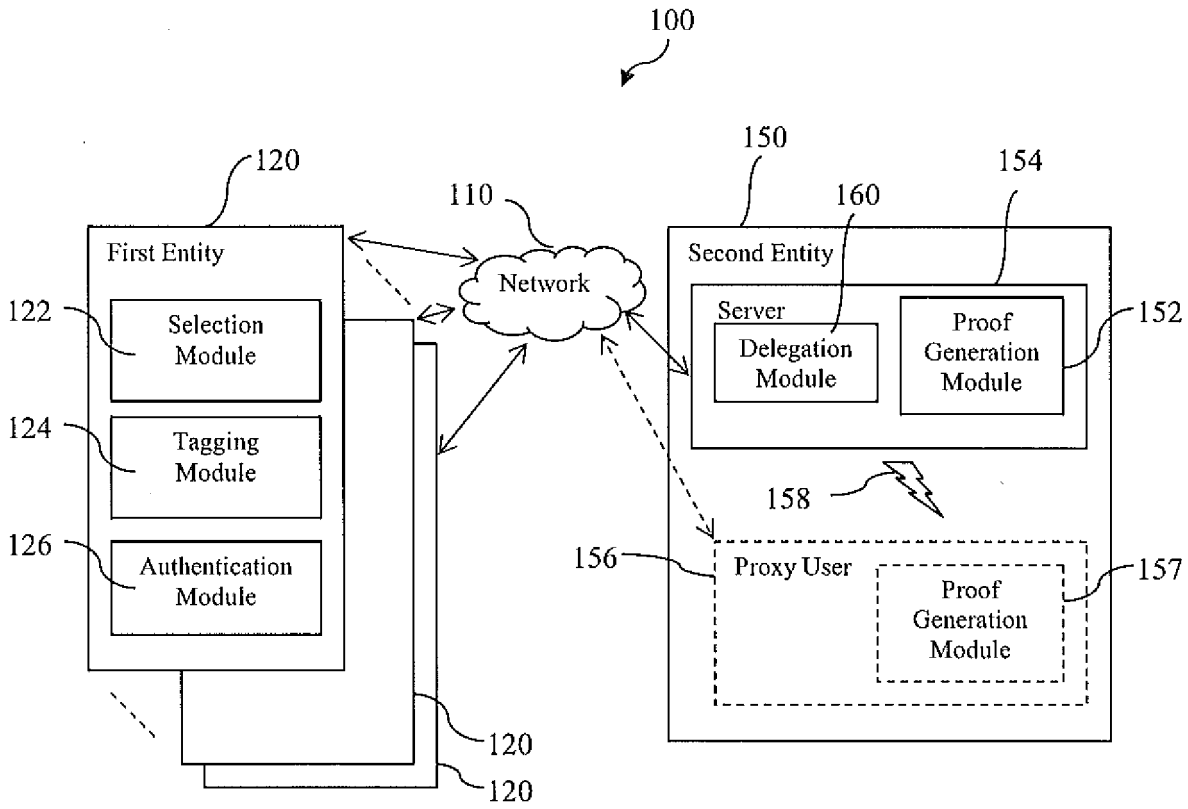

100
120
First Entity
122
Selection Module
124
Tagging Module
126
Authentication Module
110
Network
150
154
160
Second Entity
Server
Delegation Module
Proof Generation Module
152
158
156
Proxy User
Proof Generation Module
157
120
120

