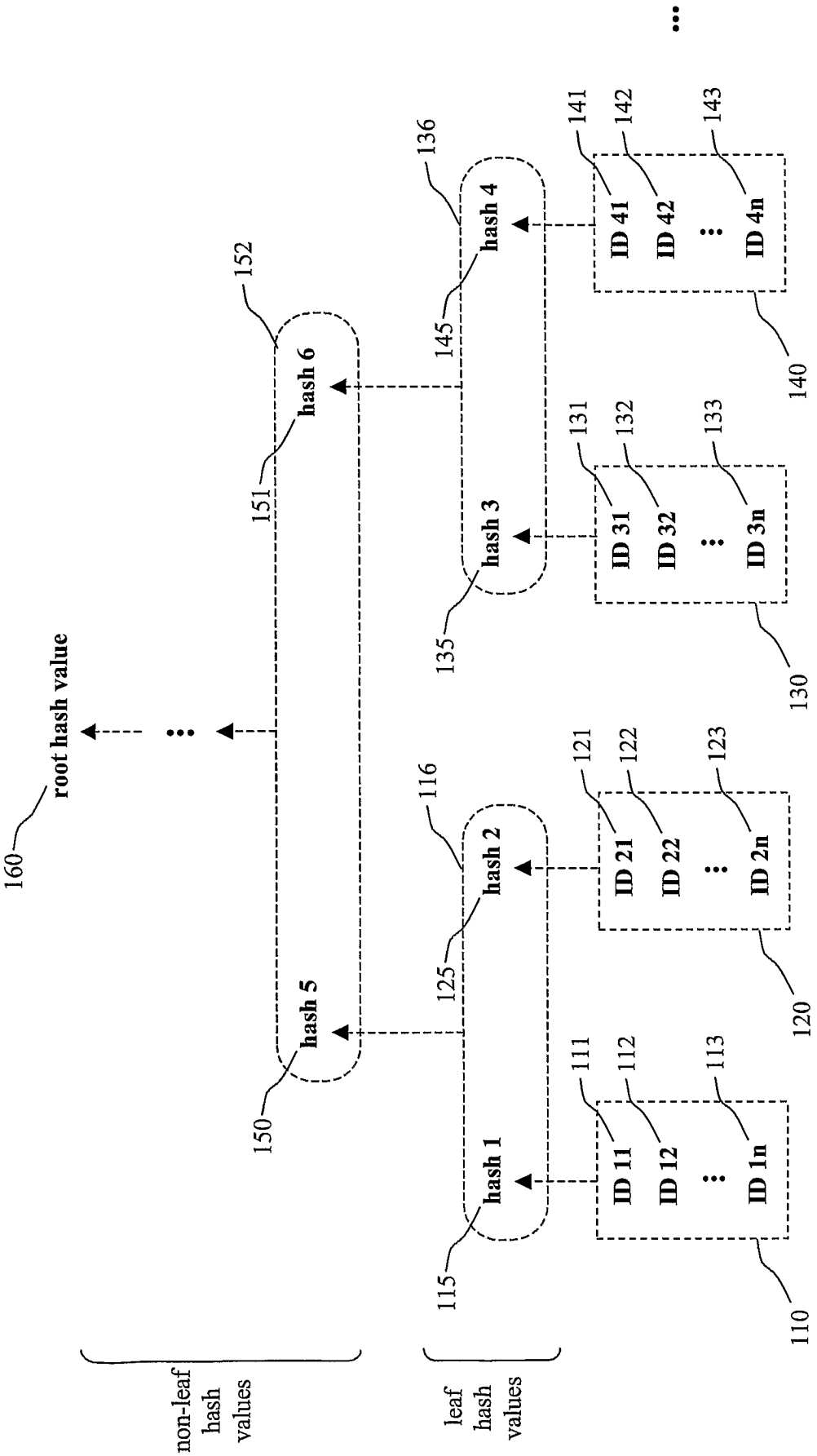

root hash value
160
hash 6
151
152
hash 5
150
hash 4
145
136
hash 3
135
hash 2
125
116
hash 1
115
ID 41
ID 42
ID 4n
141
142
143
140
ID 31
ID 32
ID 3n
131
132
133
130
ID 21
ID 22
ID 2n
121
122
123
120
ID 11
ID 12
ID 1n
111
112
113
110
non-leaf hash values
leaf hash values

