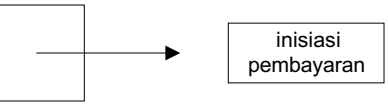
PROTOKOL CEK BILYET DIGITAL

Arrianto Mukti Wibowo
Fakultas Ilmu Komputer Universitas Indonesia
1997

Nasabah 1: Melakukan inisiasi

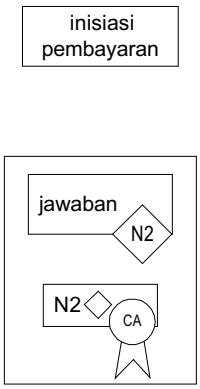
Komputer Nasabah 1

1. Nasabah 1 mengirimkan permohonan inisiasi pembayaran dengan cek digital

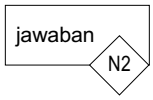


Nasabah 2: Mengirim sertifikat

Komputer Nasabah 2



2. Software nasabah 2 menerima inisiasi pembayaran



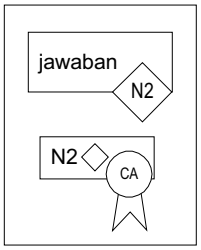
3. Software nasabah 2 membuat jawaban atas inisiasi pembayaran, serta menandatangani respons itu dengan membuat sidik jari dari jawaban dan mengenkripsinya dengan kunci privat nasabah 2

4. Software nasabah 2 mengirimkan jawaban disertai sertifikat nasabah 2.

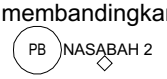
Nasabah 1: Meminta informasi rekening nasabah 2

Komputer Nasabah 1

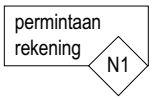
5. Software nasabah 1 menerima jawaban, dan mengotentikasi sertifikat dengan menelusurinya ke root.

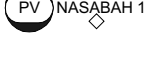


6. Software nasabah 1 mengotentikasi tanda tangan nasabah 2 dengan mendekripsi jawaban dengan kunci publik nasabah2, lalu membandingkannya dengan hash dari jawaban.

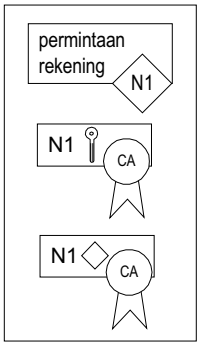


7. Software nasabah 1 membuat permintaan informasi rekening bank dari nasabah 2, serta menandatangani permintaan itu dengan membuat sidik jari dari permintaan dan mengenkripsinya dengan
kunci privat nasabah 1.