FIG. 1

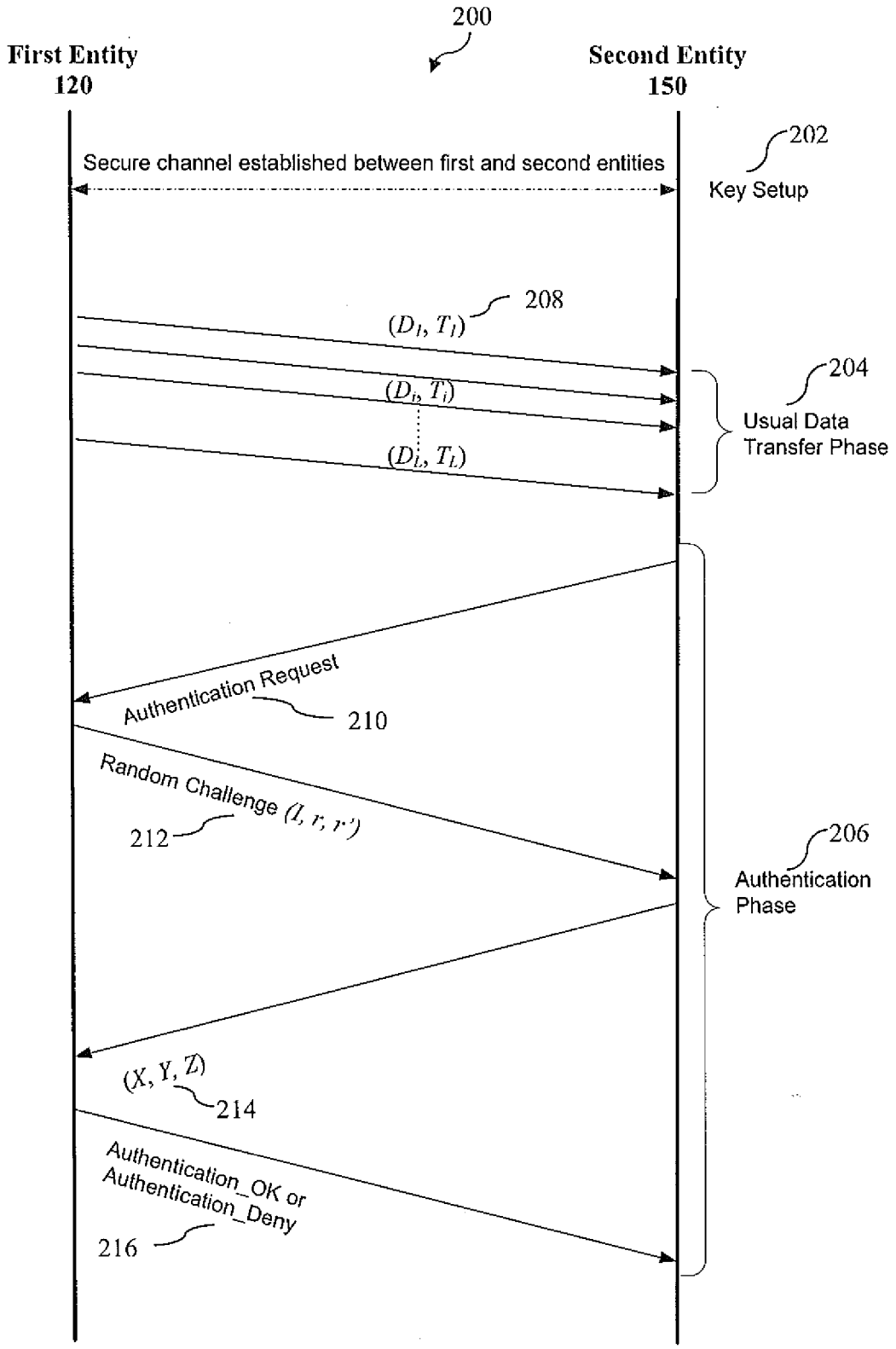

200
First Entity
120
Second Entity
150
Secure channel established between first and second entities
202
Key Setup
208
(D_1, T_1)
(D_i, T_i)
(D_L, T_L)
204
Usual Data
Transfer Phase
Authentication Request
210
Random Challenge (I, r, r')
212
206
Authentication
Phase
(X, Y, Z)
214
Authentication_OK or
Authentication_Deny
216