Fig. 1

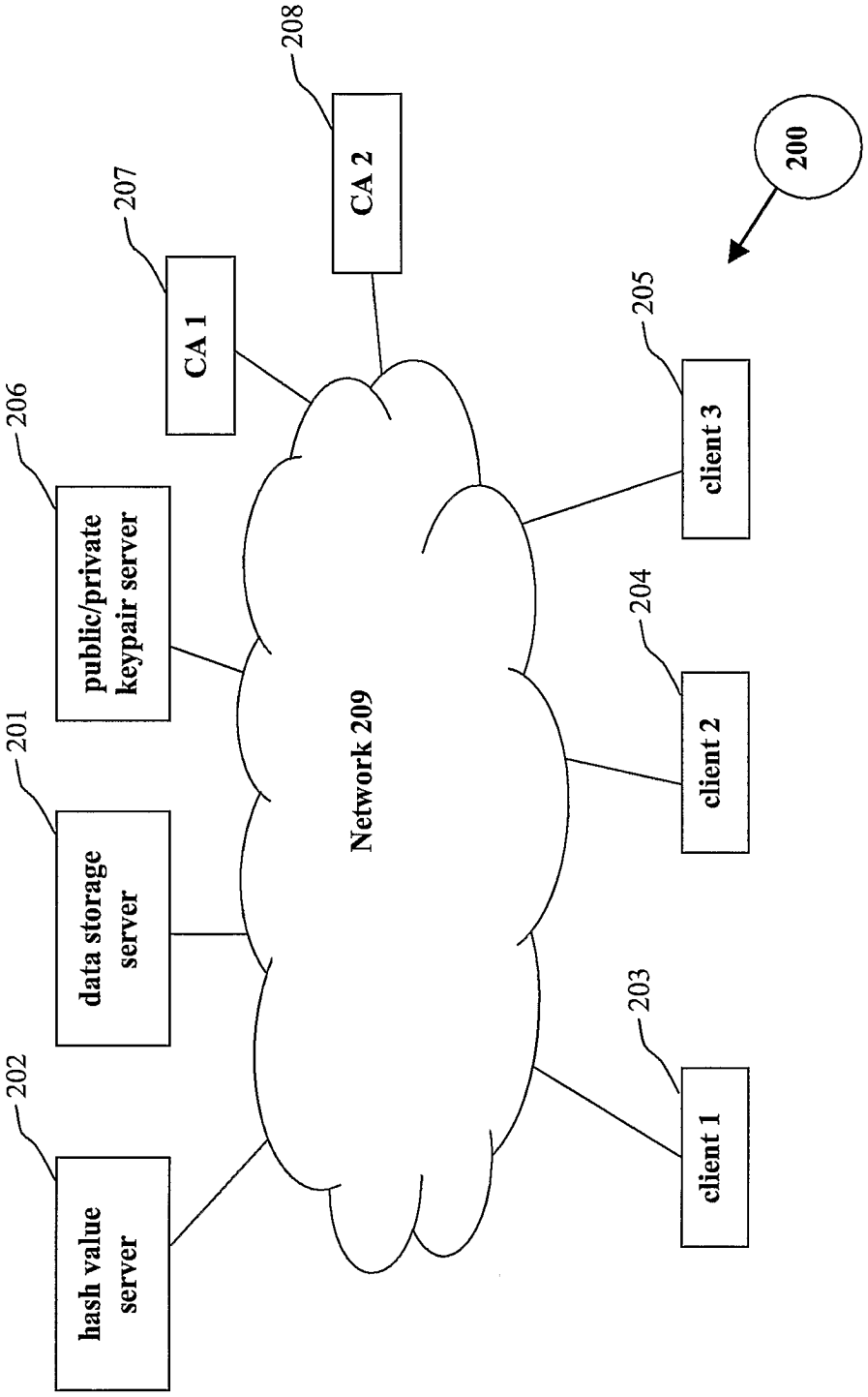

200
208
CA 2
207
CA 1
206
public/private keypair server
201
data storage server
202
hash value server
Network 209
205
client 3
204
client 2
203
client 1