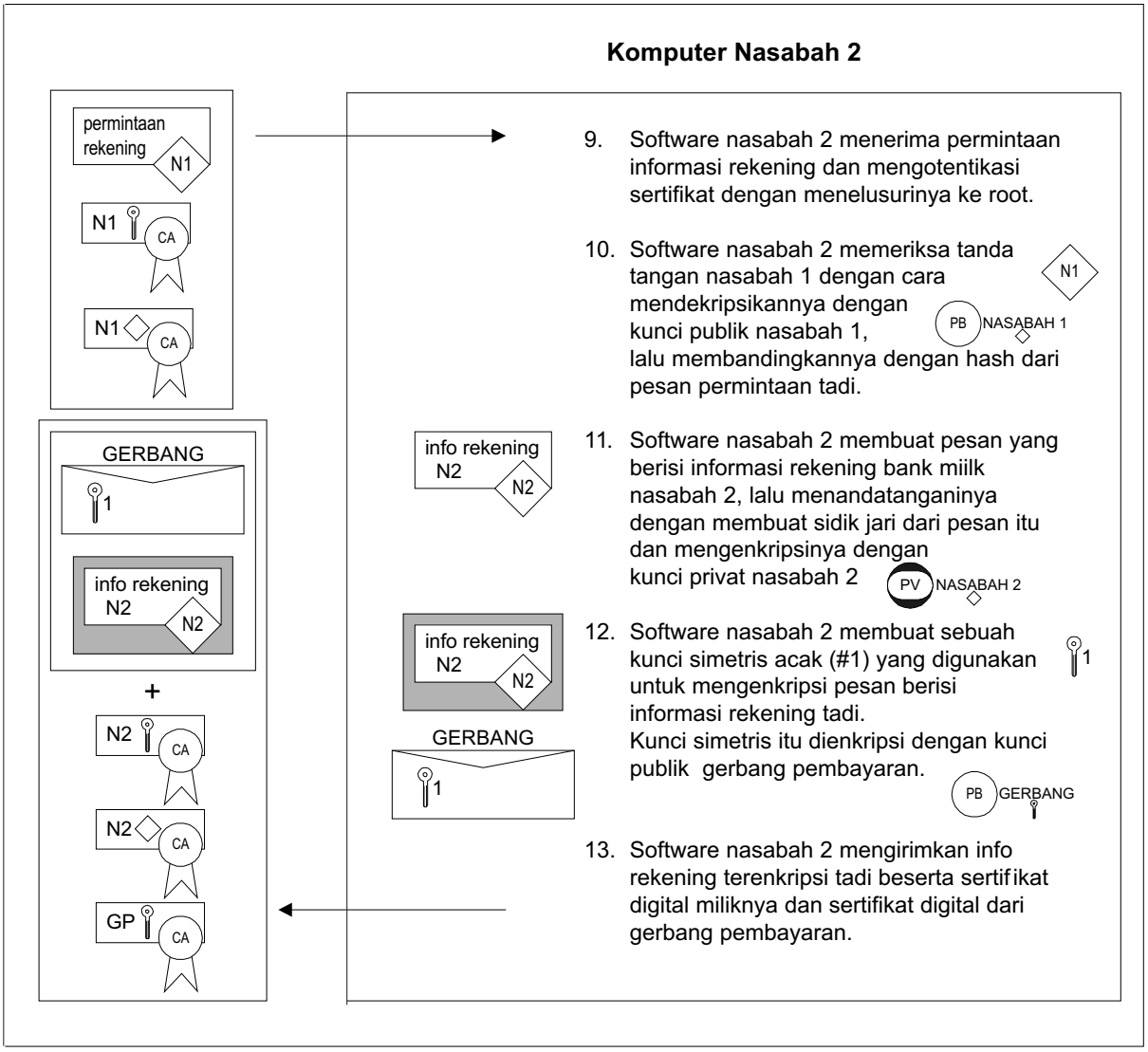




8. Software nasabah 1 mengirim permintaan informasi rekening disertai sertifikat nasabah 1.



Nasabah 2: Mengirim informasi rekening



Nasabah 1: Membuat cek digital

Komputer Nasabah 1

14. Software nasabah 1 mengotentikasi sertifikat-sertifikat yang diterimanya dengan menelusurinya ke root.

15. Software nasabah 1 menandatangani informasi rekening nasabah 1 dengan cara membuat sidik jari dari informasi itu dan mengenkripsinya dengan kunci privat nasabah 1. PV NASABAH 1

16. Software nasabah 1 membuat sebuah kunci simetris acak (#2), yang digunakan untuk mengenkripsi informasi rekening tadi. Setelah itu, kunci simetris tadi dienkripsi dengan kunci publik gerbang pembayaran. PB GERBANG

