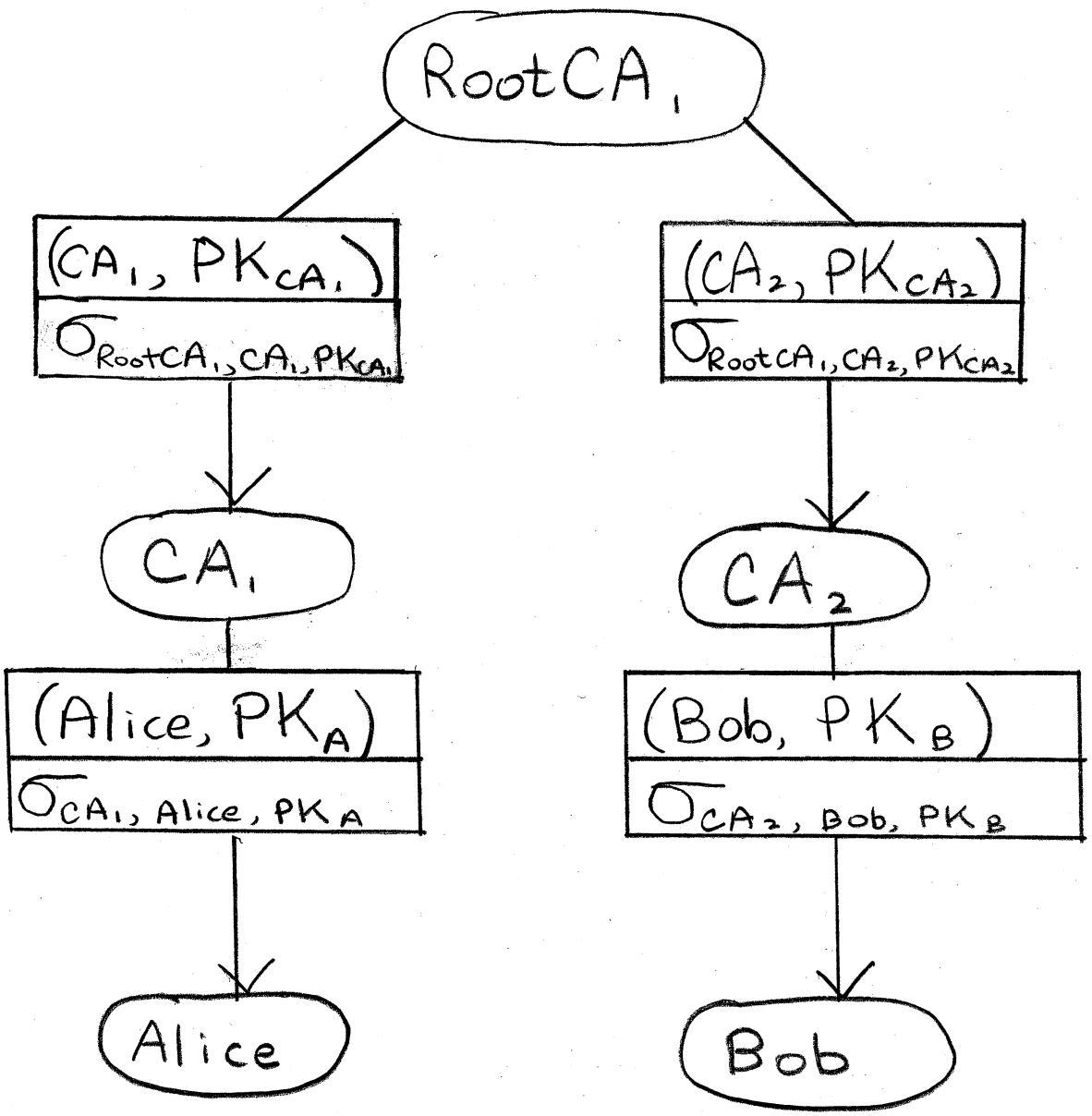

RootCA1
(CA1, PKCA1)
σRootCA1, CA1, PKCA1
(CA2, PKCA2)
σRootCA1, CA2, PKCA2
CA1
CA2
(Alice, PKA)
σCA1, Alice, PKA
(Bob, PKB)
σCA2, Bob, PKB
Alice
Bob

