0 4 JUL 2005

FIG. 1

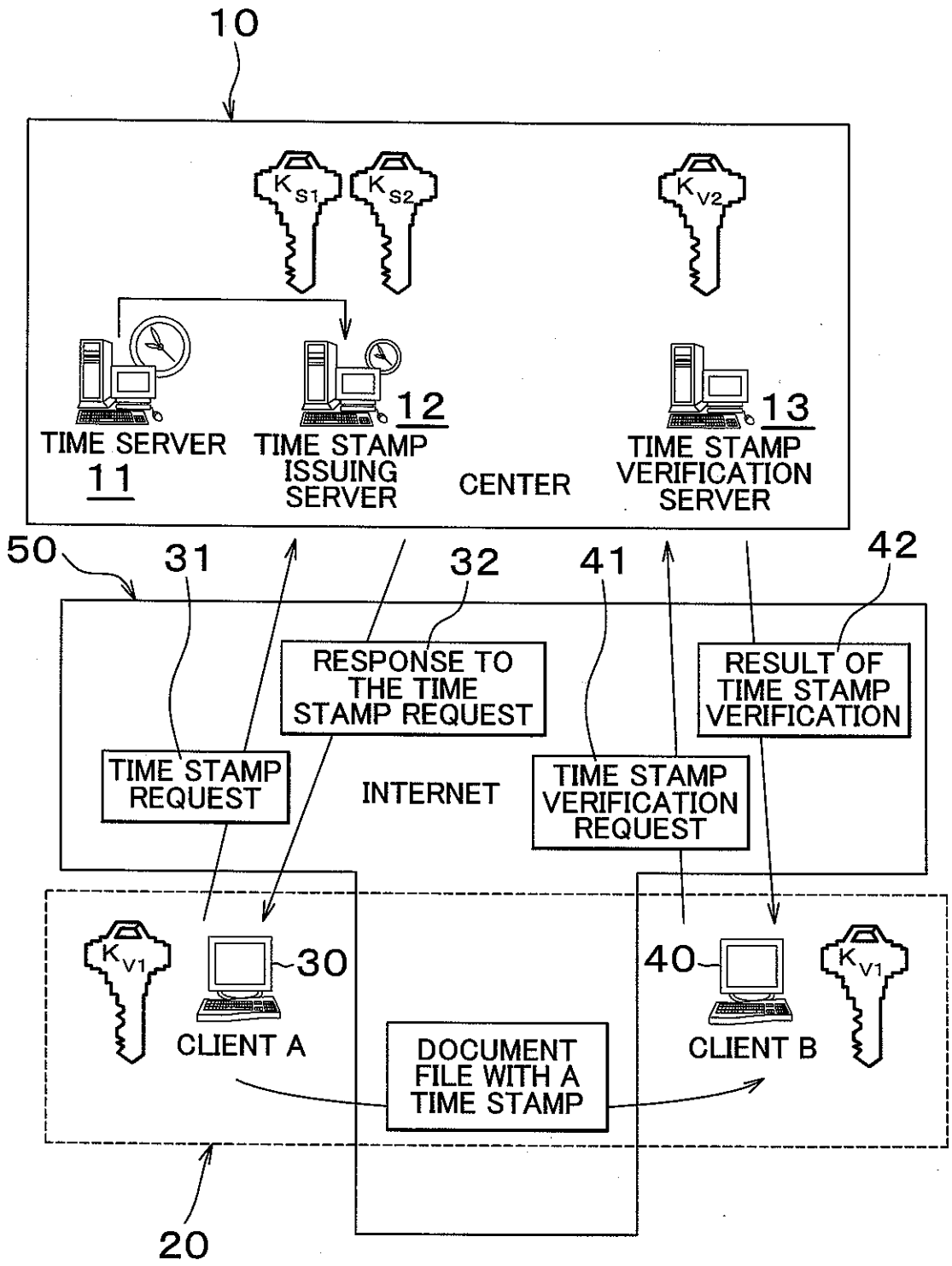


FIG. 2

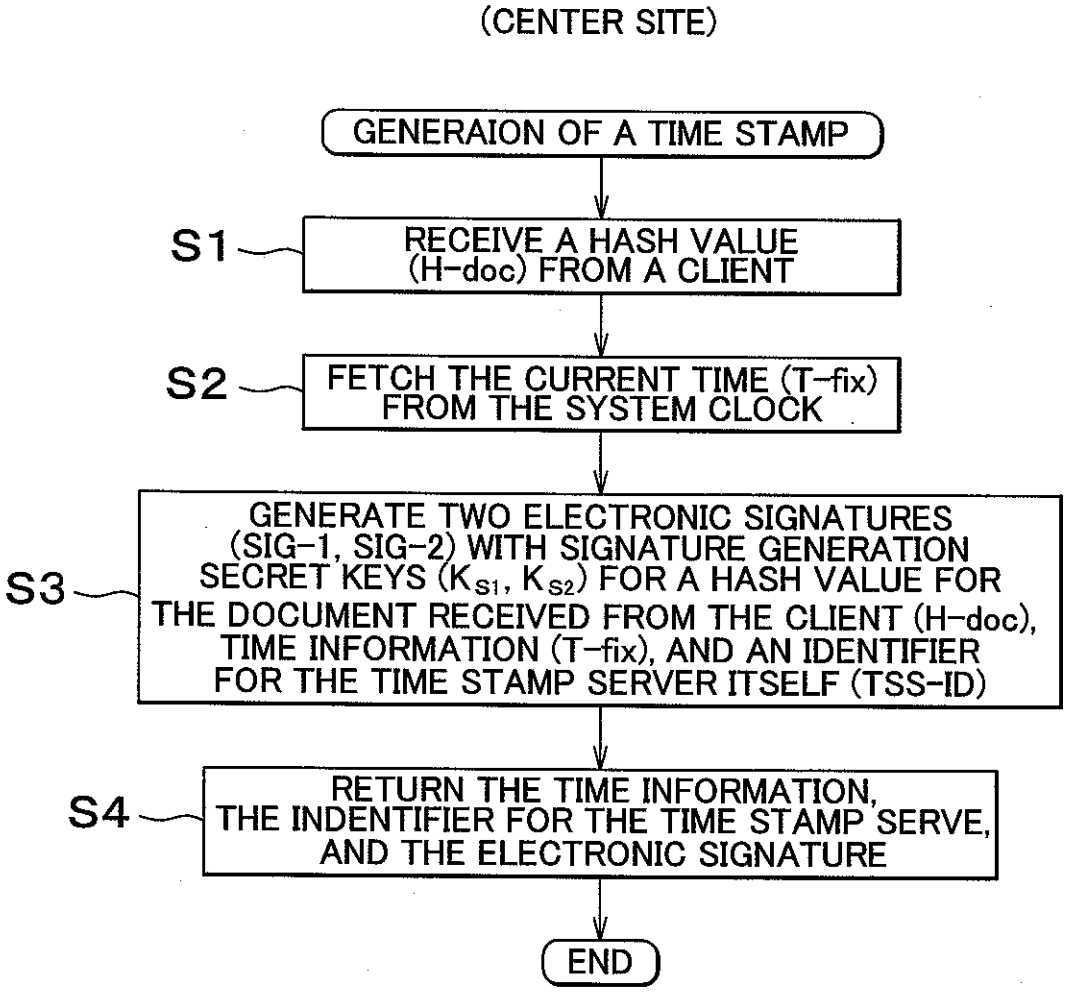

(CENTER SITE)
GENERAION OF A TIME STAMP
S1
RECEIVE A HASH VALUE (H-doc) FROM A CLIENT
S2
FETCH THE CURRENT TIME (T-fix) FROM THE SYSTEM CLOCK
S3
GENERATE TWO ELECTRONIC SIGNATURES (SIG-1, SIG-2) WITH SIGNATURE GENERATION SECRET KEYS (K_{S1}, K_{S2}) FOR A HASH VALUE FOR THE DOCUMENT RECEIVED FROM THE CLIENT (H-doc), TIME INFORMATION (T-fix), AND AN IDENTIFIER FOR THE TIME STAMP SERVER ITSELF (TSS-ID)
S4
RETURN THE TIME INFORMATION, THE INDENTIFIER FOR THE TIME STAMP SERVE, AND THE ELECTRONIC SIGNATURE
END