17. Software nasabah 1 membuat sebuah perintah pembayaran untuk banknya dari nasabah 1 kepada nasabah 2.

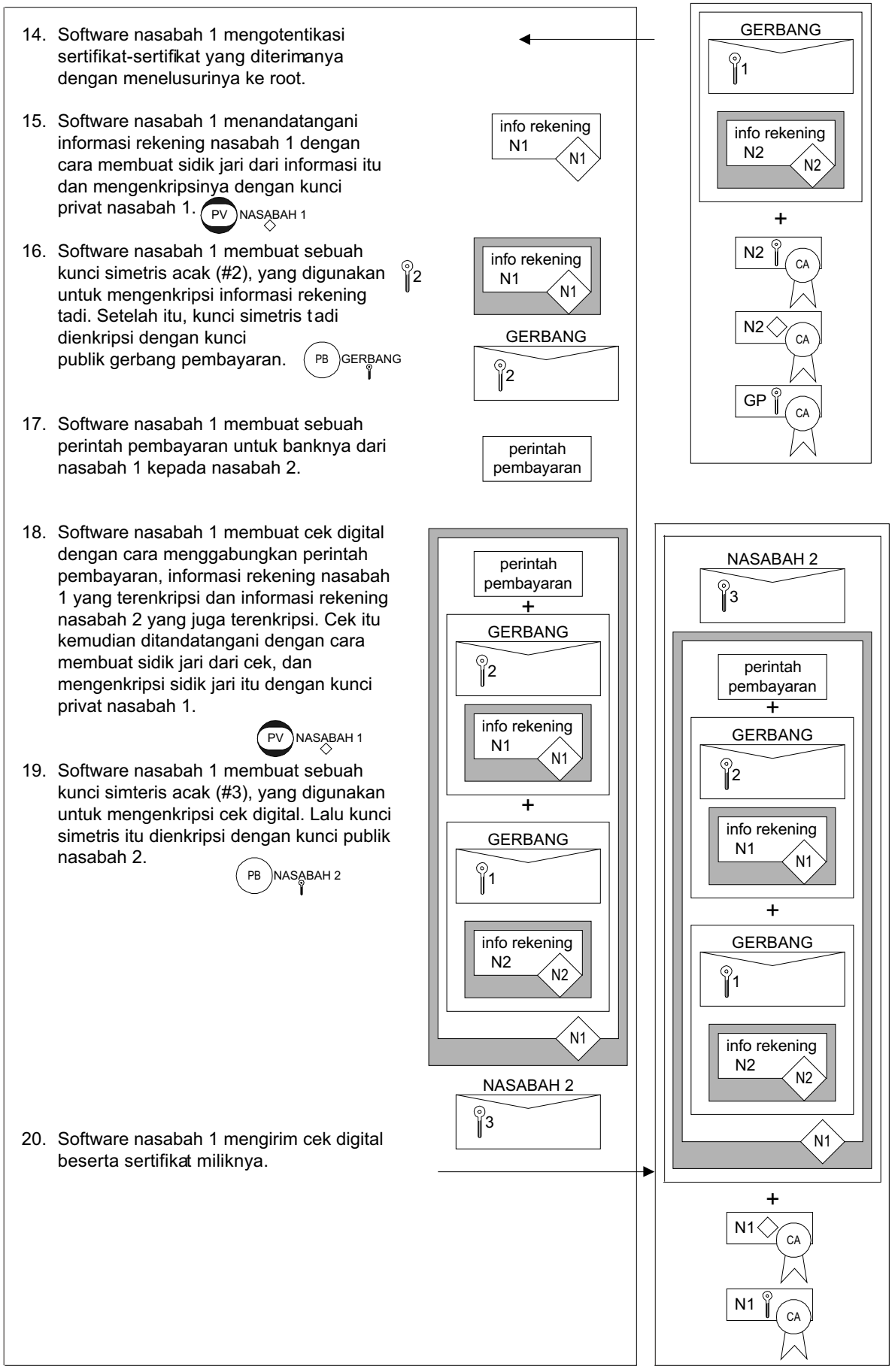
18. Software nasabah 1 membuat cek digital dengan cara menggabungkan perintah pembayaran, informasi rekening nasabah 1 yang terenkripsi dan informasi rekening nasabah 2 yang juga terenkripsi. Cek itu kemudian ditandatangani dengan cara membuat sidik jari dari cek, dan mengenkripsi sidik jari itu dengan kunci privat nasabah 1.

