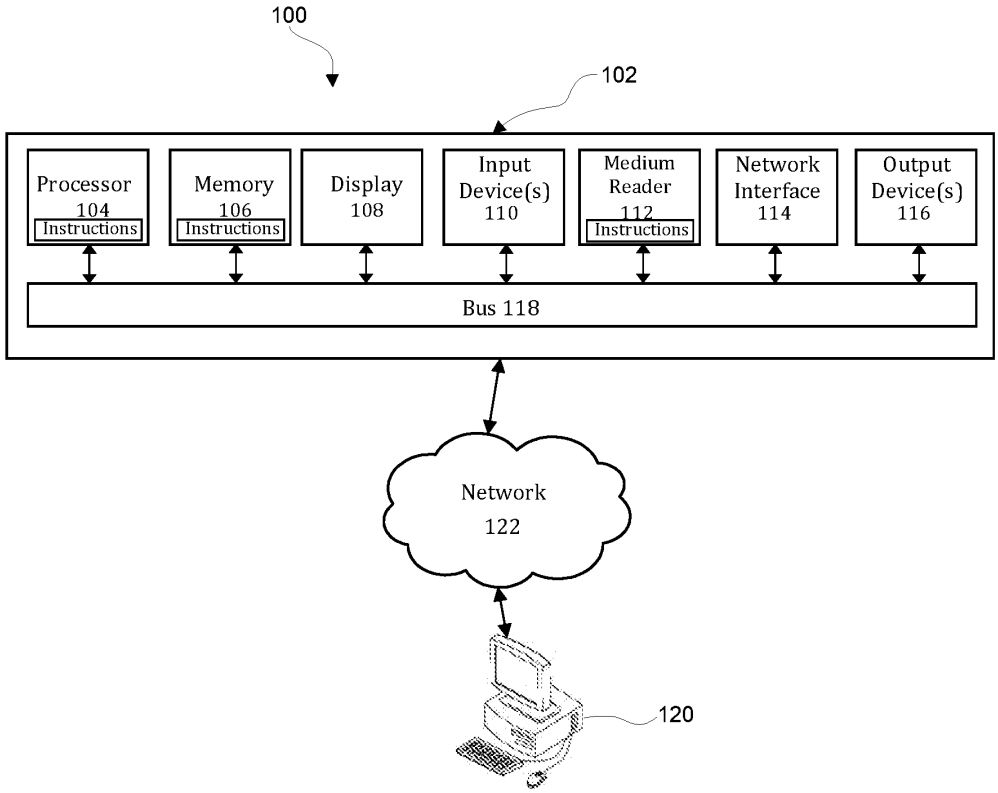
100
102
Processor
104
Instructions
Memory
106
Instructions
Display
108
Input
Device(s)
110
Medium
Reader
112
Instructions
Network
Interface
114
Output
Device(s)
116
Bus 118
Network
122
120