FIG. 3

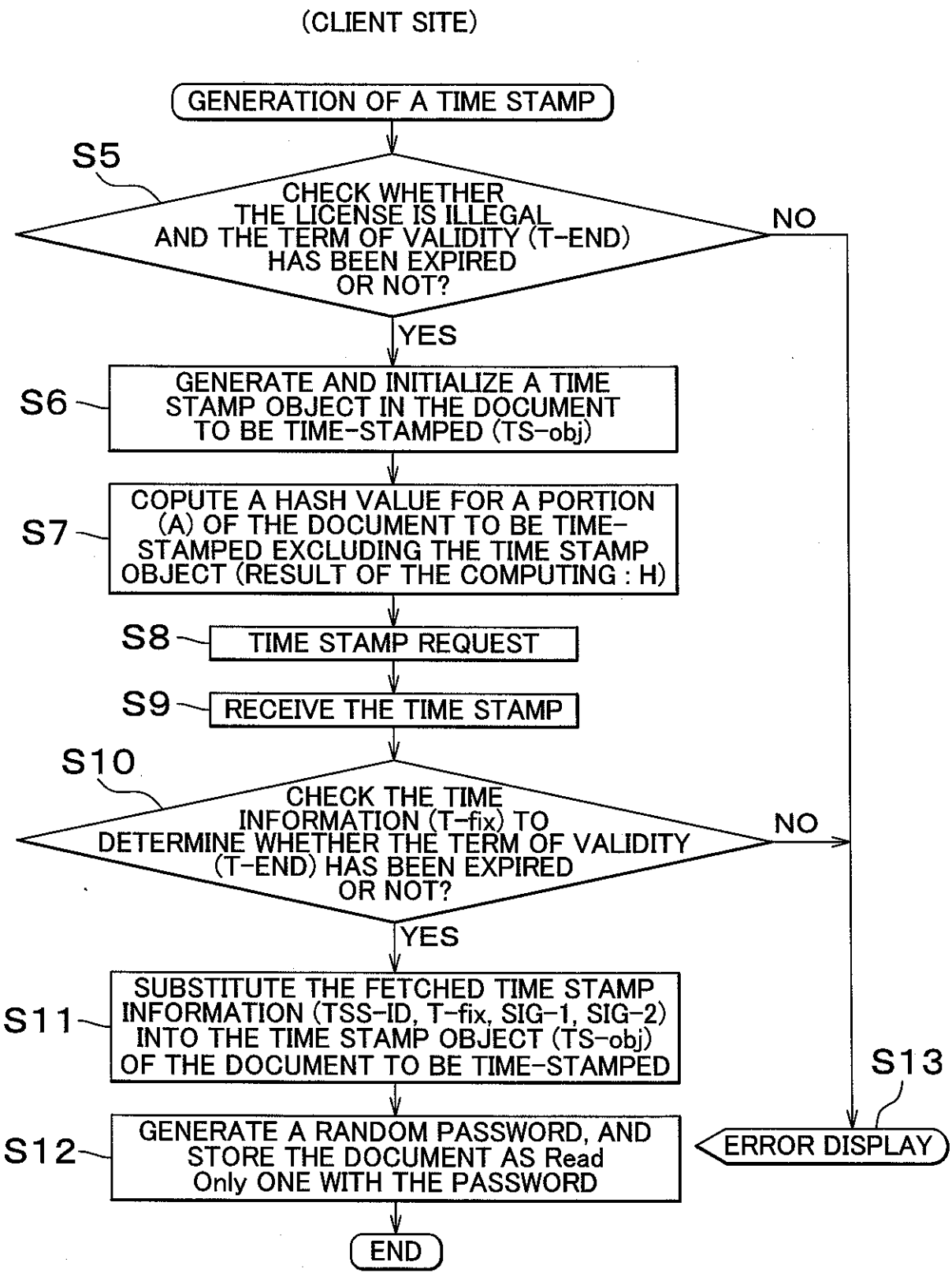