FIG. 2

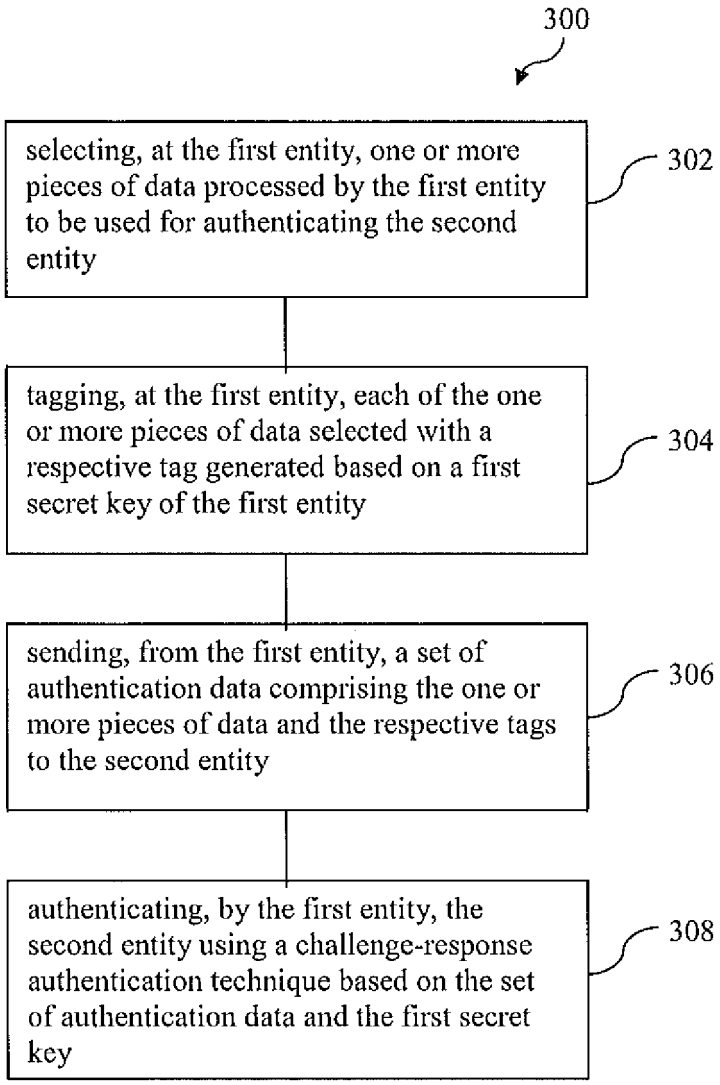

300
selecting, at the first entity, one or more pieces of data processed by the first entity to be used for authenticating the second entity
302
tagging, at the first entity, each of the one or more pieces of data selected with a respective tag generated based on a first secret key of the first entity
304
sending, from the first entity, a set of authentication data comprising the one or more pieces of data and the respective tags to the second entity
306
authenticating, by the first entity, the second entity using a challenge-response authentication technique based on the set of authentication data and the first secret key
308