Fig. 2

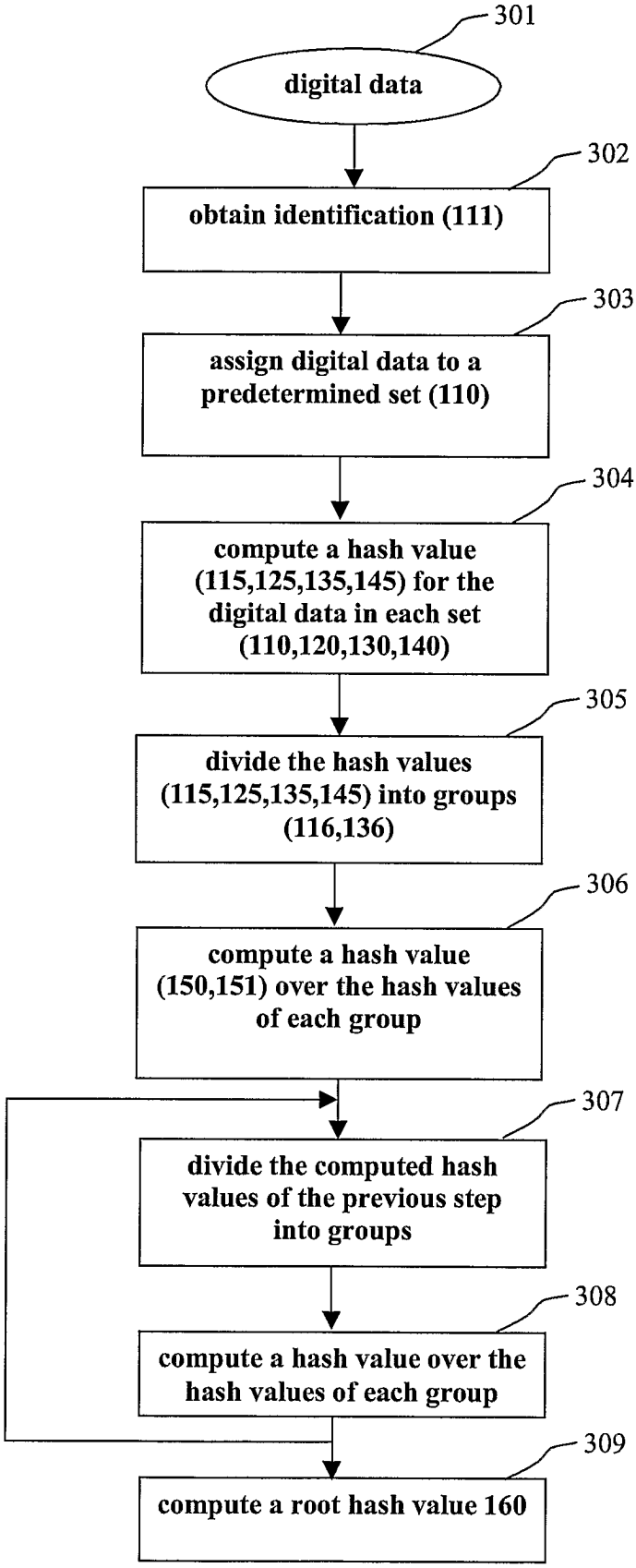

301
digital data
302
obtain identification (111)
303
assign digital data to a predetermined set (110)
304
compute a hash value (115,125,135,145) for the digital data in each set (110,120,130,140)
305
divide the hash values (115,125,135,145) into groups (116,136)
306
compute a hash value (150,151) over the hash values of each group
307
divide the computed hash values of the previous step into groups
308
compute a hash value over the hash values of each group
309
compute a root hash value 160

Fig. 3

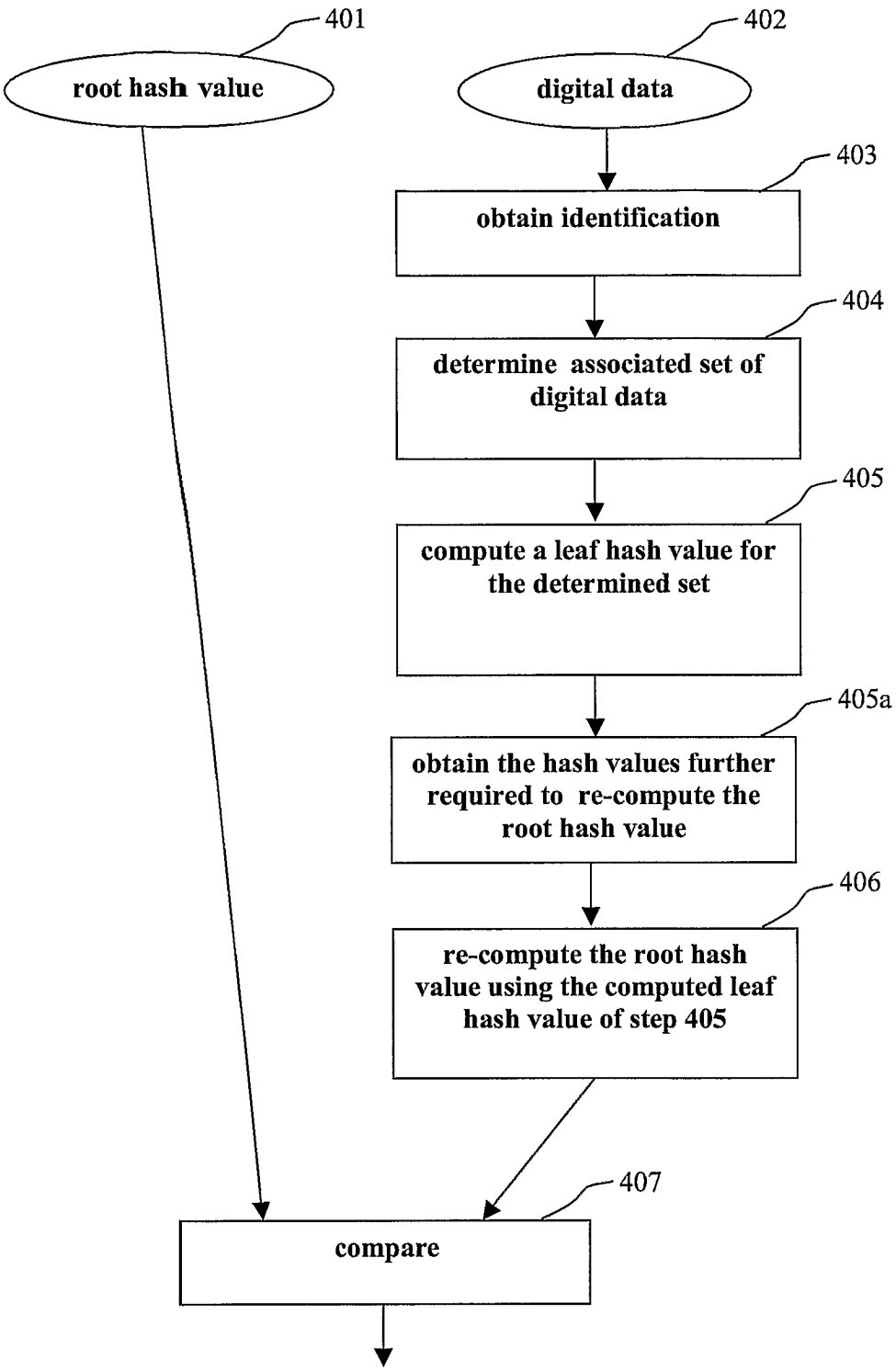

401
root hash value
402
digital data
403
obtain identification
404
determine associated set of digital data
405
compute a leaf hash value for the determined set
405a
obtain the hash values further required to re-compute the root hash value
406
re-compute the root hash value using the computed leaf hash value of step 405
407
compare