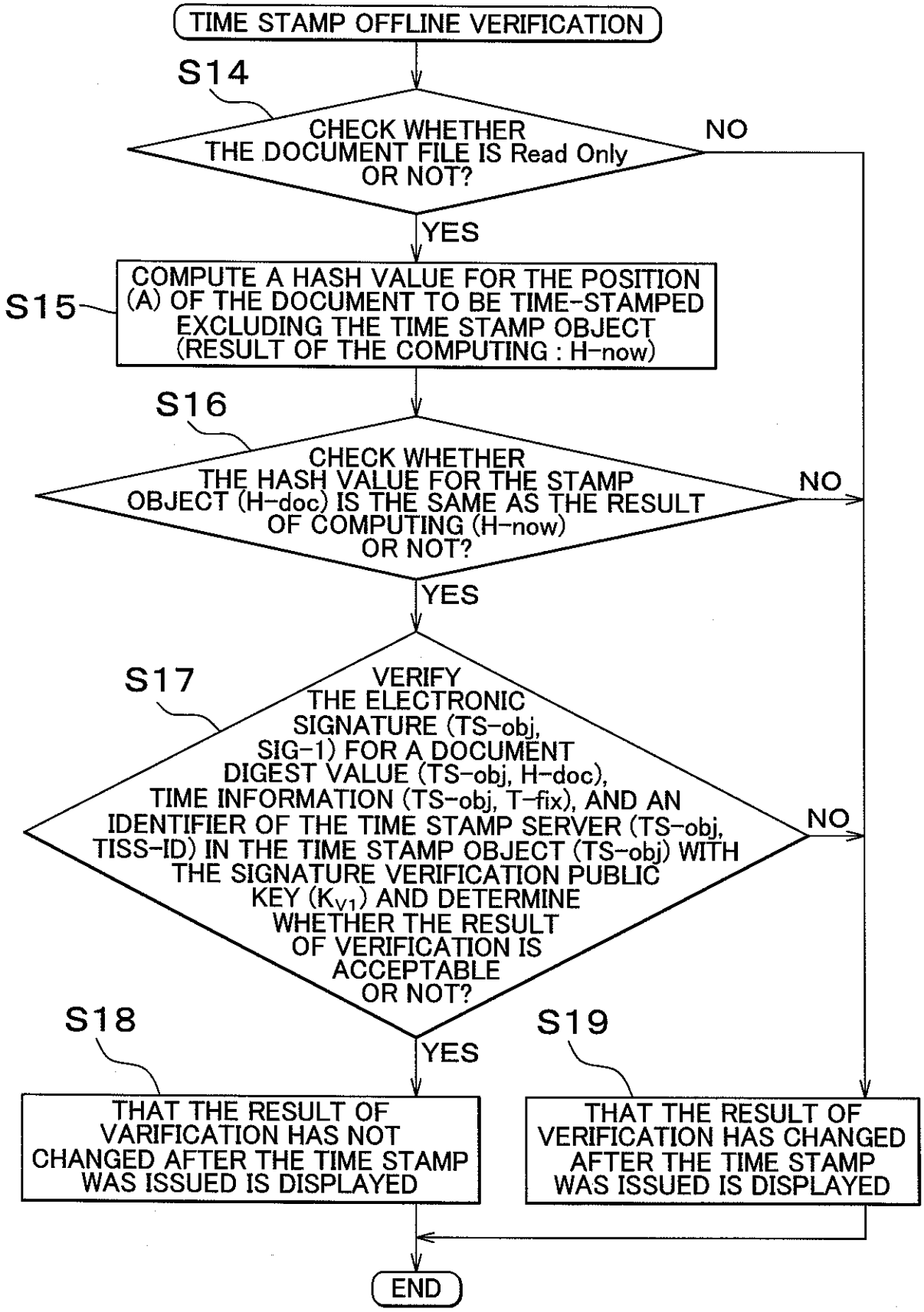
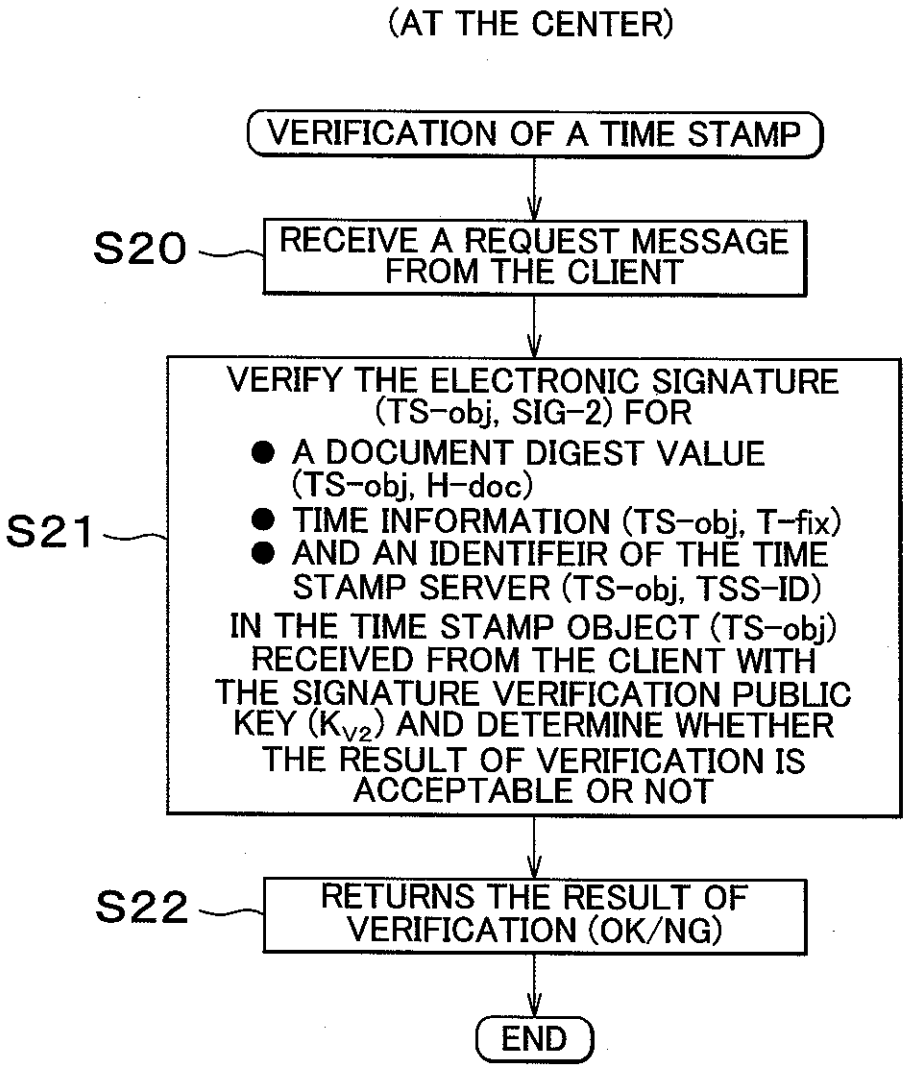