FIG. 1

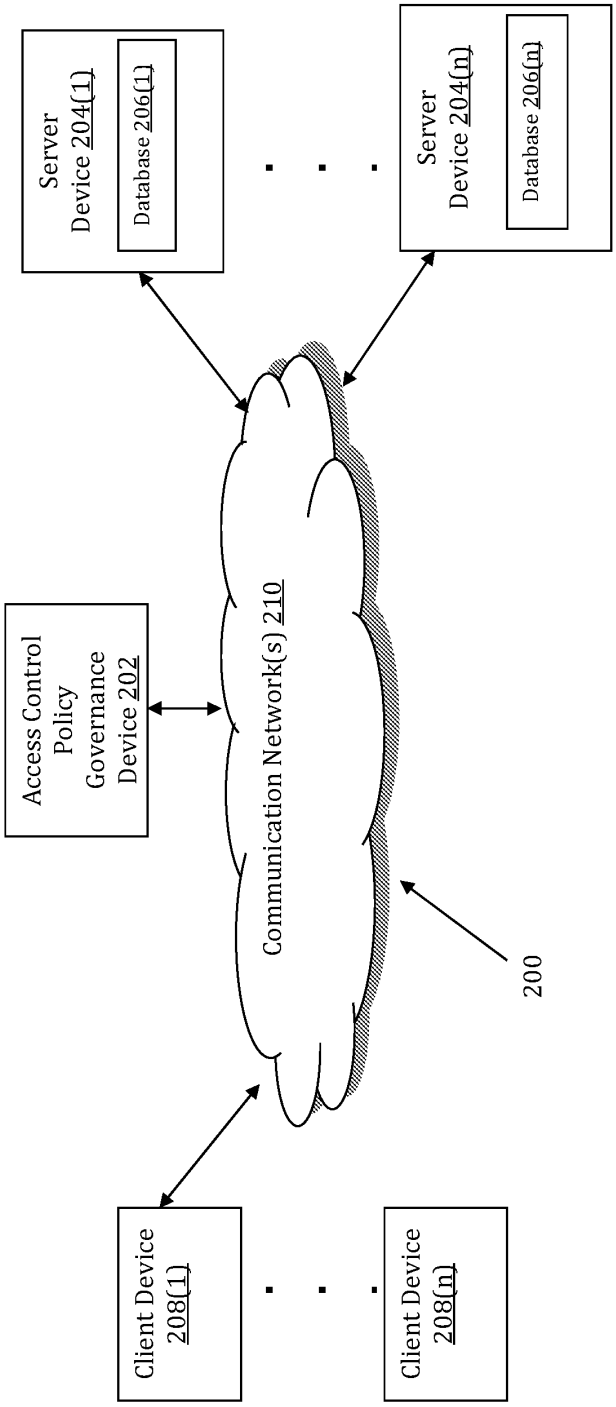
Server Device 204(1)
Database 206(1)
Server Device 204(n)
Database 206(n)
Access Control Policy Governance Device 202
Communication Network(s) 210
200
Client Device 208(1)
Client Device 208(n)

FIG. 2

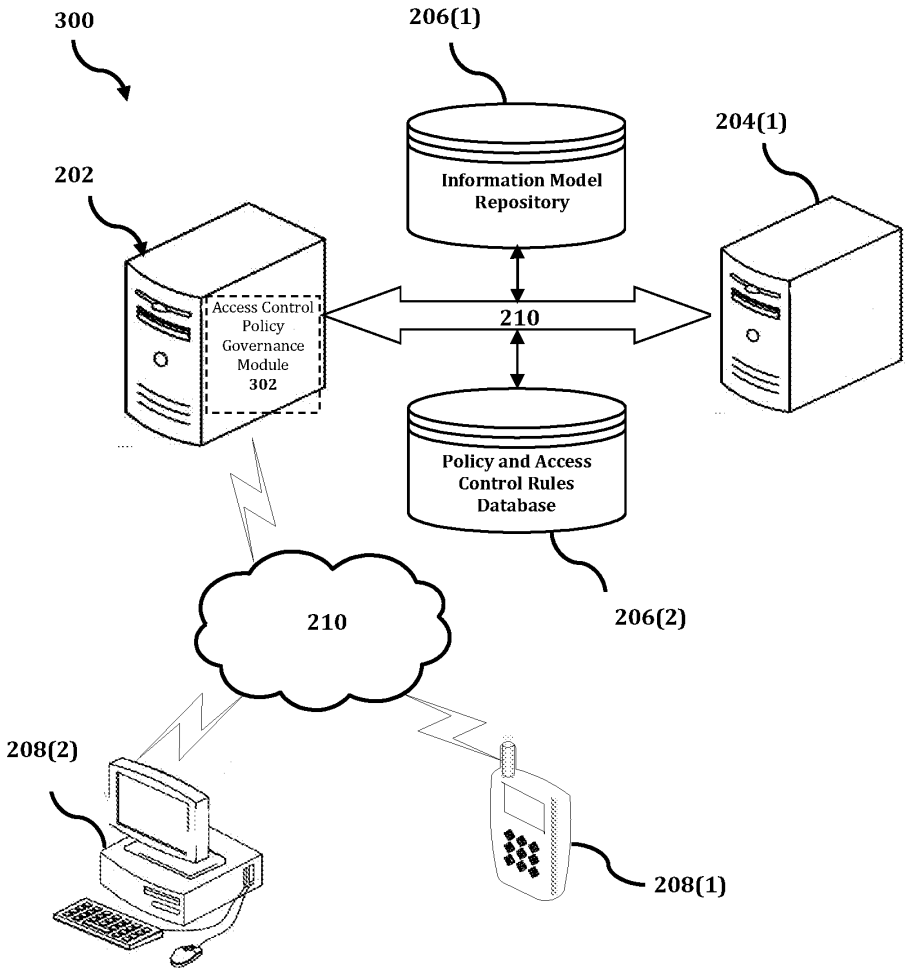
300
206(1)
204(1)
202
Information Model Repository
Access Control Policy Governance Module 302
210
Policy and Access Control Rules Database
206(2)
210
208(2)
208(1)