PV NASABAH 1

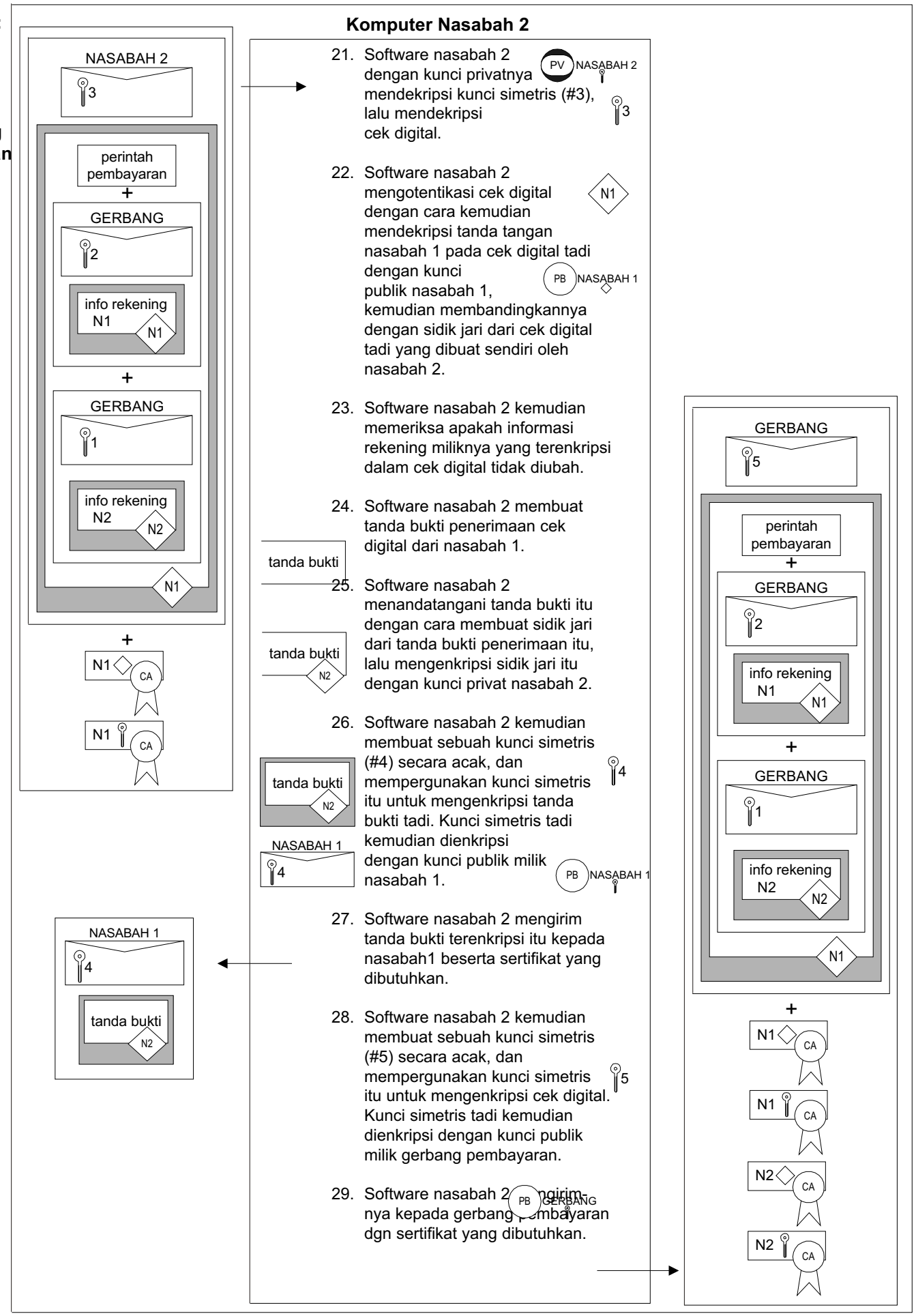
19. Software nasabah 1 membuat sebuah kunci simteris acak (#3), yang digunakan untuk mengenkripsi cek digital. Lalu kunci simetris itu dienkripsi dengan kunci publik nasabah 2.

PB NASABAH 2

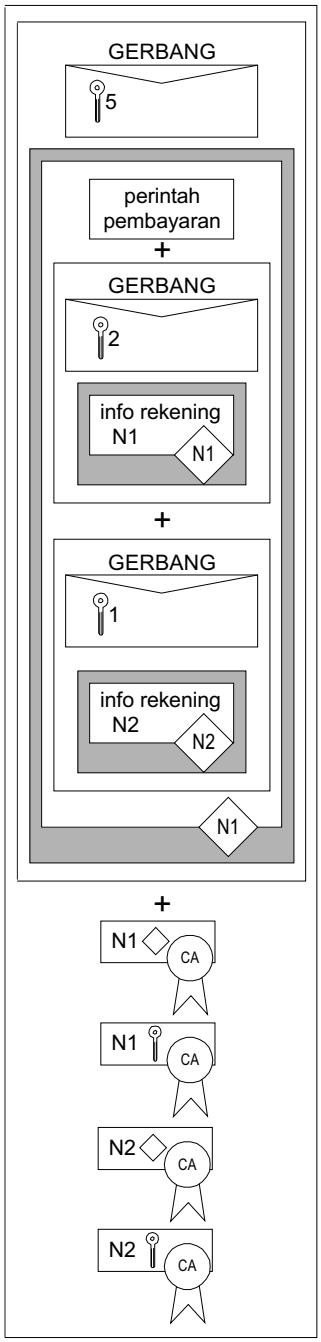
20. Software nasabah 1 mengirim cek digital beserta sertifikat miliknya.