Figure 2

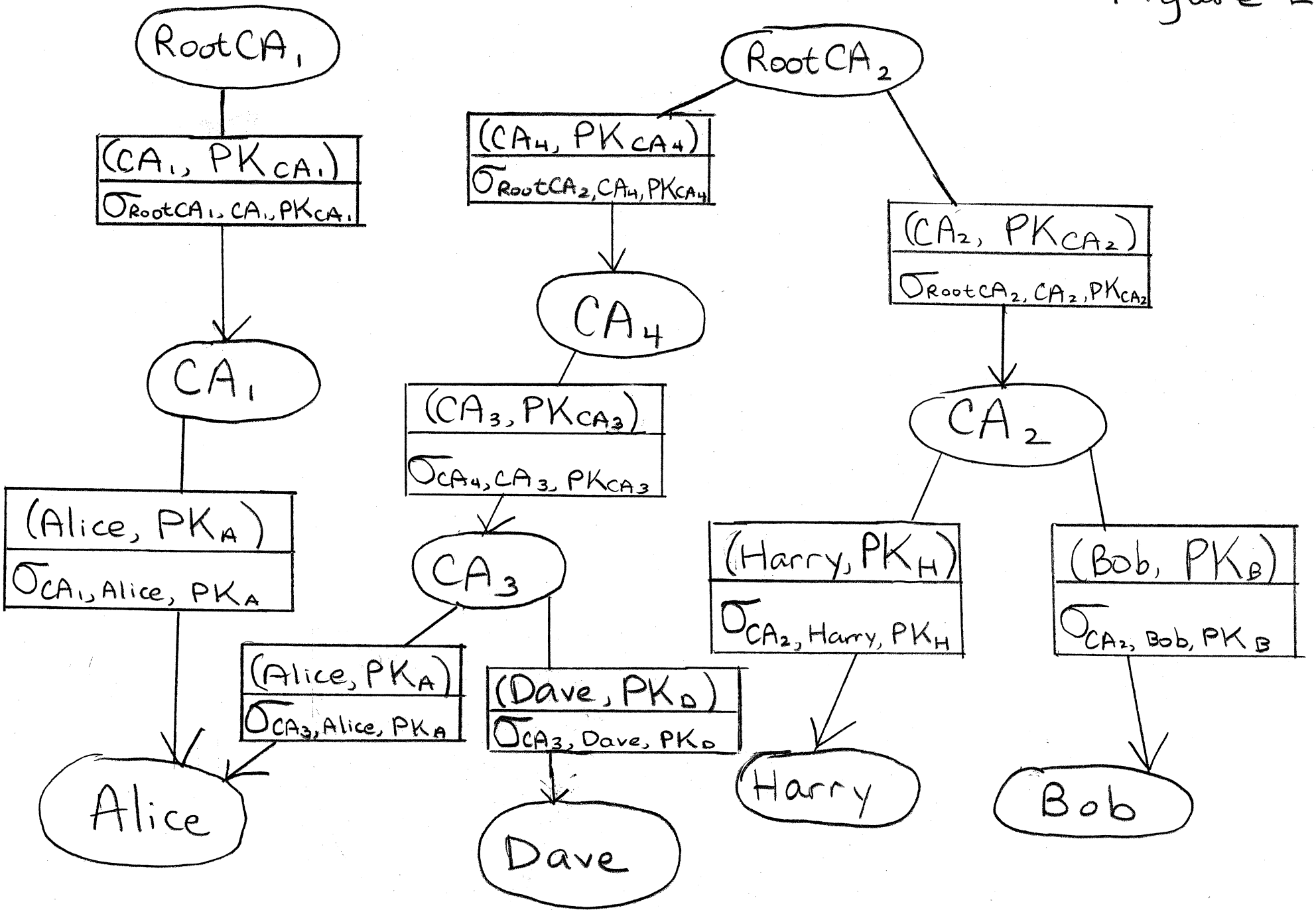
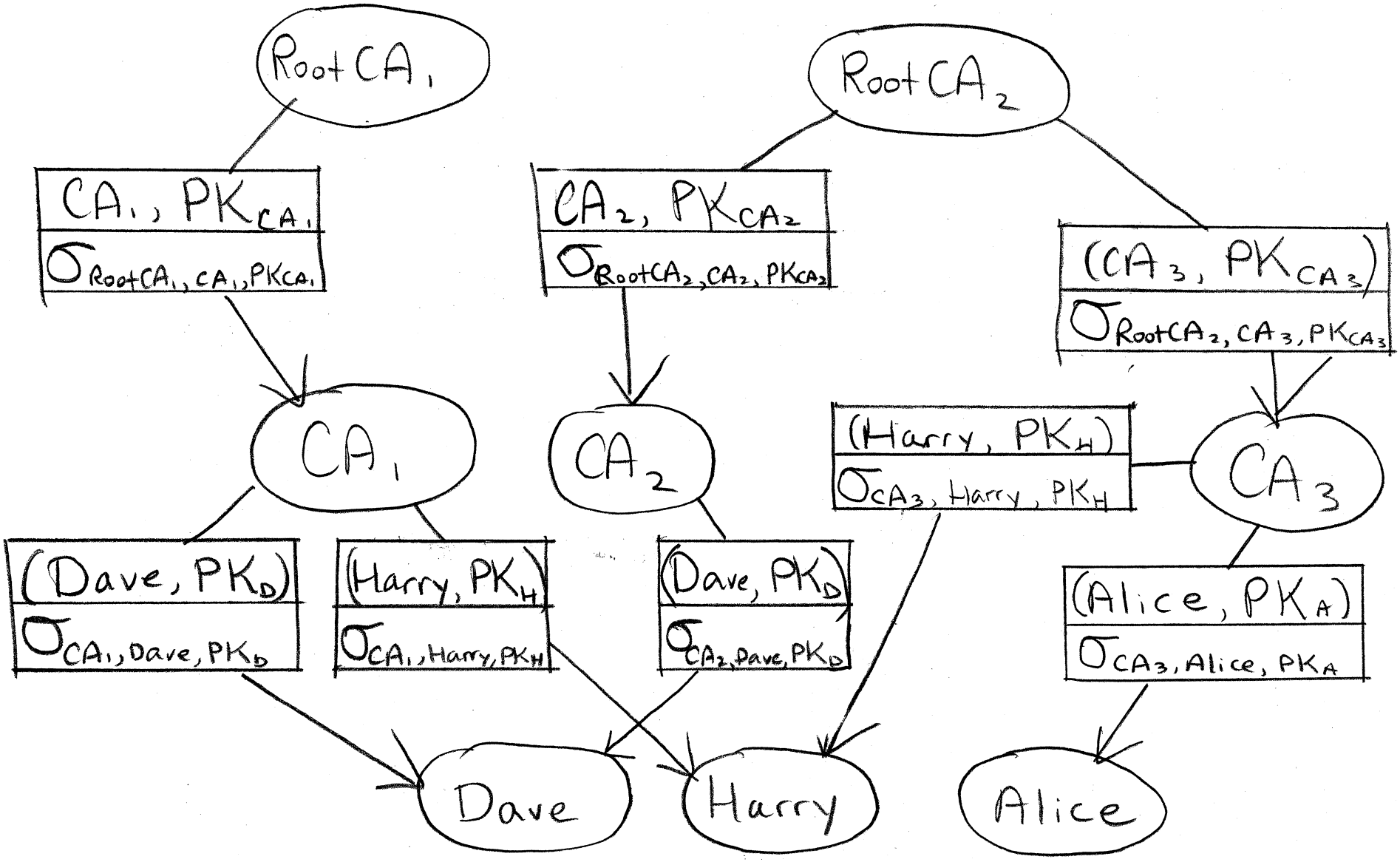