FIG. 3

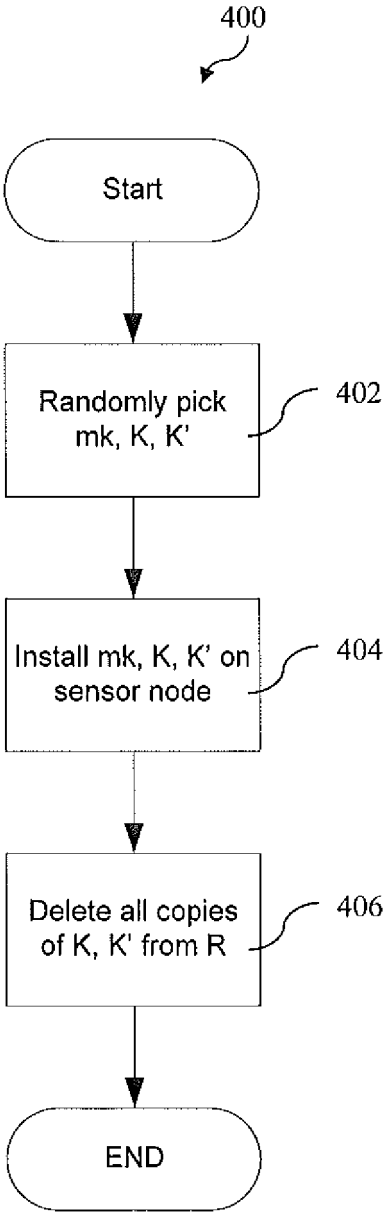

400
Start
Randomly pick mk, K, K'
402
Install mk, K, K' on sensor node
404
Delete all copies of K, K' from R
406
END

FIG. 4

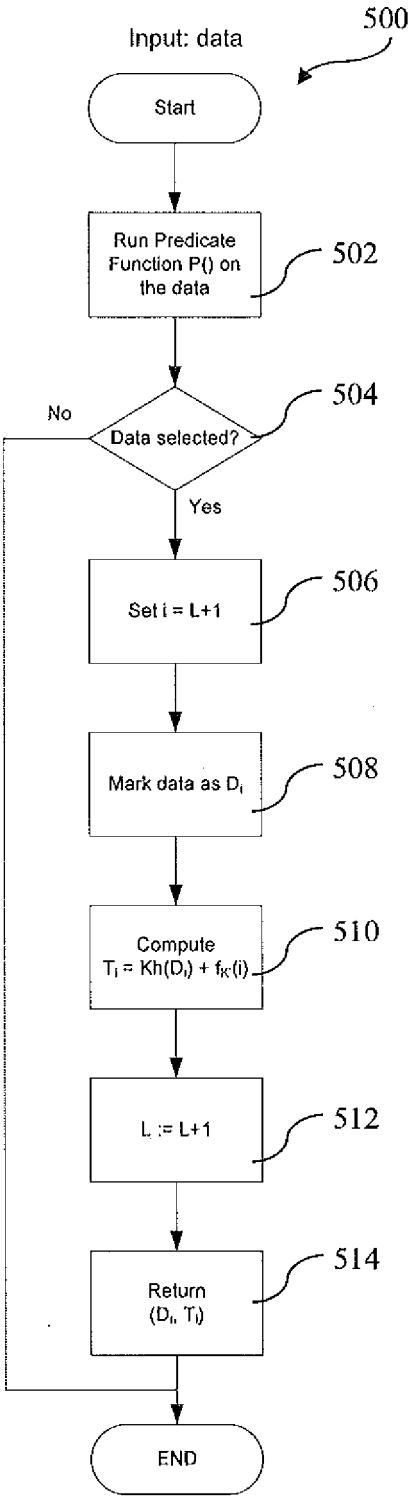

500
Input: data
Start
Run Predicate Function P() on the data
502
No
Data selected?
504
Yes
Set i = L+1
506
Mark data as D_i
508
Compute $T_i = Kh(D_i) + f_K(i)$
510
L := L+1
512
Return (D_i, T_i)
514
END