FIG. 3

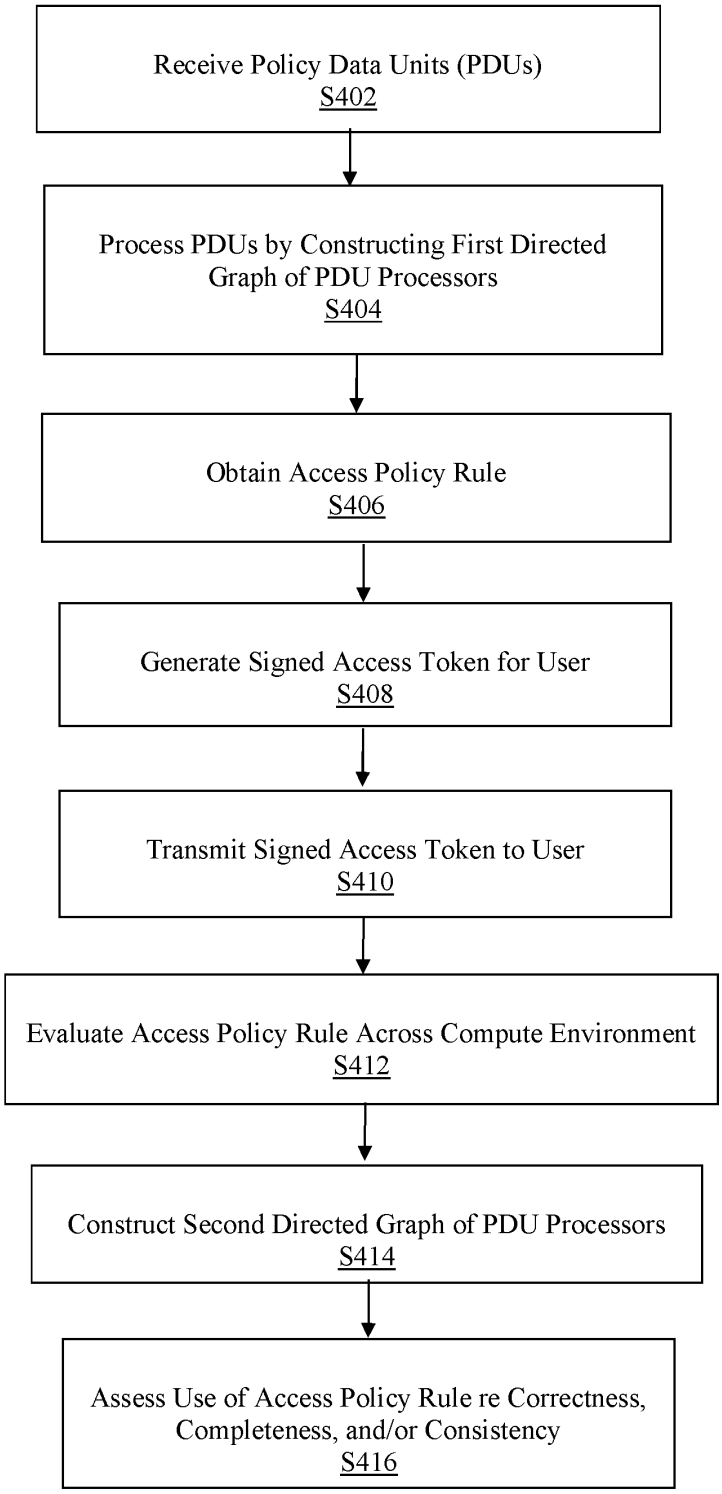
Receive Policy Data Units (PDUs)
S402
Process PDUs by Constructing First Directed Graph of PDU Processors
S404
Obtain Access Policy Rule
S406
Generate Signed Access Token for User
S408
Transmit Signed Access Token to User
S410
Evaluate Access Policy Rule Across Compute Environment
S412
Construct Second Directed Graph of PDU Processors
S414
Assess Use of Access Policy Rule re Correctness, Completeness, and/or Consistency
S416