Nasabah 2: Memeriksa cek digital dan mengirimnya ke gerbang pembayaran

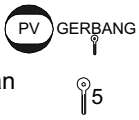


Gerbang pembayaran: Memeriksa cek, mengirimkan nya ke rumah kliring. Jika jaringan antar bank tersedia, maka sekaligus mendebit rekening nasabah 1 dan mengkredit rekening nasabah 2.

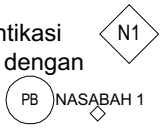


Gerbang pembayaran

33. Software gerbang pembayaran dengan kunci privatnya mendekripsi kunci simetris (#5). Kunci simetris itu dipergunakan untuk mendekripsi cek digital yang masih terenkripsi.

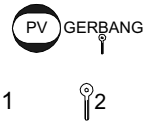


34. Software gerbang pembayaran mengotentikasi tanda tangan nasabah 1 pada cek digital dengan cara mendekripsikannya dengan kunci publik nasabah 1, lalu membandingkannya dengan sidik jari cek digital yang dibuat sendiri oleh gerbang pembayaran.

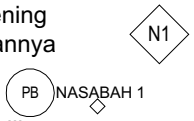


35. Software gerbang pembayaran mengekstrak informasi cek (identifier, waktu, nilai, mata uang) dari perintah pembayaran.

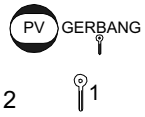
36. Software gerbang pembayaran dengan kunci privatnya mendekripsi kunci simetris (#2). Kunci simetris itu dipergunakan untuk mendekripsi informasi rekening nasabah 1 (pemberi cek) yang masih terenkripsi.



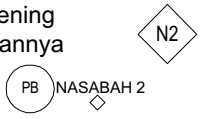
37. Software gerbang pembayaran mengotentikasi tanda tangan nasabah 1 pada info rekening nasabah 1 dengan cara mendekripsikannya dengan kunci publik nasabah 1, lalu membandingkannya dengan sidik jari info rekening nasabah 1 yang dibuat sendiri oleh gerbang pembayaran.



38. Software gerbang pembayaran dengan kunci privatnya mendekripsi kunci simetris (#1). Kunci simetris itu dipergunakan untuk mendekripsi informasi rekening nasabah 2 (penerima cek) yang masih terenkripsi.

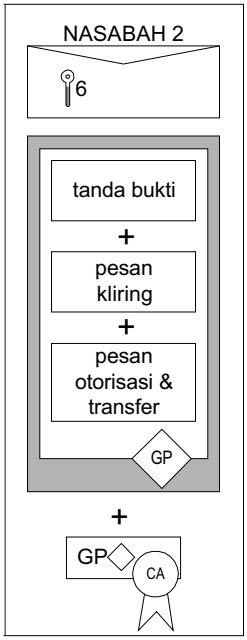


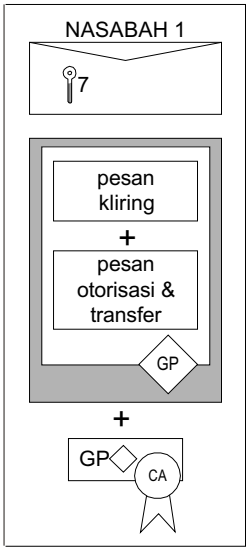
39. Software gerbang pembayaran mengotentikasi tanda tangan nasabah 2 pada info rekening nasabah 2 dengan cara mendekripsikannya dengan kunci publik nasabah 2, lalu membandingkannya dengan sidik jari info rekening nasabah 2 yang dibuat sendiri oleh gerbang pembayaran.