FIG. 5

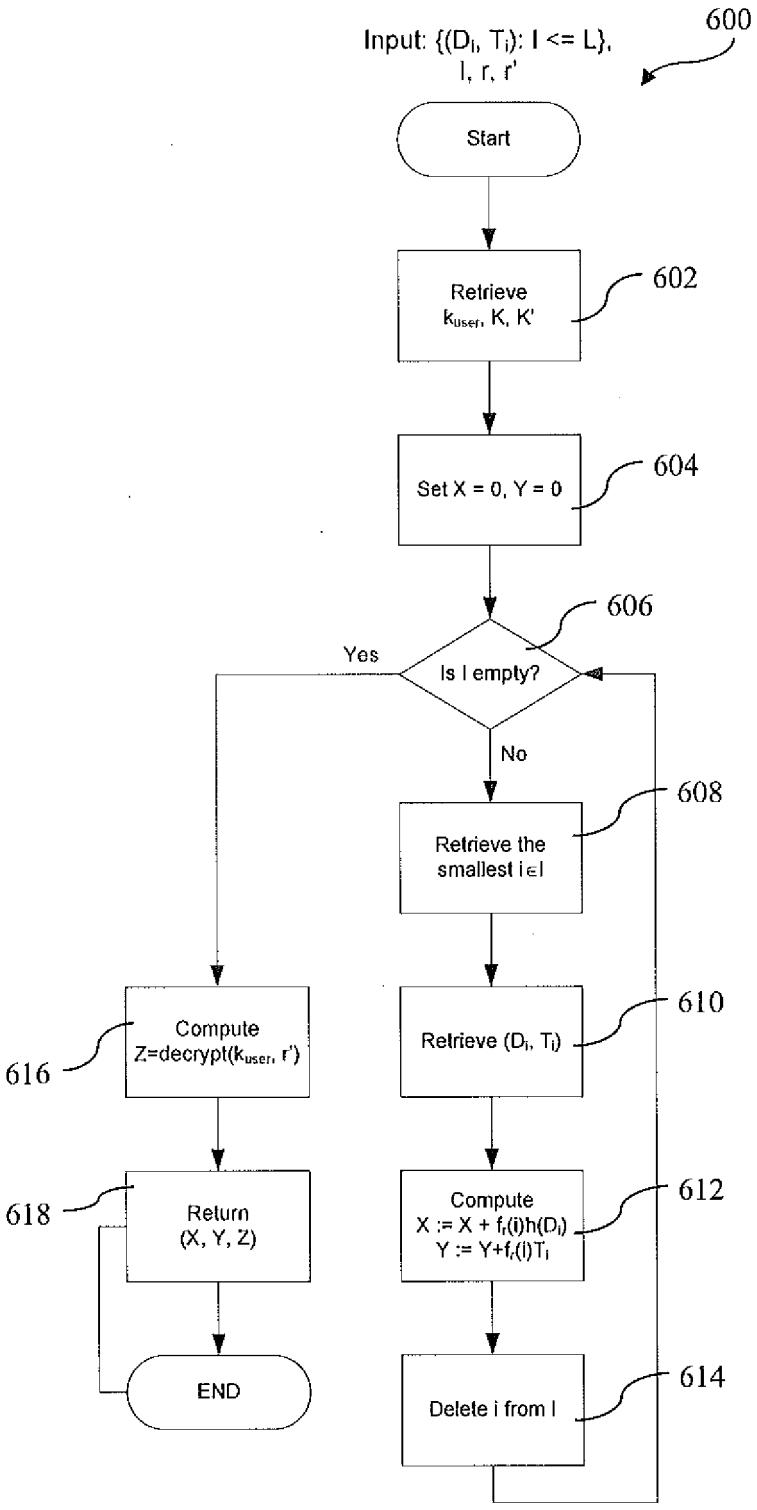

Input: {(Di, Ti): I <= L},
I, r, r'
600
Start
Retrieve
kuser, K, K'
602
Set X = 0, Y = 0
604
606
Is I empty?
Yes
No
608
Retrieve the
smallest i∈I
Retrieve (Di, Ti)
610
Compute
X := X + fr(i)h(Di)
Y := Y+fr(I)Ti
612
Delete i from I
614
Compute
Z=decrypt(kuser, r')
616
Return
(X, Y, Z)
618
END

FIG. 6

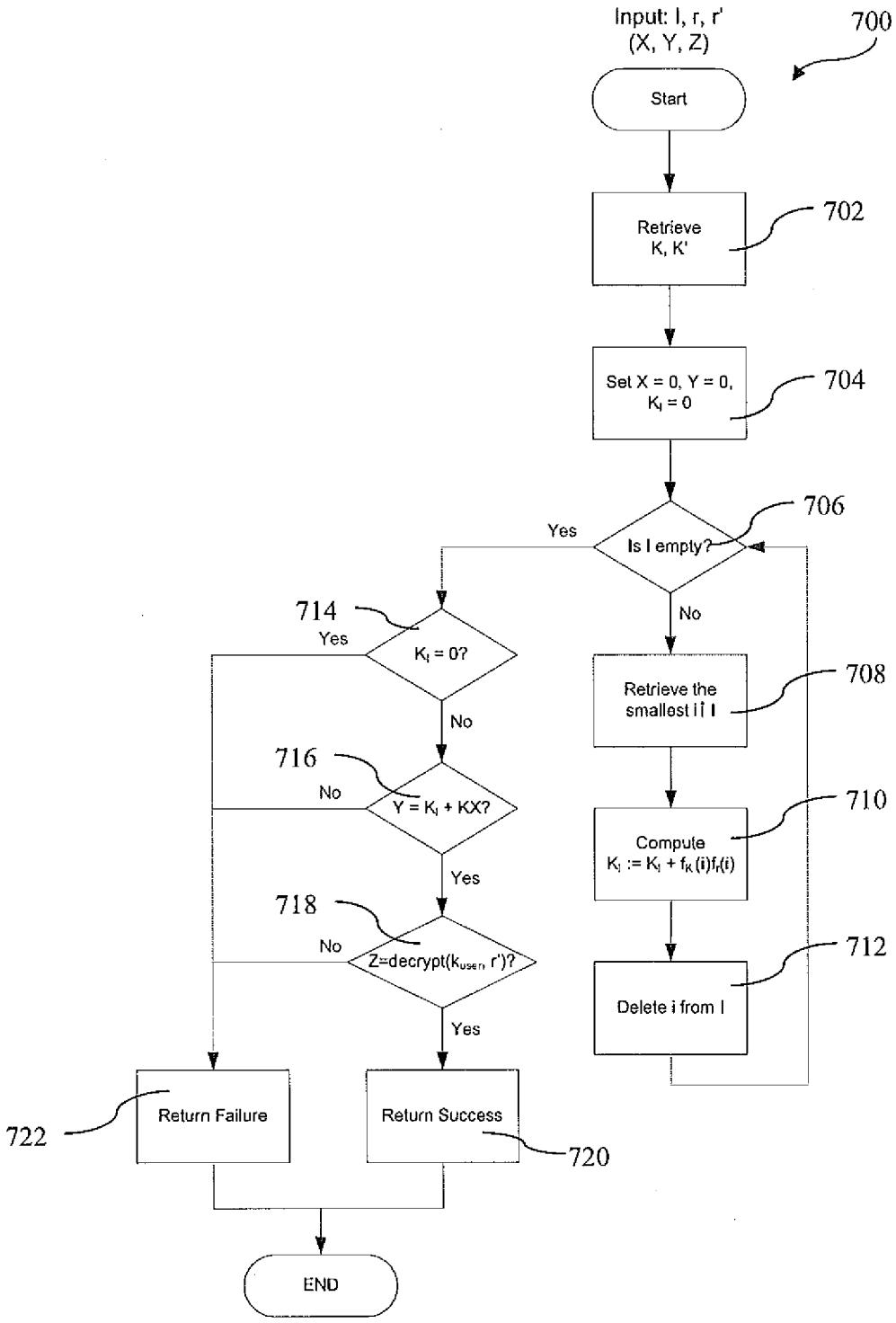

Input: I, r, r'
(X, Y, Z)
700
Start
Retrieve
K, K'
702
Set X = 0, Y = 0,
K_I = 0
704
Is I empty?
706
Yes
No
714
Yes
K_I = 0?
No
716
No
Y = K_I + KX?
Yes
718
No
Z=decrypt(k_{user}, r')?
Yes
Retrieve the
smallest i ∈ I
708
Compute
$K_I := K_I + f_K(i)f_r(i)$
710
Delete i from I
712
Return Failure
722
Return Success
720
END

