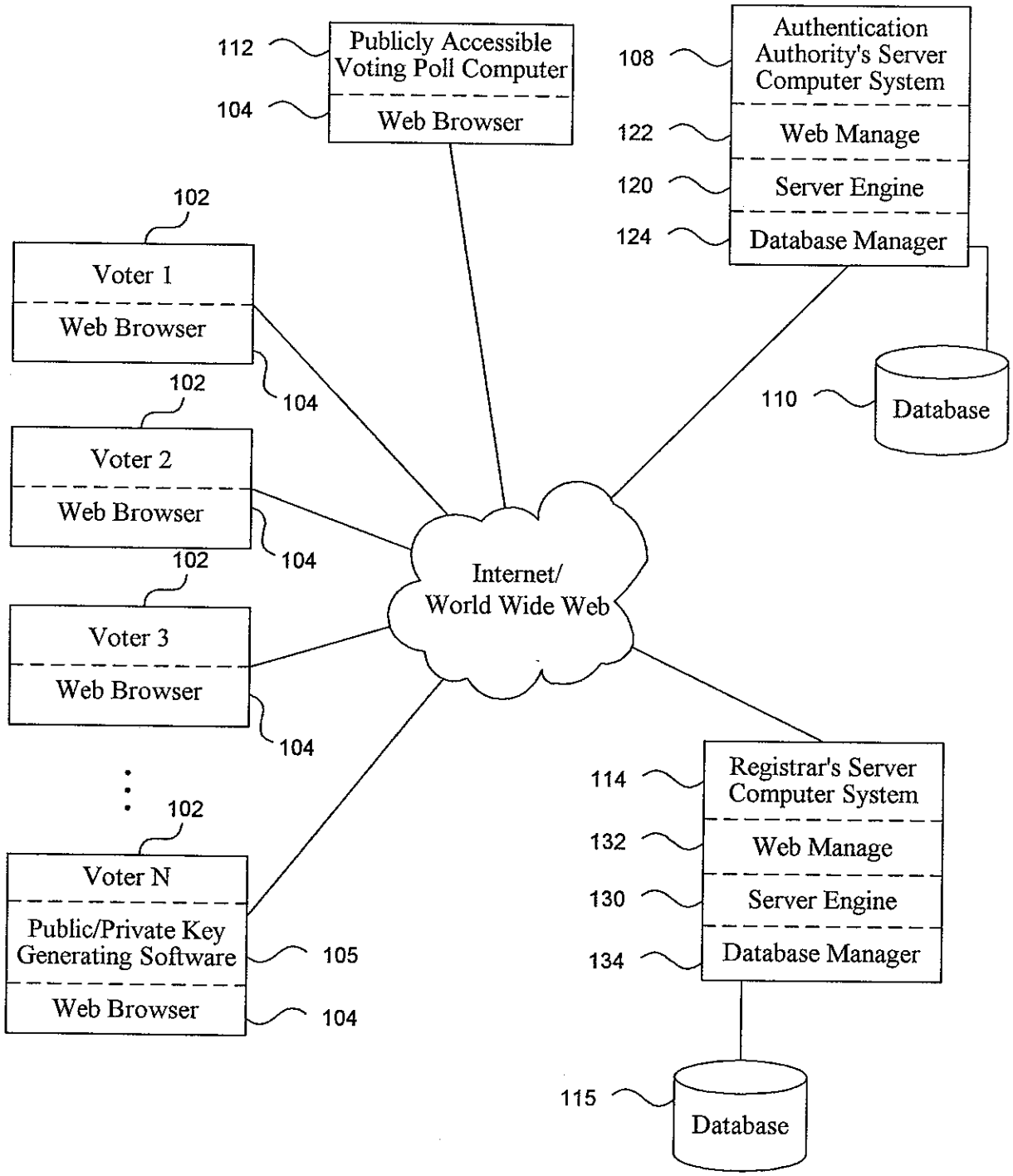

112
Publicly Accessible Voting Poll Computer
104
Web Browser
108
Authentication Authority's Server Computer System
122
Web Manage
120
Server Engine
124
Database Manager
110
Database
102
Voter 1
Web Browser
104
102
Voter 2
Web Browser
104
102
Voter 3
Web Browser
104
Internet/ World Wide Web
102
Voter N
Public/Private Key Generating Software
105
Web Browser
104
114
Registrar's Server Computer System
132
Web Manage
130
Server Engine
134
Database Manager
115
Database