Fig. 4

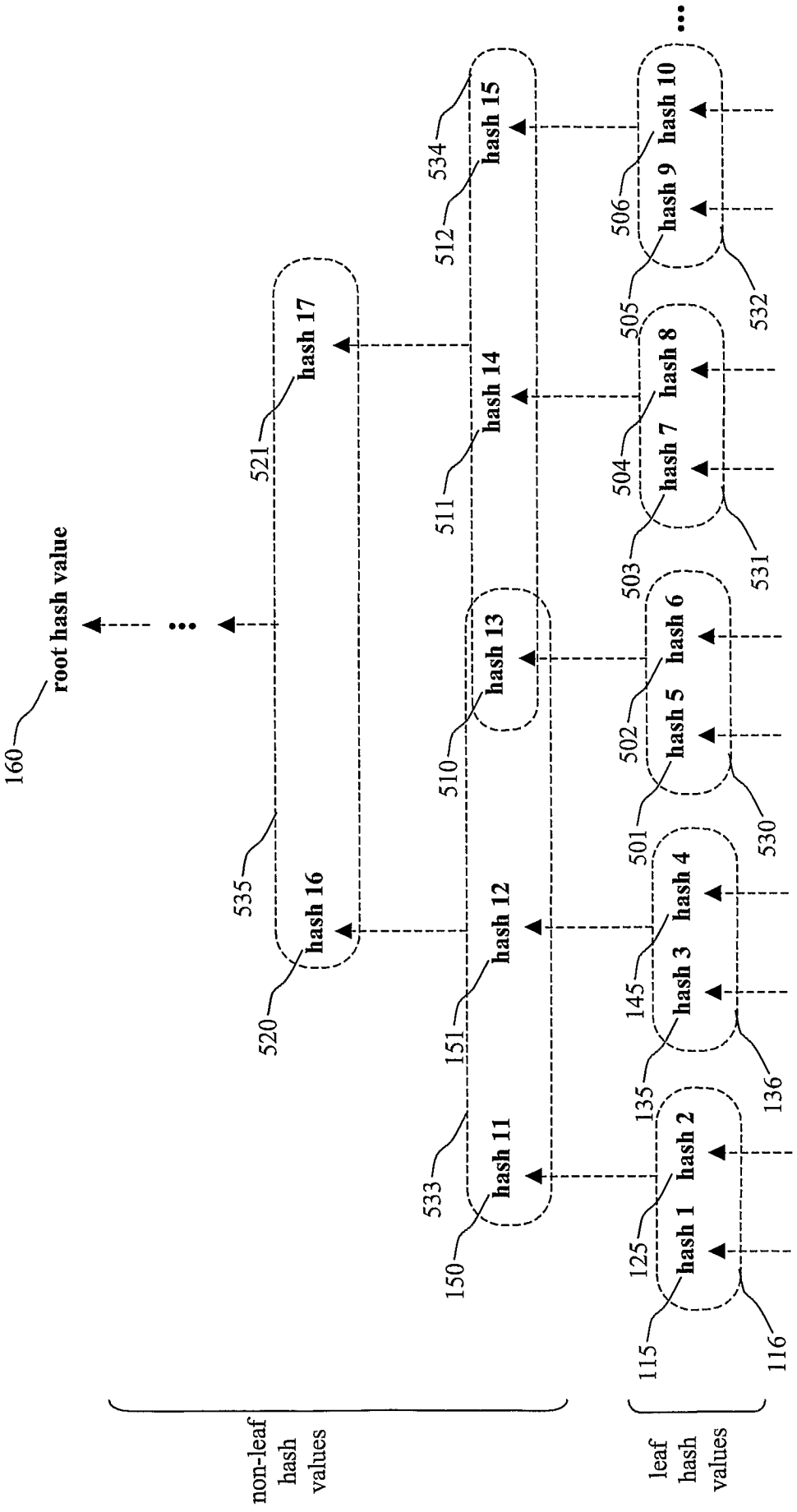

root hash value
160
hash 17
521
hash 16
520
535
hash 15
534
hash 14
511
hash 13
510
hash 12
151
hash 11
533
150
hash 10
506
hash 9
505
hash 8
504
hash 7
503
hash 6
502
hash 5
501
hash 4
145
hash 3
135
hash 2
125
hash 1
115
512
532
531
530
136
116
non-leaf hash values
leaf hash values