(CLIENT SITE)
GENERATION OF A TIME STAMP
S5
CHECK WHETHER THE LICENSE IS ILLEGAL AND THE TERM OF VALIDITY (T-END) HAS BEEN EXPIRED OR NOT?
NO
YES
S6
GENERATE AND INITIALIZE A TIME STAMP OBJECT IN THE DOCUMENT TO BE TIME-STAMPED (TS-obj)
S7
COPUTE A HASH VALUE FOR A PORTION (A) OF THE DOCUMENT TO BE TIME-STAMPED EXCLUDING THE TIME STAMP OBJECT (RESULT OF THE COMPUTING : H)
S8
TIME STAMP REQUEST
S9
RECEIVE THE TIME STAMP
S10
CHECK THE TIME INFORMATION (T-fix) TO DETERMINE WHETHER THE TERM OF VALIDITY (T-END) HAS BEEN EXPIRED OR NOT?
NO
YES
S11
SUBSTITUTE THE FETCHED TIME STAMP INFORMATION (TSS-ID, T-fix, SIG-1, SIG-2) INTO THE TIME STAMP OBJECT (TS-obj) OF THE DOCUMENT TO BE TIME-STAMPED
S12
GENERATE A RANDOM PASSWORD, AND STORE THE DOCUMENT AS Read Only ONE WITH THE PASSWORD
S13
ERROR DISPLAY
END