*Fig. 1*

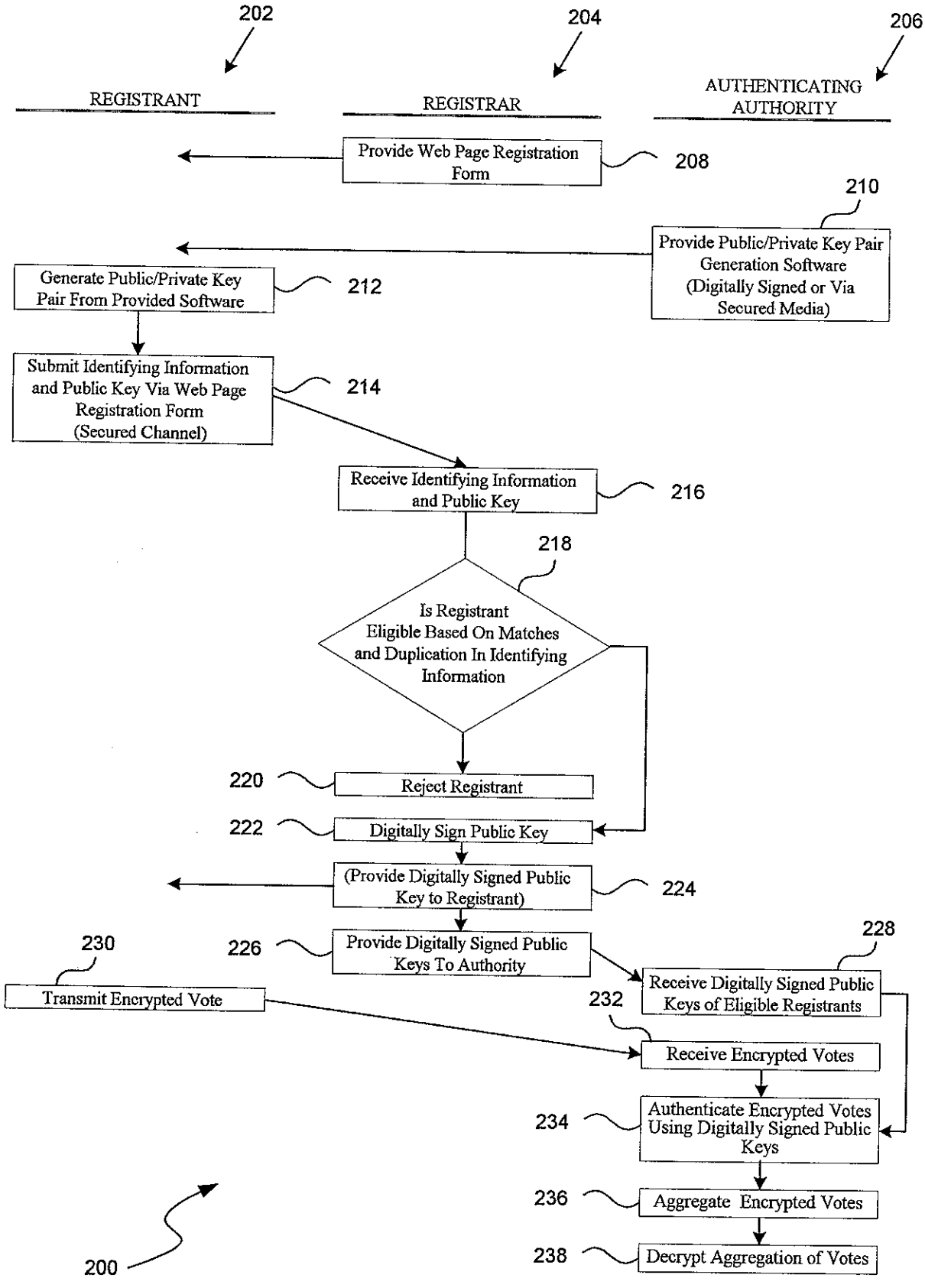

202
204
206
REGISTRANT
REGISTRAR
AUTHENTICATING AUTHORITY
Provide Web Page Registration Form
208
210
Provide Public/Private Key Pair Generation Software (Digitally Signed or Via Secured Media)
Generate Public/Private Key Pair From Provided Software
212
Submit Identifying Information and Public Key Via Web Page Registration Form (Secured Channel)
214
Receive Identifying Information and Public Key
216
218
Is Registrant Eligible Based On Matches and Duplication In Identifying Information
220
Reject Registrant
222
Digitally Sign Public Key
(Provide Digitally Signed Public Key to Registrant)
224
226
Provide Digitally Signed Public Keys To Authority
228
230
Transmit Encrypted Vote
Receive Digitally Signed Public Keys of Eligible Registrants
232
Receive Encrypted Votes
234
Authenticate Encrypted Votes Using Digitally Signed Public Keys
236
Aggregate Encrypted Votes
238
Decrypt Aggregation of Votes
200