Fig. 5a

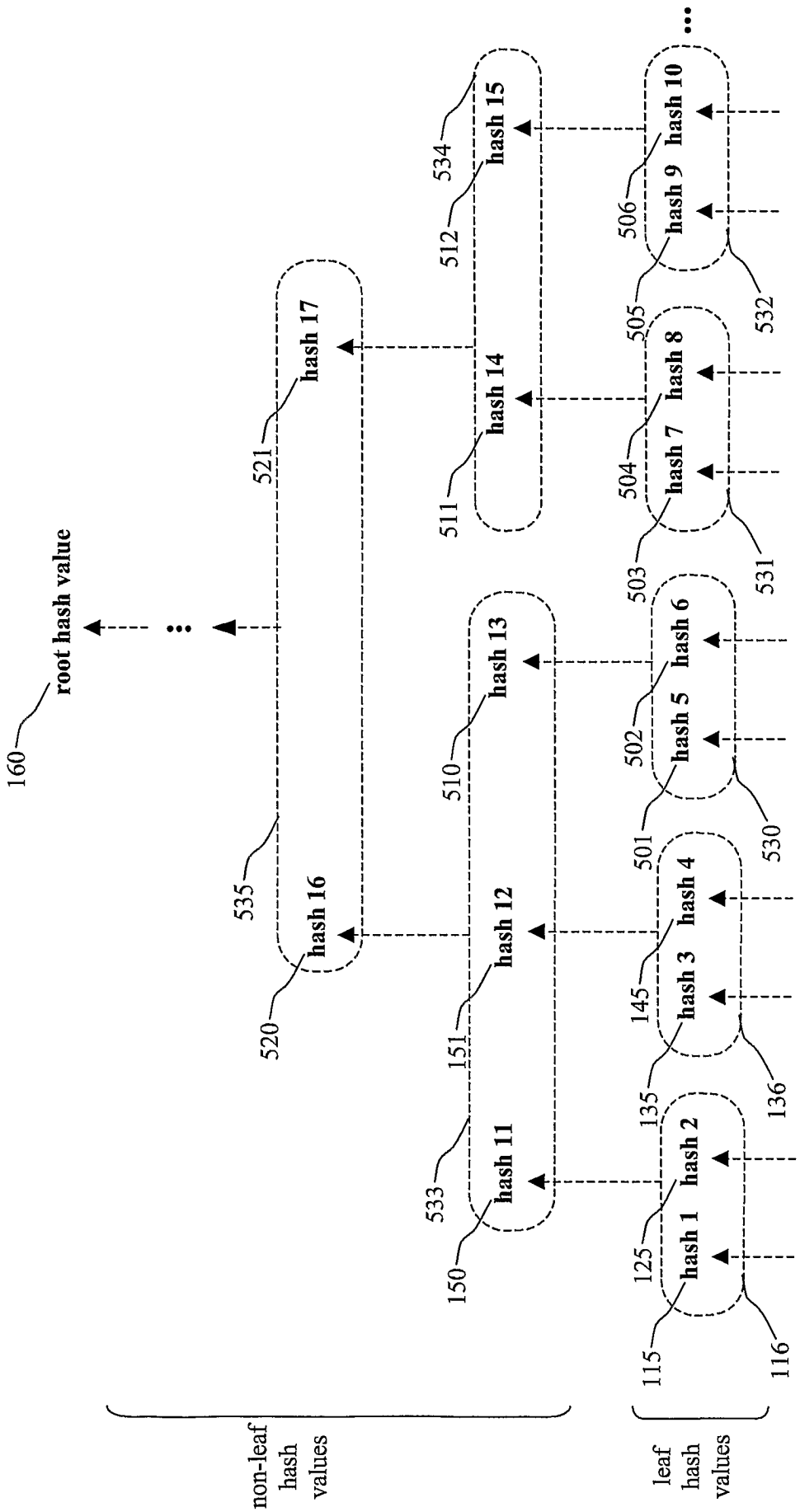

root hash value
160
hash 17
521
hash 16
520
535
hash 15
534
512
hash 14
511
hash 13
510
hash 12
151
hash 11
150
533
hash 10
506
hash 9
505
532
hash 8
504
hash 7
503
531
hash 6
502
hash 5
501
530
hash 4
145
hash 3
135
136
hash 2
125
hash 1
115
116
non-leaf hash values
leaf hash values