FIG. 4


TIME STAMP OFFLINE VERIFICATION
S14
CHECK WHETHER THE DOCUMENT FILE IS Read Only OR NOT?
NO
YES
S15
COMPUTE A HASH VALUE FOR THE POSITION (A) OF THE DOCUMENT TO BE TIME-STAMPED EXCLUDING THE TIME STAMP OBJECT (RESULT OF THE COMPUTING : H-now)
S16
CHECK WHETHER THE HASH VALUE FOR THE STAMP OBJECT (H-doc) IS THE SAME AS THE RESULT OF COMPUTING (H-now) OR NOT?
NO
YES
S17
VERIFY THE ELECTRONIC SIGNATURE (TS-obj, SIG-1) FOR A DOCUMENT DIGEST VALUE (TS-obj, H-doc), TIME INFORMATION (TS-obj, T-fix), AND AN IDENTIFIER OF THE TIME STAMP SERVER (TS-obj, TISS-ID) IN THE TIME STAMP OBJECT (TS-obj) WITH THE SIGNATURE VERIFICATION PUBLIC KEY (K_{V1}) AND DETERMINE WHETHER THE RESULT OF VERIFICATION IS ACCEPTABLE OR NOT?
NO
YES
S18
THAT THE RESULT OF VARIFICATION HAS NOT CHANGED AFTER THE TIME STAMP WAS ISSUED IS DISPLAYED
S19
THAT THE RESULT OF VERIFICATION HAS CHANGED AFTER THE TIME STAMP WAS ISSUED IS DISPLAYED
END