FIG. 7

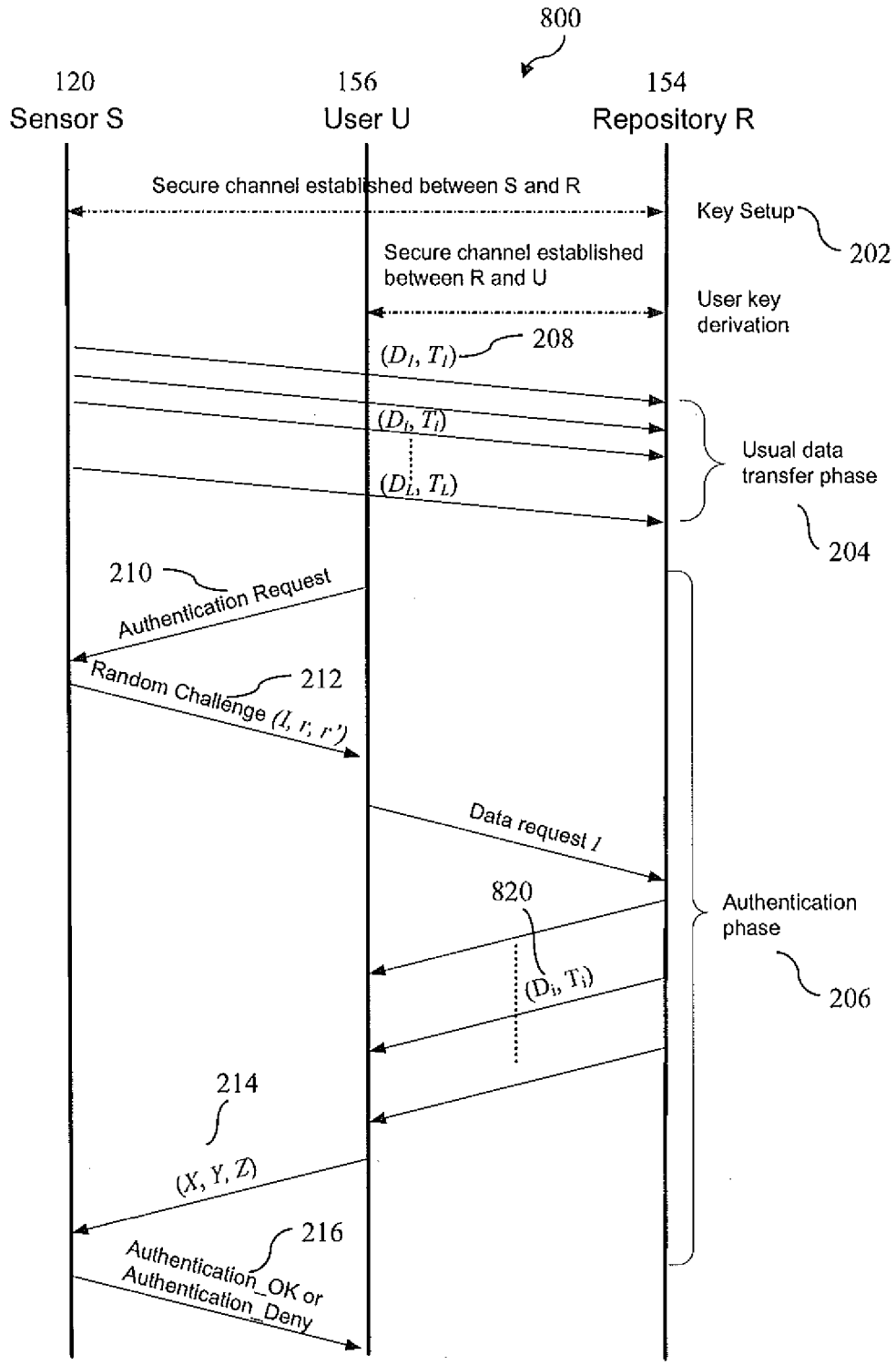

800
120
Sensor S
156
User U
154
Repository R
Secure channel established between S and R
Key Setup
202
Secure channel established between R and U
User key derivation
208
(D_I, T_I)
(D_i, T_i)
(D_L, T_L)
Usual data transfer phase
204
210
Authentication Request
Random Challenge (I, r, r')
212
Data request I
820
(D_i, T_i)
Authentication phase
206
214
(X, Y, Z)
216
Authentication_OK or Authentication_Deny