RootCA1
(CA1, PKCA1)
σRootCA1, CA1, PKCA1
CA1
(Alice, PKA)
σCA1, Alice, PKA
Alice
RootCA2
(CA4, PKCA4)
σRootCA2, CA4, PKCA4
CA4
(CA3, PKCA3)
σCA4, CA3, PKCA3
CA3
(Alice, PKA)
σCA3, Alice, PKA
(Dave, PKD)
σCA3, Dave, PKD
Dave
(CA2, PKCA2)
σRootCA2, CA2, PKCA2
CA2
(Harry, PKH)
σCA2, Harry, PKH
Harry
(Bob, PKB)
σCA2, Bob, PKB
Bob

Figure 3


Root CA1
Root CA2
CA1, PKCA1
σRootCA1, CA1, PKCA1
CA2, PKCA2
σRootCA2, CA2, PKCA2
(CA3, PKCA3)
σRootCA2, CA3, PKCA3
CA1
CA2
(Harry, PKH)
σCA3, Harry, PKH
CA3
(Dave, PKD)
σCA1, Dave, PKD
(Harry, PKH)
σCA1, Harry, PKH
(Dave, PKD)
σCA2, Dave, PKD
(Alice, PKA)
σCA3, Alice, PKA
Dave
Harry
Alice