FIG. 4

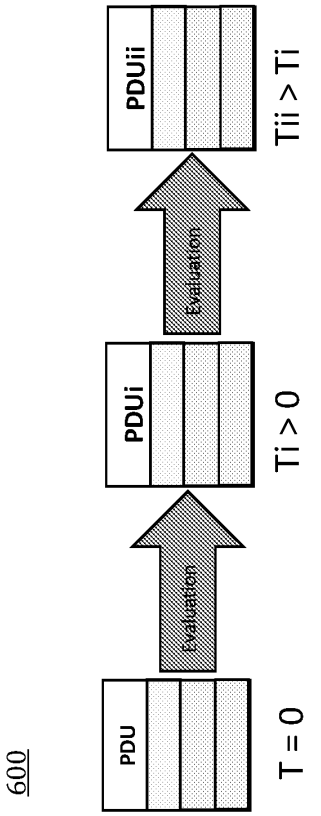
600
PDU
T = 0
Evaluation
PDUi
Ti > 0
Evaluation
PDUii
Tii > Ti

FIG. 6

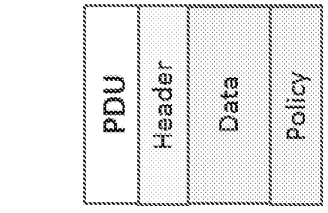
500
PDU
Header
Data
Policy

FIG. 5

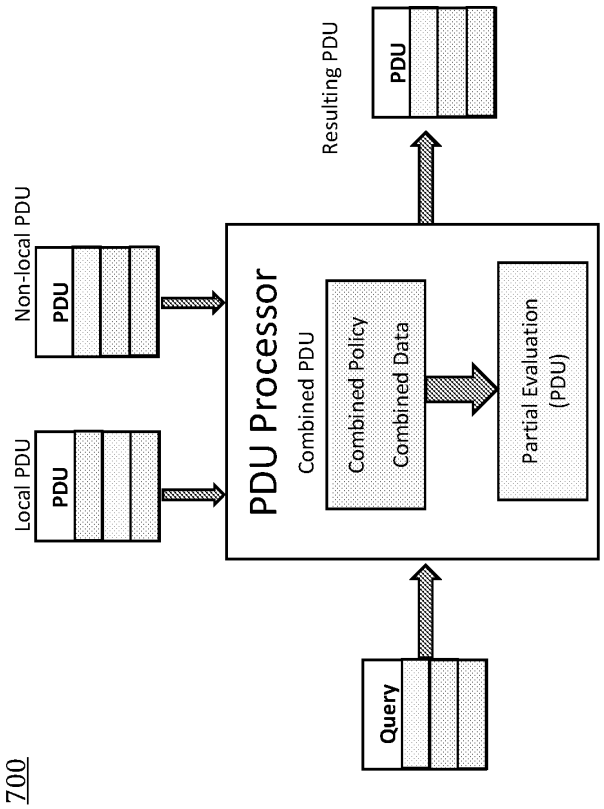
700
Query
PDU Processor
Combined PDU
Combined Policy
Combined Data
Partial Evaluation
(PDU)
Local PDU
PDU
Non-local PDU
PDU
Resulting PDU
PDU