FIG. 8

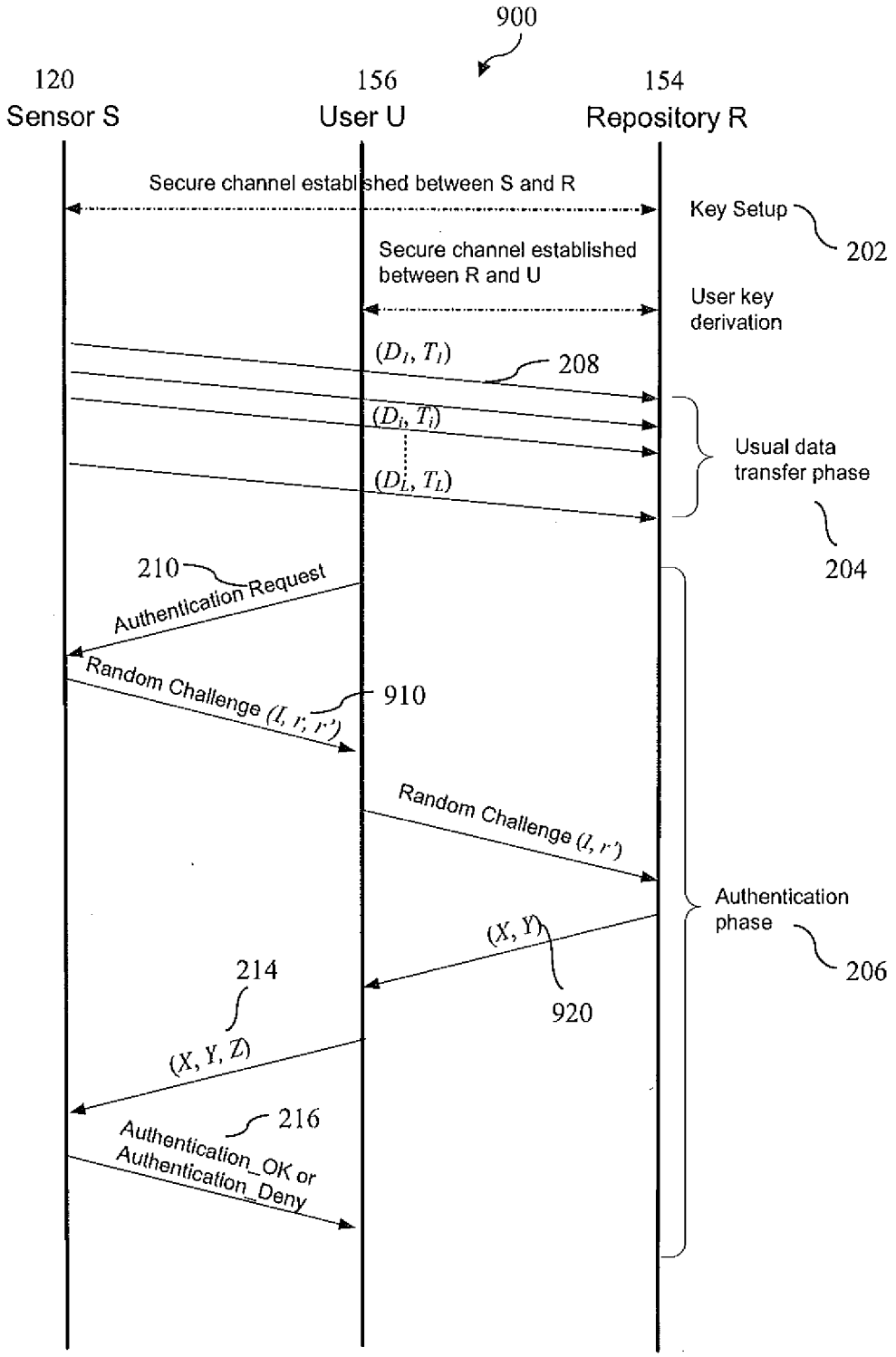

900
120
Sensor S
156
User U
154
Repository R
Secure channel established between S and R
Key Setup
202
Secure channel established between R and U
User key derivation
(D_1, T_1)
208
(D_i, T_i)
(D_L, T_L)
Usual data transfer phase
204
210
Authentication Request
Random Challenge $(I, r; r')$
910
Random Challenge (I, r')
Authentication phase
206
(X, Y)
920
214
(X, Y, Z)
216
Authentication_OK or Authentication_Deny