04 JUL 2005

FIG. 5



04 JUL 2005

FIG. 6

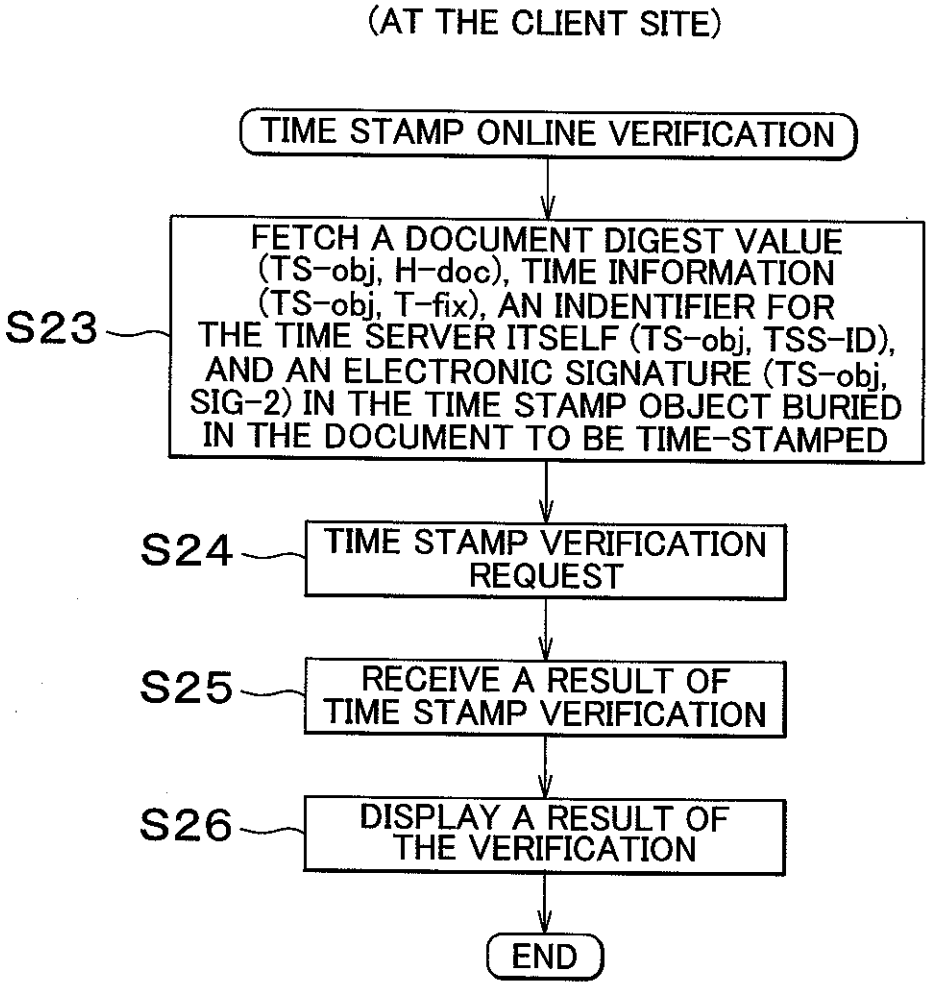


FIG. 7

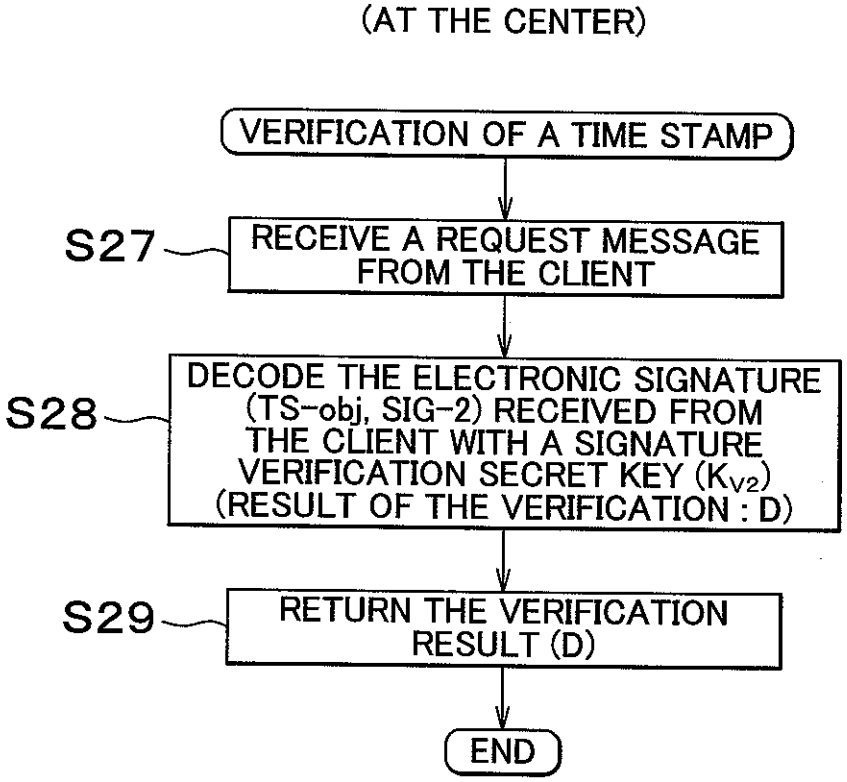
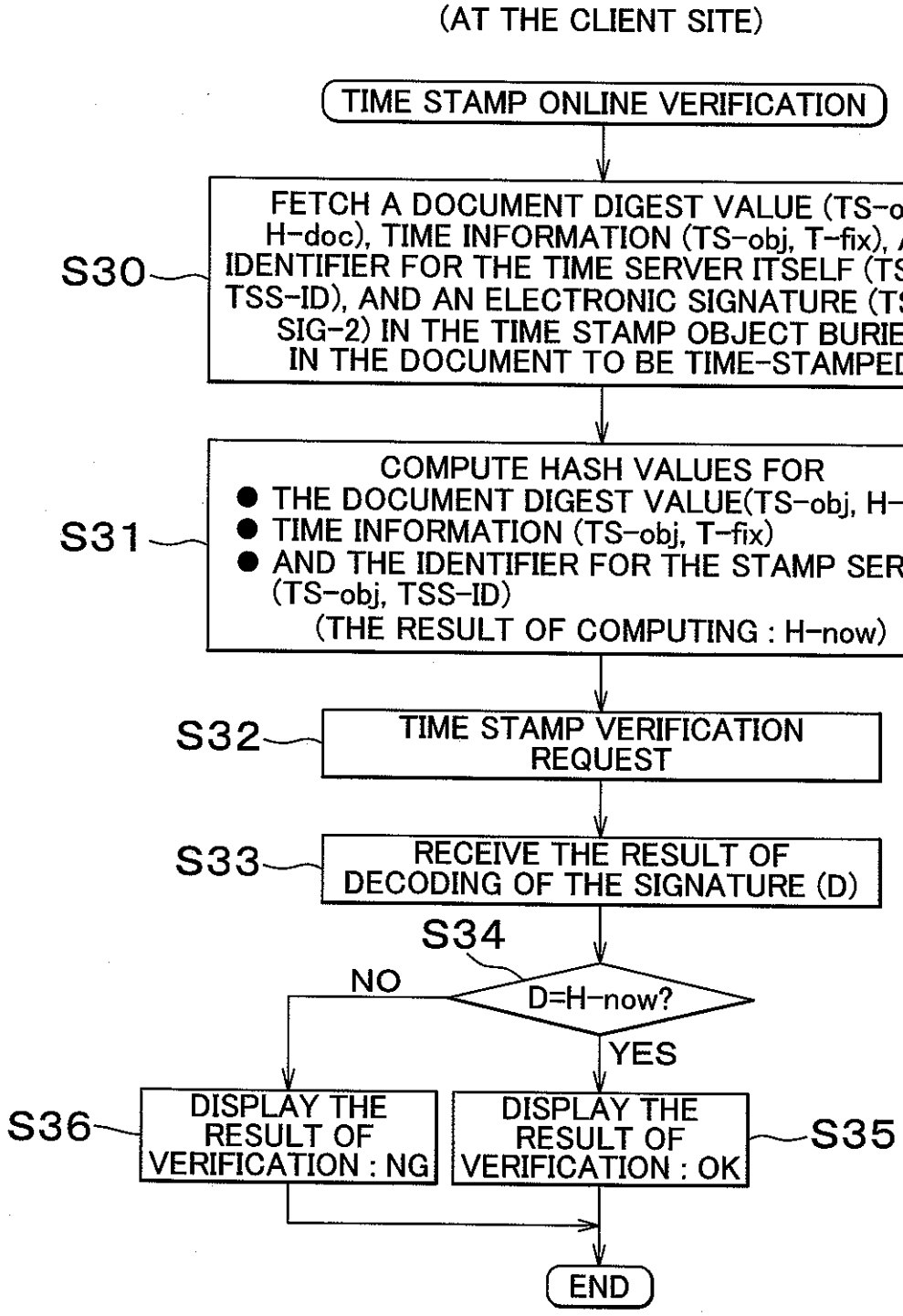