Fig. 5b

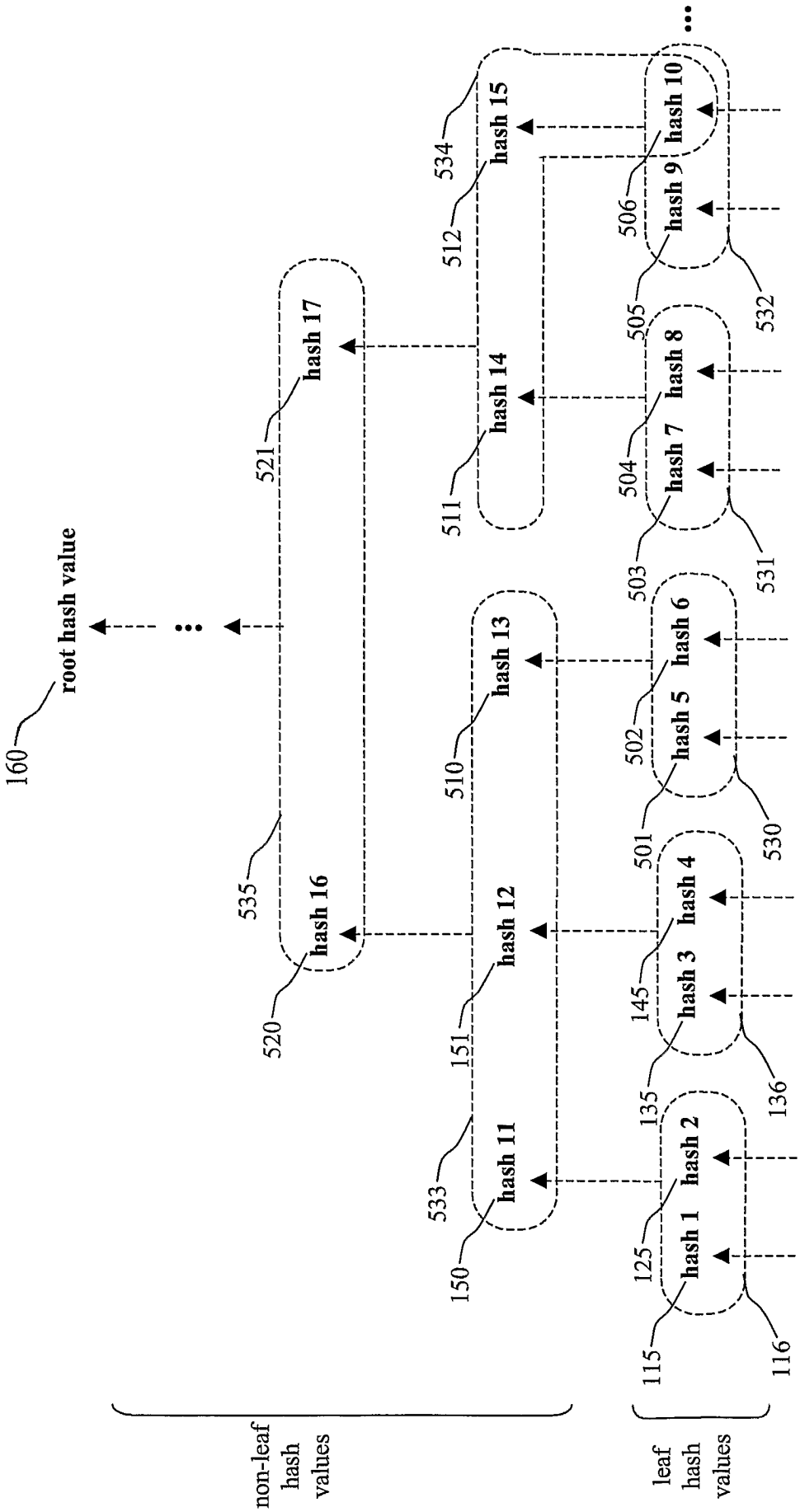

root hash value
160
hash 17
521
hash 16
520
hash 15
534
hash 14
511
hash 13
510
hash 12
151
hash 11
150
hash 10
506
hash 9
505
hash 8
504
hash 7
503
hash 6
502
hash 5
501
hash 4
145
hash 3
135
hash 2
125
hash 1
115
532
531
530
136
116
535
512
533
non-leaf hash values
leaf hash values