FIG. 9

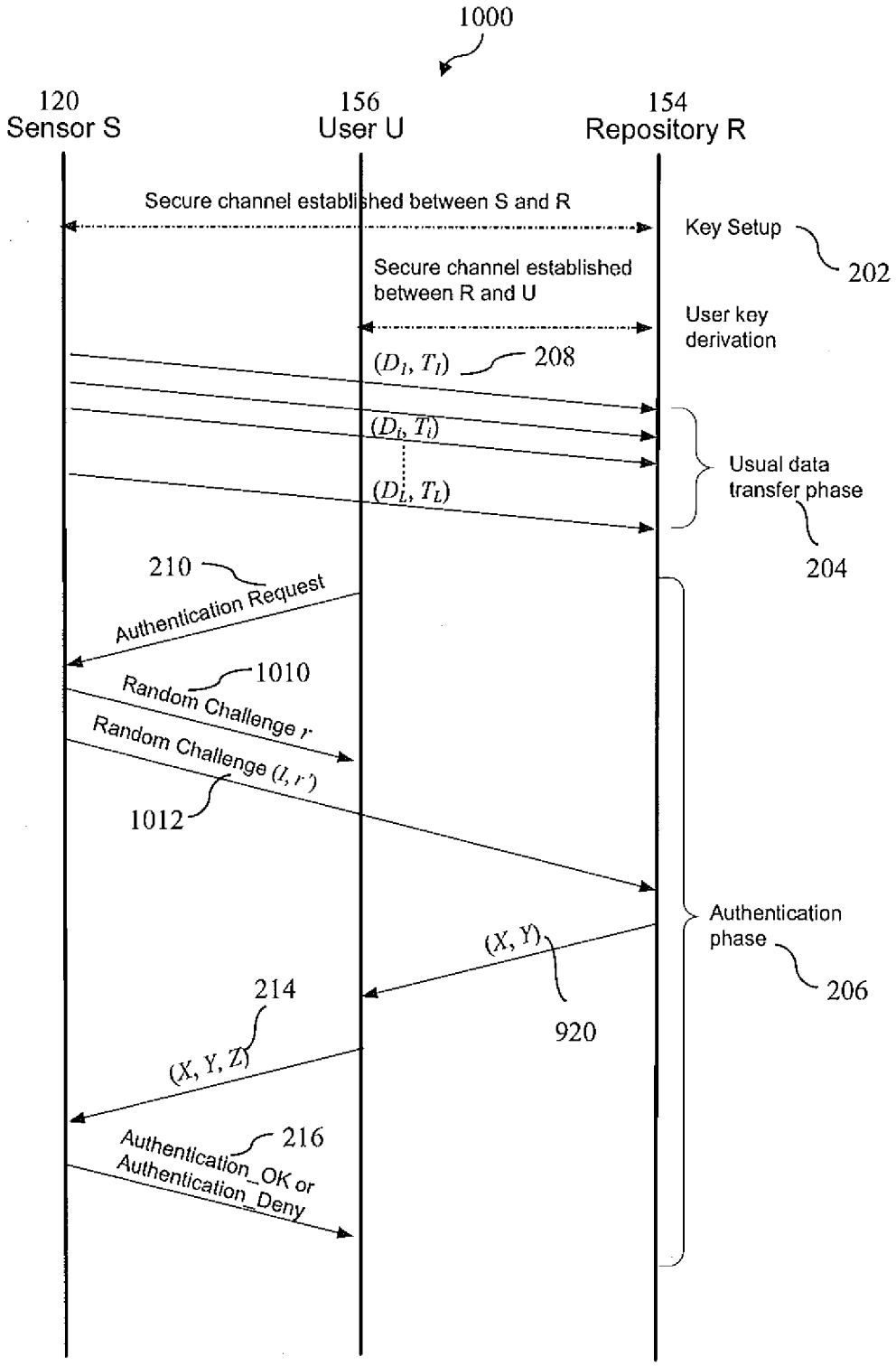

1000
120
Sensor S
156
User U
154
Repository R
Secure channel established between S and R
Key Setup
202
Secure channel established between R and U
User key derivation
(D_1, T_1)
208
(D_i, T_i)
(D_L, T_L)
Usual data transfer phase
204
210
Authentication Request
1010
Random Challenge r
Random Challenge (I, r')
1012
Authentication phase
206
(X, Y)
920
214
(X, Y, Z)
216
Authentication_OK or Authentication_Deny

FIG. 10