*Fig. 2*

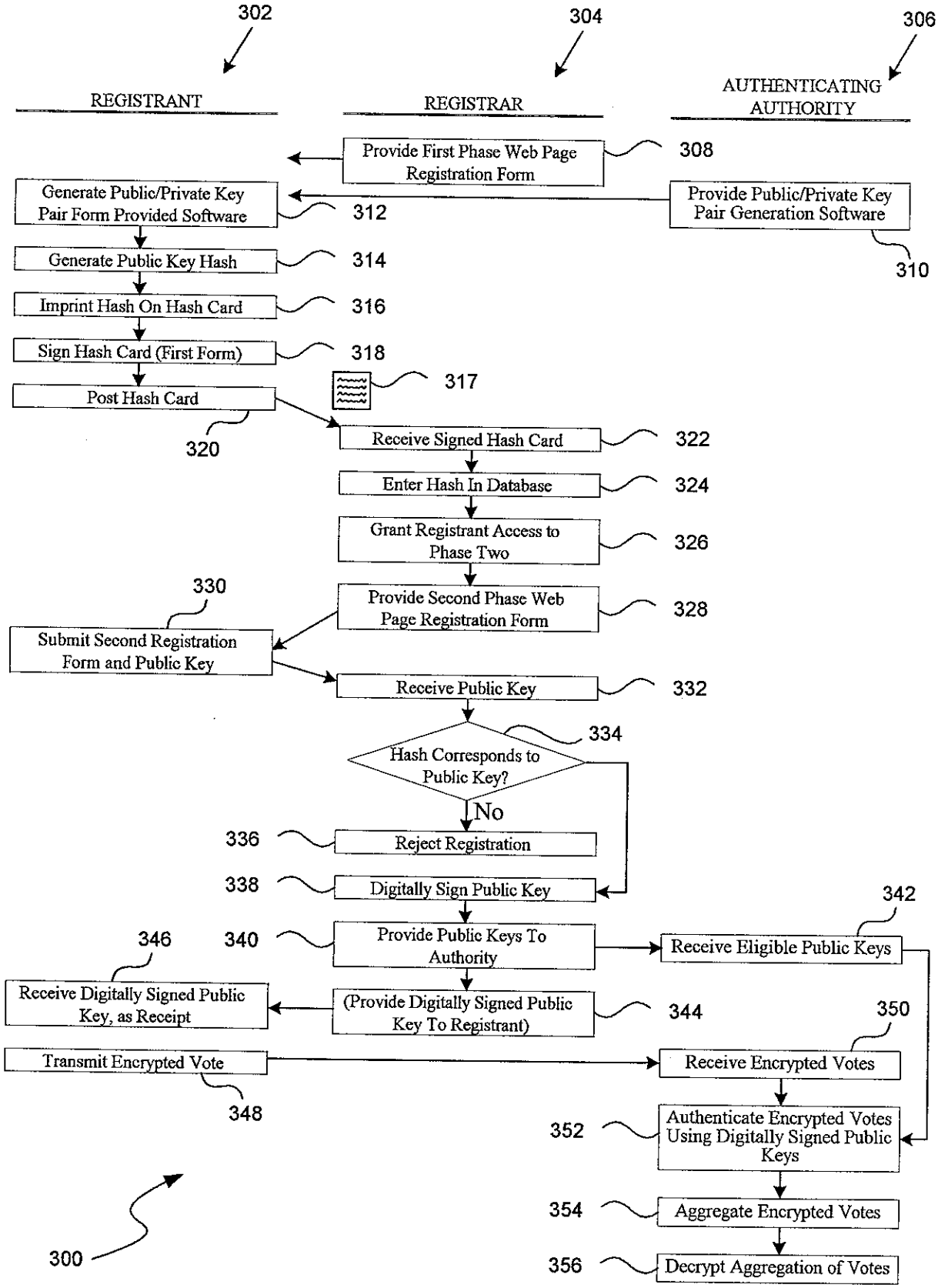

302
304
306
REGISTRANT
REGISTRAR
AUTHENTICATING AUTHORITY
Provide First Phase Web Page Registration Form
308
Generate Public/Private Key Pair Form Provided Software
312
Provide Public/Private Key Pair Generation Software
310
Generate Public Key Hash
314
Imprint Hash On Hash Card
316
Sign Hash Card (First Form)
318
317
Post Hash Card
320
Receive Signed Hash Card
322
Enter Hash In Database
324
Grant Registrant Access to Phase Two
326
330
Provide Second Phase Web Page Registration Form
328
Submit Second Registration Form and Public Key
Receive Public Key
332
334
Hash Corresponds to Public Key?
No
336
Reject Registration
338
Digitally Sign Public Key
342
346
340
Provide Public Keys To Authority
Receive Eligible Public Keys
Receive Digitally Signed Public Key, as Receipt
(Provide Digitally Signed Public Key To Registrant)
344
350
Transmit Encrypted Vote
Receive Encrypted Votes
348
352
Authenticate Encrypted Votes Using Digitally Signed Public Keys
354
Aggregate Encrypted Votes
356
Decrypt Aggregation of Votes
300