FIG. 7

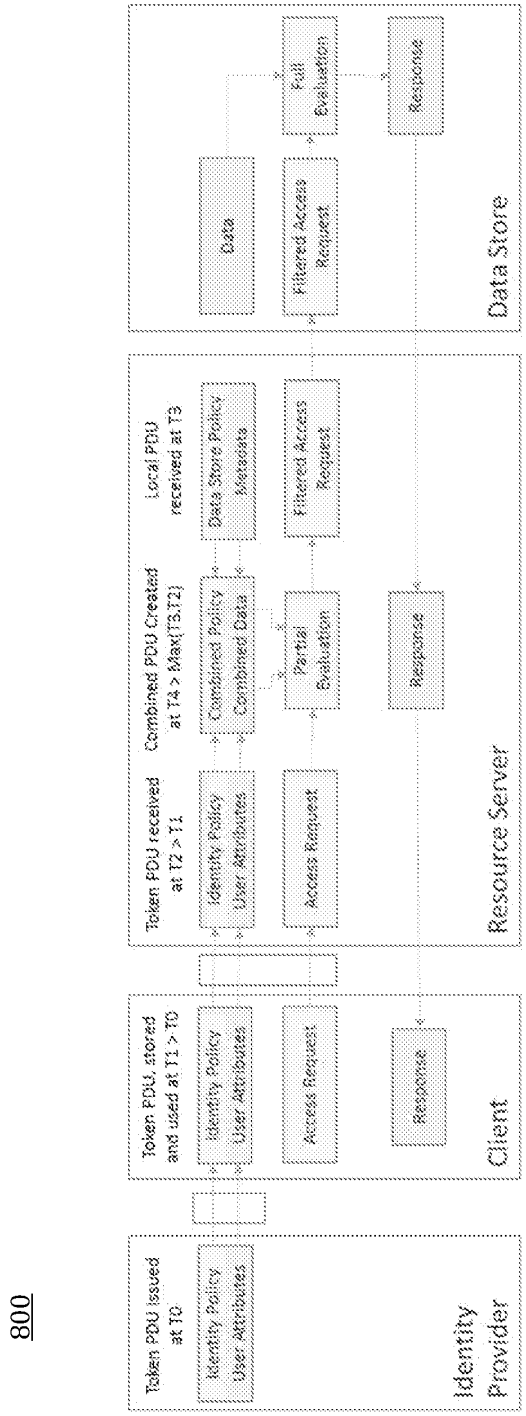
800
Token PDU issued at T0
Identity Policy
User Attributes
Identity Provider
Token PDU, stored and used at T1 > T0
Identity Policy
User Attributes
Access Request
Response
Client
Token PDU received at T2 > T1
Identity Policy
User Attributes
Access Request
Combined PDU Created at T4 > Max{T3,T2}
Combined Policy
Combined Data
Partial Evaluation
Response
Local PDU received at T3
Data Store Policy
Metadata
Filtered Access Request
Resource Server
Data
Filtered Access Request
Full Evaluation
Response
Data Store