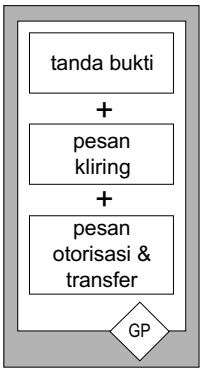


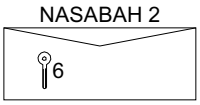
40. Software payment mengirimkan informasi cek lengkap, termasuk informasi rekening nasabah 1 (pemberi cek) dan nasabah 2 (penerima cek) kepada rumah kliring (*clearing house*). Jika jaringan antar bank memungkinkan, gerbang pembayaran segera melakukan otorisasi dan transfer. Ini dilakukan dengan cara menginstruksikan bank nasabah 1 agar mendebit rekening bank milik nasabah 1, dan menginstruksikan kepada bank nasabah 2 untuk mengkredit rekening bank nasabah 2. Semua ini dilakukan di jaringan privat perbankan.

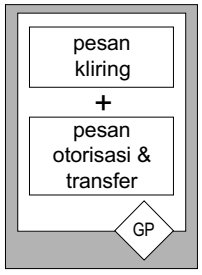
- bersambung ke halaman berikutnya -

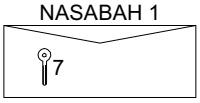


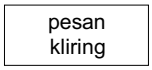


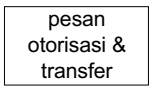












41. Software gerbang pembayaran membuat tanda bukti bahwa payment gateway sudah menerima cek digital dari nasabah 2.

42. Software gerbang pembayaran membuat pesan bahwa message telah dikirim dan diterima oleh rumah kliring. Proses kliring sendiri bisa memakan waktu 1 hari.

43. Jika jaringan antar bank tersedia, software gerbang pembayaran juga membuat pesan yang berisi hasil otorisasi dan transfer.

44. Software gerbang pembayaran menggabungkan tanda bukti penerimaan cek, pesan pengiriman ke rumah kliring dan pesan hasil otorisasi & transfer, kemudian menandatanganinya dengan cara membuat sidik jari dari pesan gabungan tadi, serta mengenkripsi sidik jari itu dengan kunci privat gerbang pembayaran.

45. Software gerbang pembayaran membuat kunci simetris (#6) secara acak, dan menggunakannya untuk mengenkripsi pesan gabungan tadi. Kunci simetris tadi kemudian dienkripsi dengan kunci publik dari nasabah 2.

46. Software gerbang pembayaran mengirim pesan gabungan yang terenkripsi itu kepada nasabah 2, beserta sertifikat yang diperlukan.

47. Software gerbang pembayaran menggabungkan pesan pengiriman ke rumah kliring dengan pesan hasil otorisasi & transfer, kemudian menandatanganinya dengan cara membuat sidik jari dari pesan gabungan tadi, serta mengenkripsi sidik jari itu dengan kunci privat gerbang pembayaran.

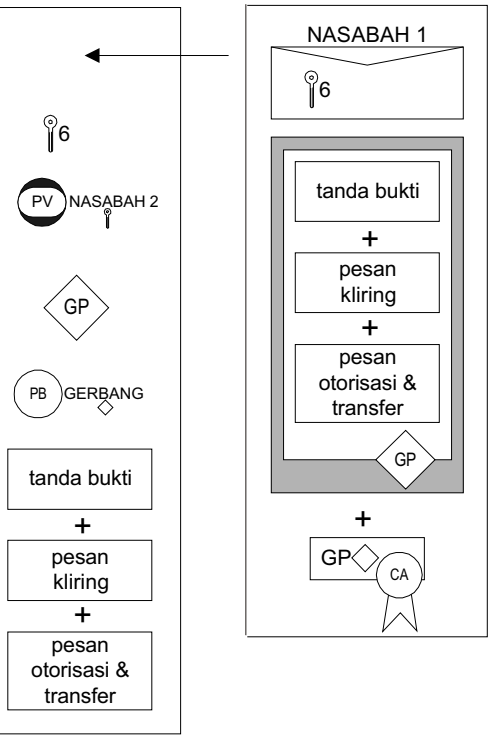
48. Software gerbang pembayaran membuat kunci simetris (#7) secara acak, dan menggunakannya untuk mengenkripsi pesan gabungan tadi. Kunci simetris tadi kemudian dienkripsi dengan kunci publik dari nasabah 1.