*Fig. 3*

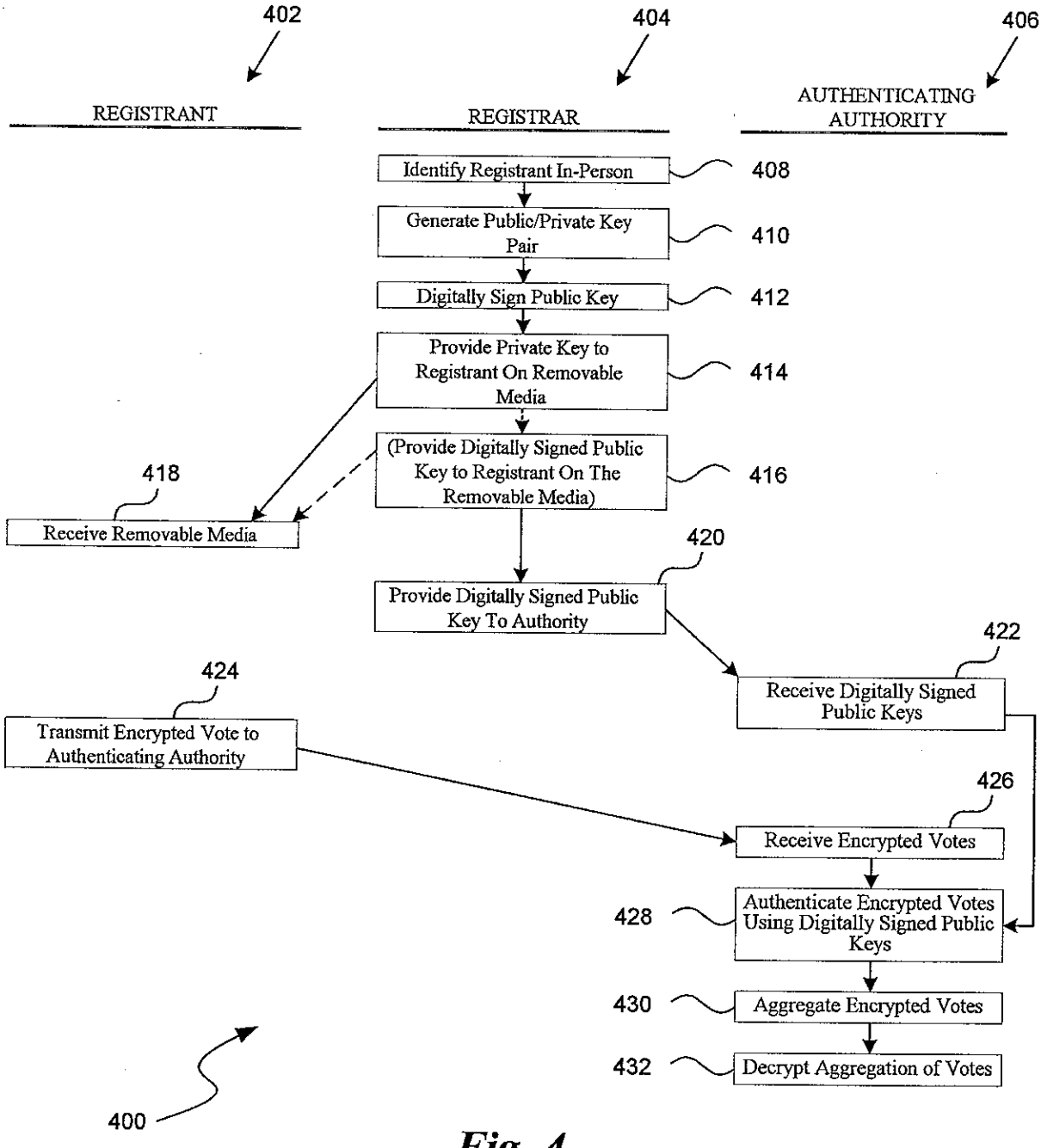

402
404
406
REGISTRANT
REGISTRAR
AUTHENTICATING AUTHORITY
Identify Registrant In-Person
408
Generate Public/Private Key Pair
410
Digitally Sign Public Key
412
Provide Private Key to Registrant On Removable Media
414
(Provide Digitally Signed Public Key to Registrant On The Removable Media)
416
418
Receive Removable Media
420
Provide Digitally Signed Public Key To Authority
422
Receive Digitally Signed Public Keys
424
Transmit Encrypted Vote to Authenticating Authority
426
Receive Encrypted Votes
428
Authenticate Encrypted Votes Using Digitally Signed Public Keys
430
Aggregate Encrypted Votes
432
Decrypt Aggregation of Votes
400