FIG. 8

P65052

900

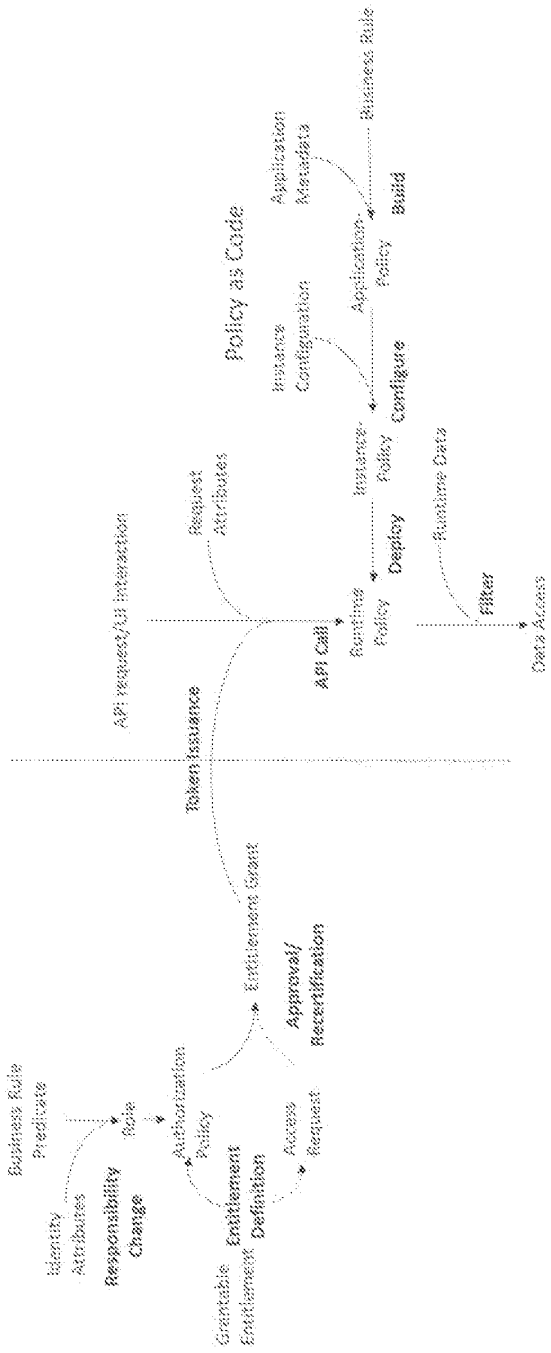

FIG. 9

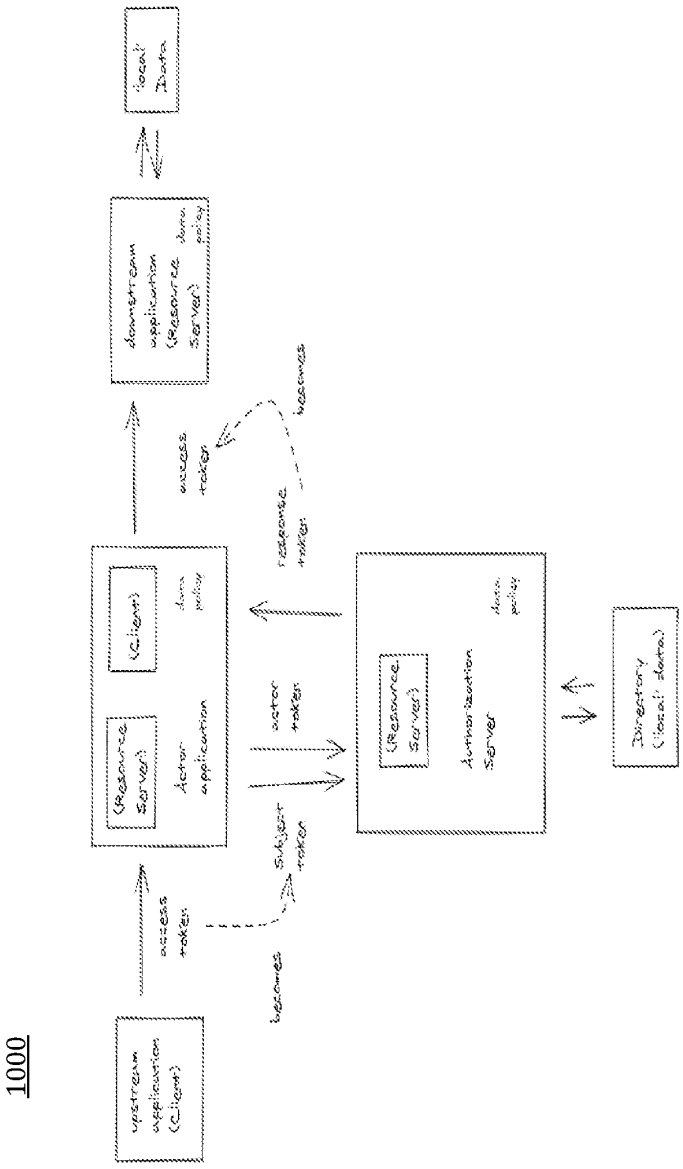
1000
upstream application (Client)
access token
becomes
Subject token
(Resource Server)
Actor application
(Client)
Actor policy
actor token
(Resource Server)
Authorization Server
Actor policy
resource token
becomes
access token
downstream application (Resource Server)
Actor policy
local Data
Directory (local data)

FIG. 10

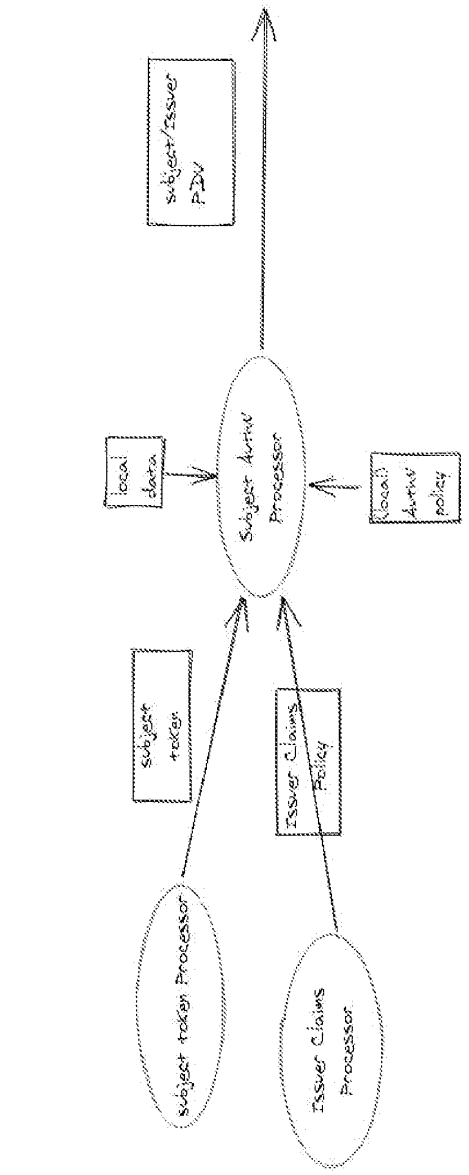
1100
Subject token Processor
Issuer Claims Processor
Subject token
Issuer Claims Policy
local data
Subject Authn Processor
local Authn policy
Subject/Issuer PDV