Fig. 5c

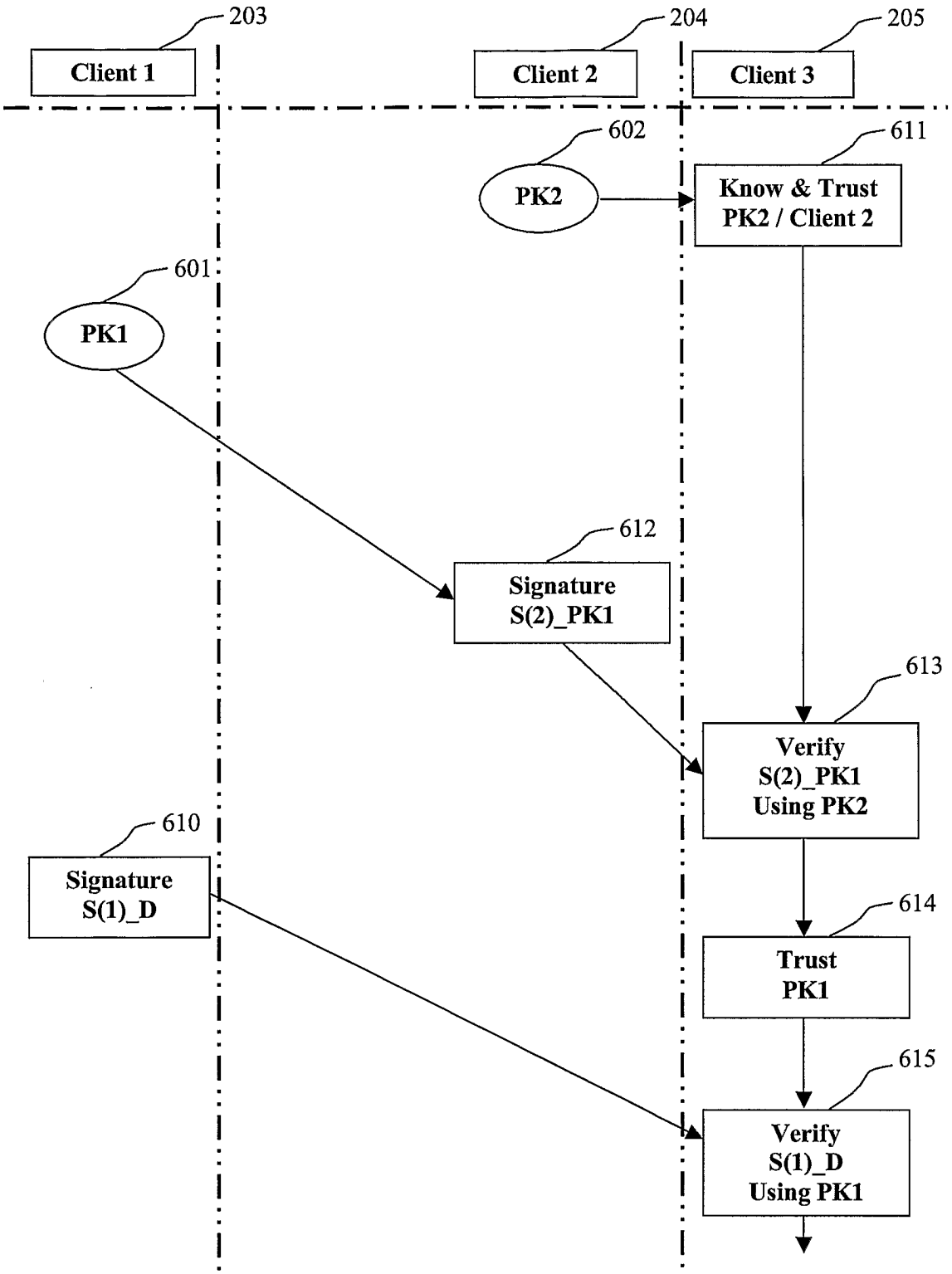

203
204
205
Client 1
Client 2
Client 3
602
611
PK2
Know & Trust
PK2 / Client 2
601
PK1
612
Signature
S(2)_PK1
613
Verify
S(2)_PK1
Using PK2
610
Signature
S(1)_D
614
Trust
PK1
615
Verify
S(1)_D
Using PK1