(AT THE CENTER)
VERIFICATION OF A TIME STAMP
S27
RECEIVE A REQUEST MESSAGE FROM THE CLIENT
S28
DECODE THE ELECTRONIC SIGNATURE (TS-obj, SIG-2) RECEIVED FROM THE CLIENT WITH A SIGNATURE VERIFICATION SECRET KEY (K_{V2}) (RESULT OF THE VERIFICATION : D)
S29
RETURN THE VERIFICATION RESULT (D)
END

FIG. 8


(AT THE CLIENT SITE)
TIME STAMP ONLINE VERIFICATION
S30
FETCH A DOCUMENT DIGEST VALUE (TS-obj, H-doc), TIME INFORMATION (TS-obj, T-fix), AN IDENTIFIER FOR THE TIME SERVER ITSELF (TS-obj, TSS-ID), AND AN ELECTRONIC SIGNATURE (TS-obj, SIG-2) IN THE TIME STAMP OBJECT BURIED IN THE DOCUMENT TO BE TIME-STAMPED
S31
COMPUTE HASH VALUES FOR
● THE DOCUMENT DIGEST VALUE(TS-obj, H-doc)
● TIME INFORMATION (TS-obj, T-fix)
● AND THE IDENTIFIER FOR THE STAMP SERVER (TS-obj, TSS-ID)
(THE RESULT OF COMPUTING : H-now)
S32
TIME STAMP VERIFICATION REQUEST
S33
RECEIVE THE RESULT OF DECODING OF THE SIGNATURE (D)
S34
D=H-now?
NO
YES
S36
DISPLAY THE RESULT OF VERIFICATION : NG
DISPLAY THE RESULT OF VERIFICATION : OK
S35
END