FIG. 11

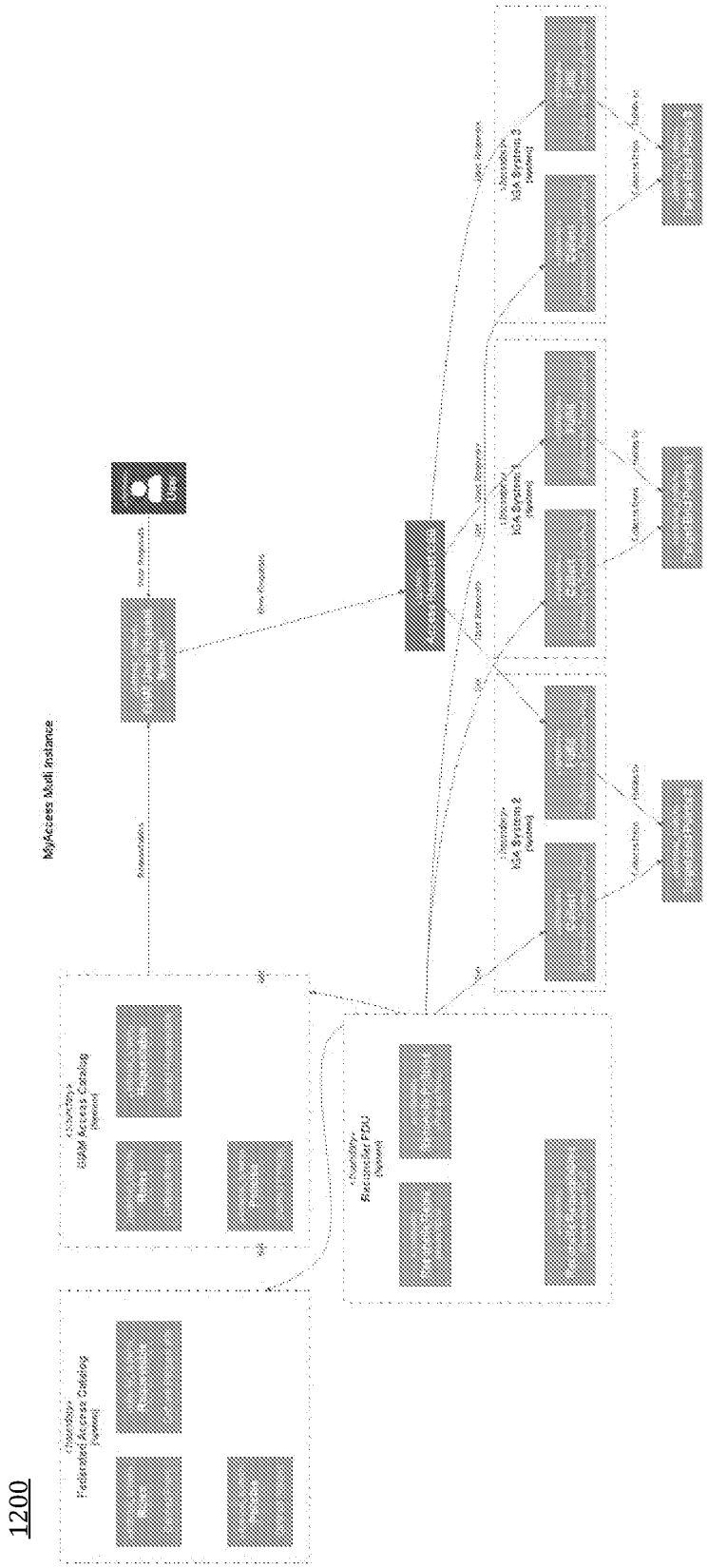

FIG. 12