49. Software gerbang pembayaran mengirim pesan gabungan yang terenkripsi itu kepada nasabah 1, beserta sertifikat yang diperlukan.

Nasabah 2: Menerima pesan kliring dan pesan otorisasi & transfer

Komputer Nasabah 2

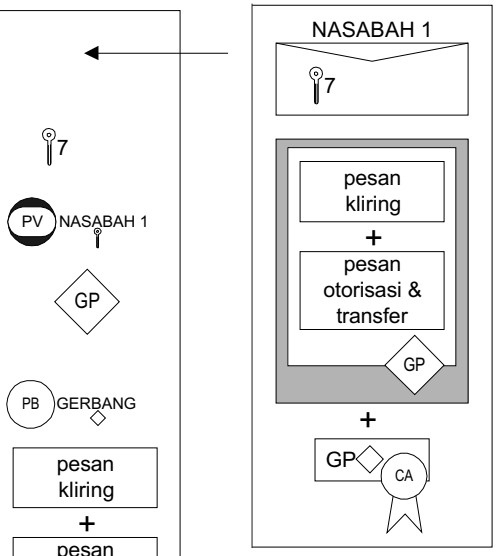
50. Software nasabah 2 mengotentikasi sertifikat digital yang diterimanya.
51. Software nasabah 2 mendekripsi kunci simetris (#6) dengan menggunakan kunci privat miliknya, lalu menggunakan kunci simetris itu untuk mendekripsi pesan-pesan dari gerbang pembayaran.
52. Software nasabah 2 mengotentikasi tanda tangan gerbang pembayaran pada pesan-pesan itu dengan cara mendekripsikannya dengan kunci publik gerbang pembayaran, lalu membandingkannya dengan sidik jari dari pesan-pesan itu yang dibuat sendiri oleh nasabah 2.
53. Nasabah 2 menerima status pembayaran cek digital.



Nasabah 1: Menerima pesan kliring dan pesan otorisasi & transfer

Komputer Nasabah 1

54. Software nasabah 1 mengotentikasi sertifikat digital yang diterimanya.
55. Software nasabah 1 mendekripsi kunci simetris (#7) dengan menggunakan kunci privat miliknya, lalu menggunakan kunci simetris itu untuk mendekripsi pesan-pesan dari gerbang pembayaran.
56. Software nasabah 1 mengotentikasi tanda tangan gerbang pembayaran pada pesan-pesan itu dengan cara mendekripsikannya dengan kunci publik gerbang pembayaran, lalu membandingkannya dengan sidik jari dari pesan-pesan itu yang dibuat sendiri oleh nasabah 1.
57. Nasabah 1 menerima status pembayaran cek digital.



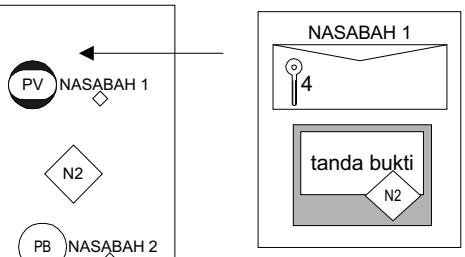
Nasabah 1: Menerima tanda bukti penerimaan cek

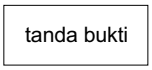
Komputer Nasabah 1

30. Software nasabah 1 mendekripsi kunci simetris (#4) dengan kunci privat miliknya, lalu dengan kunci simetris itu mendekripsi tanda bukti dari nasabah 2.

31. Software nasabah 1 mengotentikasi tanda tangan nasabah 2 pada tanda bukti dengan cara mendekripsikannya dengan kunci publik nasabah 2, lalu membandingkannya dengan sidik jari dari tanda bukti yang dibuat sendiri oleh nasabah 1.

32. Nasabah 1 menerima dan mencatat tanda bukti konfirmasi penerimaan cek digital dari nasabah 1 oleh nasabah 2.





amwibowo@excite.com
amwibowo@caplin.cs.ui.ac.id