Fig. 6

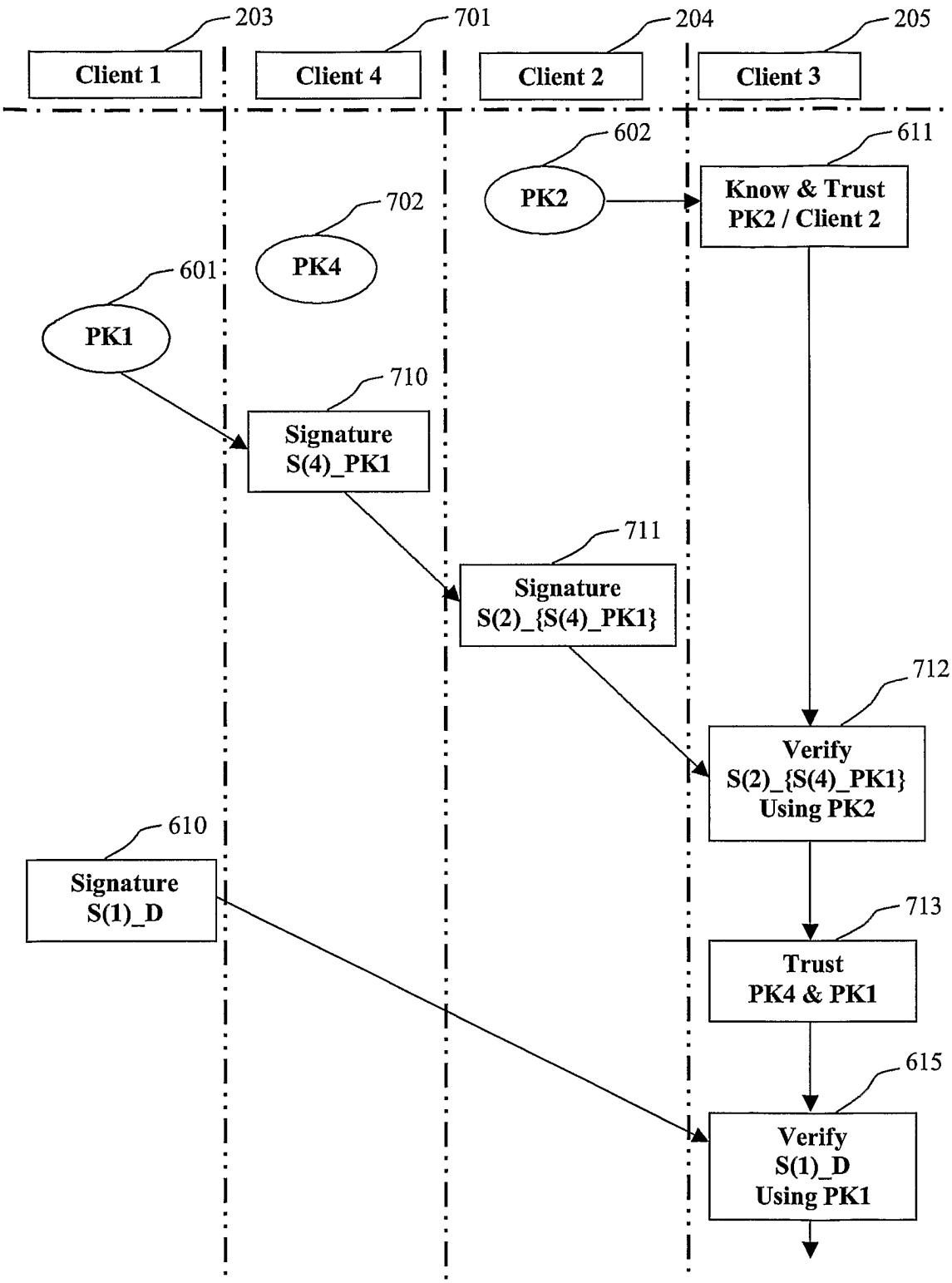

203
701
204
205
Client 1
Client 4
Client 2
Client 3
602
611
PK2
Know & Trust
PK2 / Client 2
702
PK4
601
PK1
710
Signature
S(4)_PK1
711
Signature
S(2)_{S(4)_PK1}
712
Verify
S(2)_{S(4)_PK1}
Using PK2
610
Signature
S(1)_D
713
Trust
PK4 & PK1
615
Verify
S(1)_D
Using PK1

Fig. 7

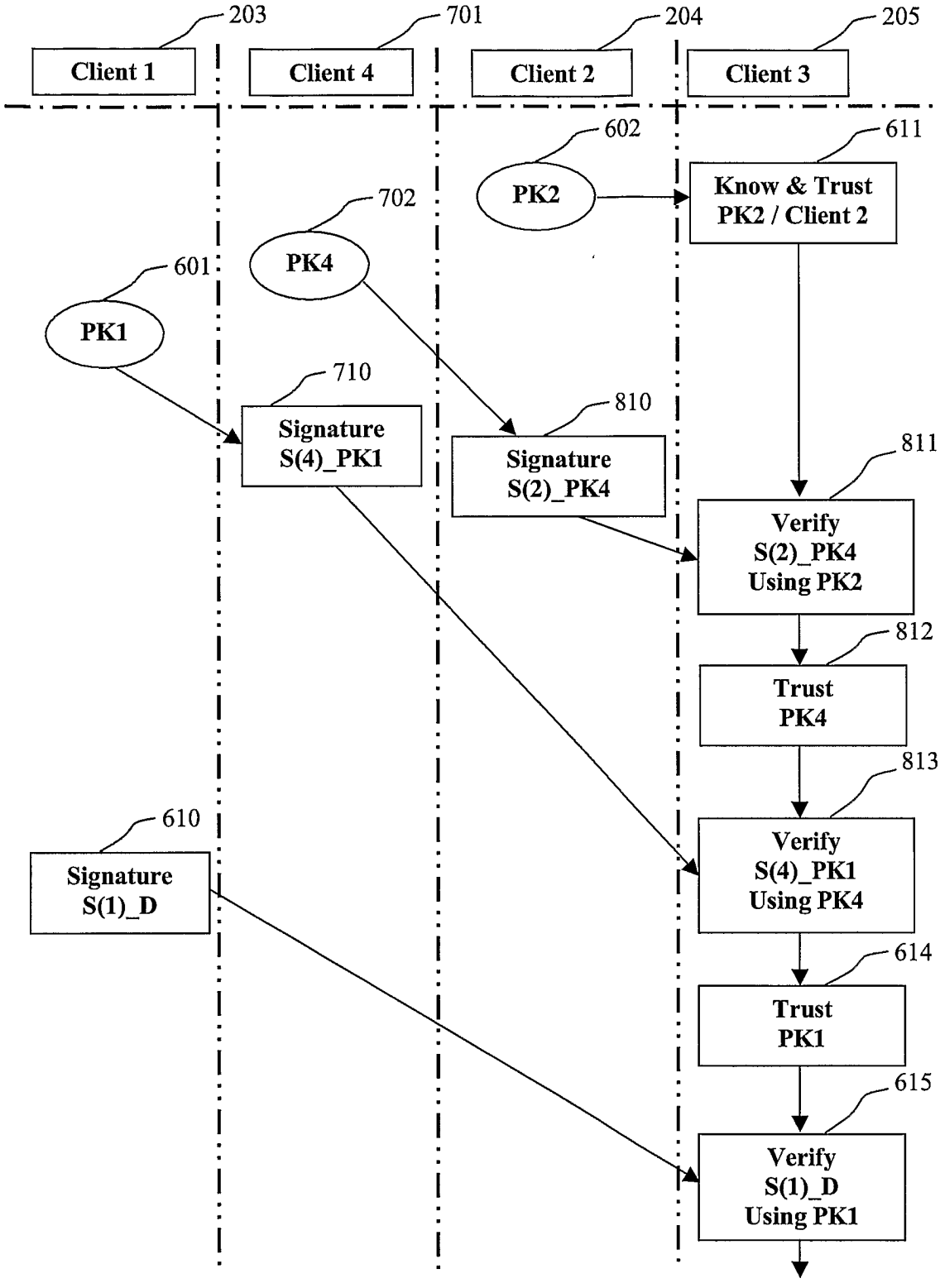

203
701
204
205
Client 1
Client 4
Client 2
Client 3
602
611
PK2
Know & Trust
PK2 / Client 2
702
PK4
601
PK1
710
Signature
S(4)_PK1
810
Signature
S(2)_PK4
811
Verify
S(2)_PK4
Using PK2
812
Trust
PK4
813
610
Signature
S(1)_D
Verify
S(4)_PK1
Using PK4
614
Trust
PK1
615
Verify
S(1)_D
Using PK1

Fig. 8