*Fig. 4*

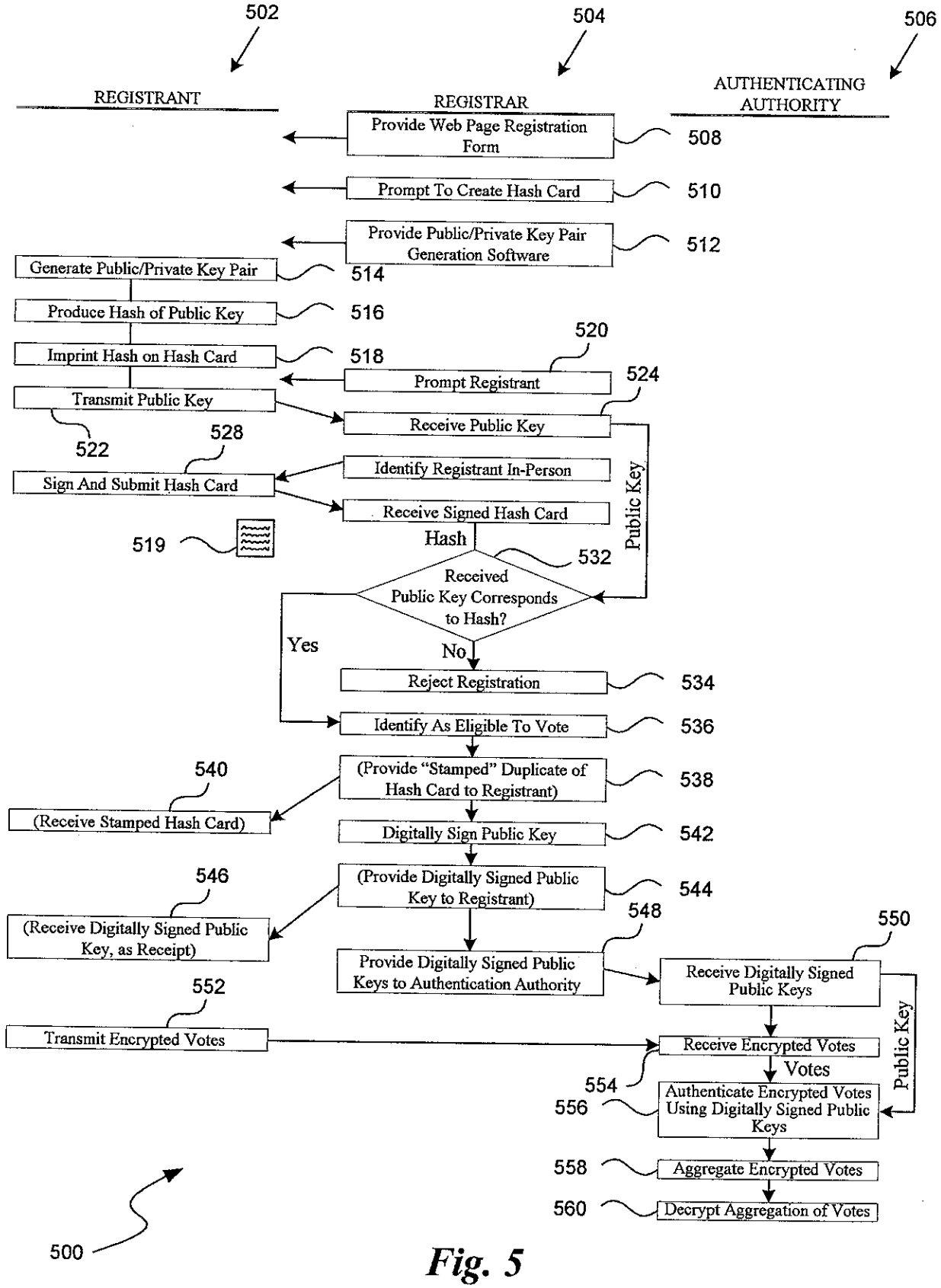

502
504
506
REGISTRANT
REGISTRAR
AUTHENTICATING AUTHORITY
Provide Web Page Registration Form
508
Prompt To Create Hash Card
510
Provide Public/Private Key Pair Generation Software
512
Generate Public/Private Key Pair
514
Produce Hash of Public Key
516
Imprint Hash on Hash Card
518
520
Prompt Registrant
524
Transmit Public Key
Receive Public Key
522
528
Sign And Submit Hash Card
Identify Registrant In-Person
Receive Signed Hash Card
Public Key
519
Hash
532
Received Public Key Corresponds to Hash?
Yes
No
Reject Registration
534
Identify As Eligible To Vote
536
540
(Provide "Stamped" Duplicate of Hash Card to Registrant)
538
(Receive Stamped Hash Card)
Digitally Sign Public Key
542
546
(Provide Digitally Signed Public Key to Registrant)
544
548
550
(Receive Digitally Signed Public Key, as Receipt)
Provide Digitally Signed Public Keys to Authentication Authority
Receive Digitally Signed Public Keys
552
Transmit Encrypted Votes
Receive Encrypted Votes
Votes
Public Key
554
556
Authenticate Encrypted Votes Using Digitally Signed Public Keys
558
Aggregate Encrypted Votes
560
Decrypt Aggregation of Votes
500

*Fig. 5*