04 JUL 2005

FIG. 9

TIME STAMP DATA STRUCTURE

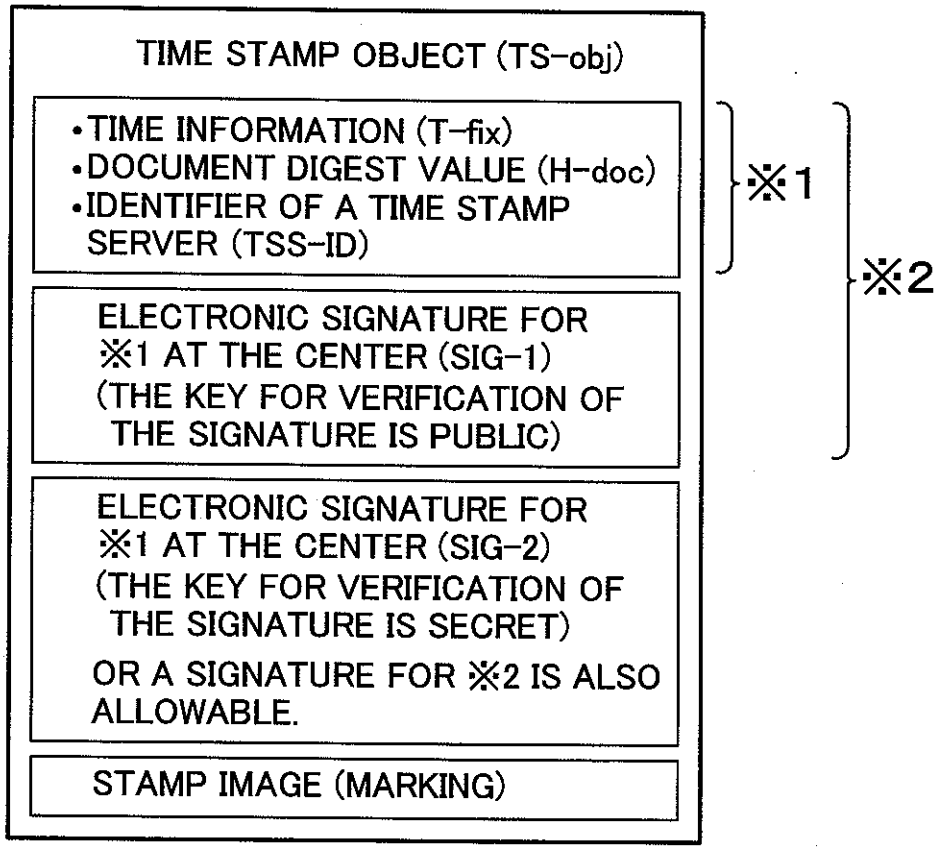
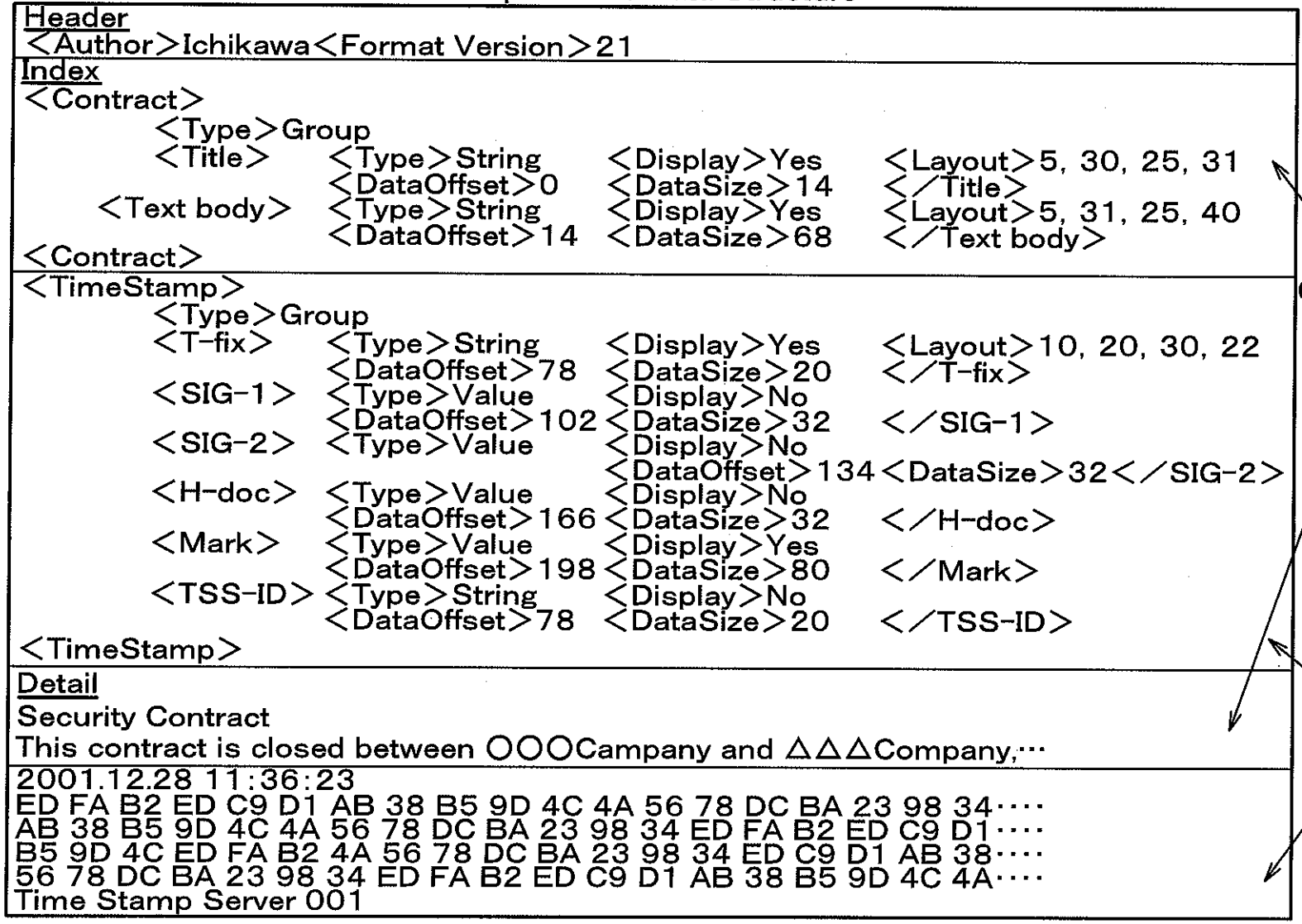


FIG. 10

Example of the Data Structure



04 JUL 2005