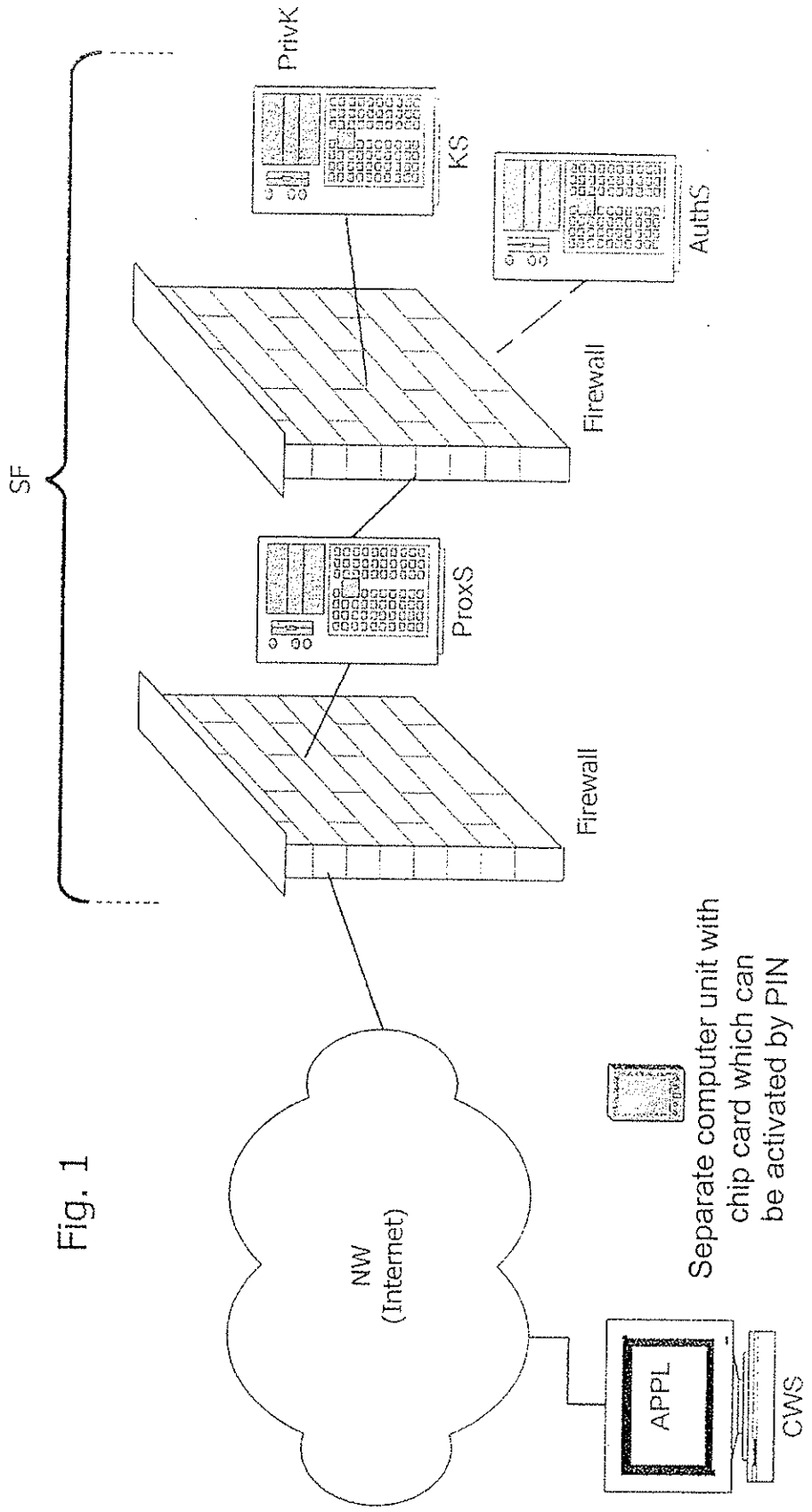

PrivK
KS
AuthS
Firewall
SF
ProxS
Firewall
NW
(Internet)
Separate computer unit with
chip card which can
be activated by PIN
APPL
CWS

Fig. 1

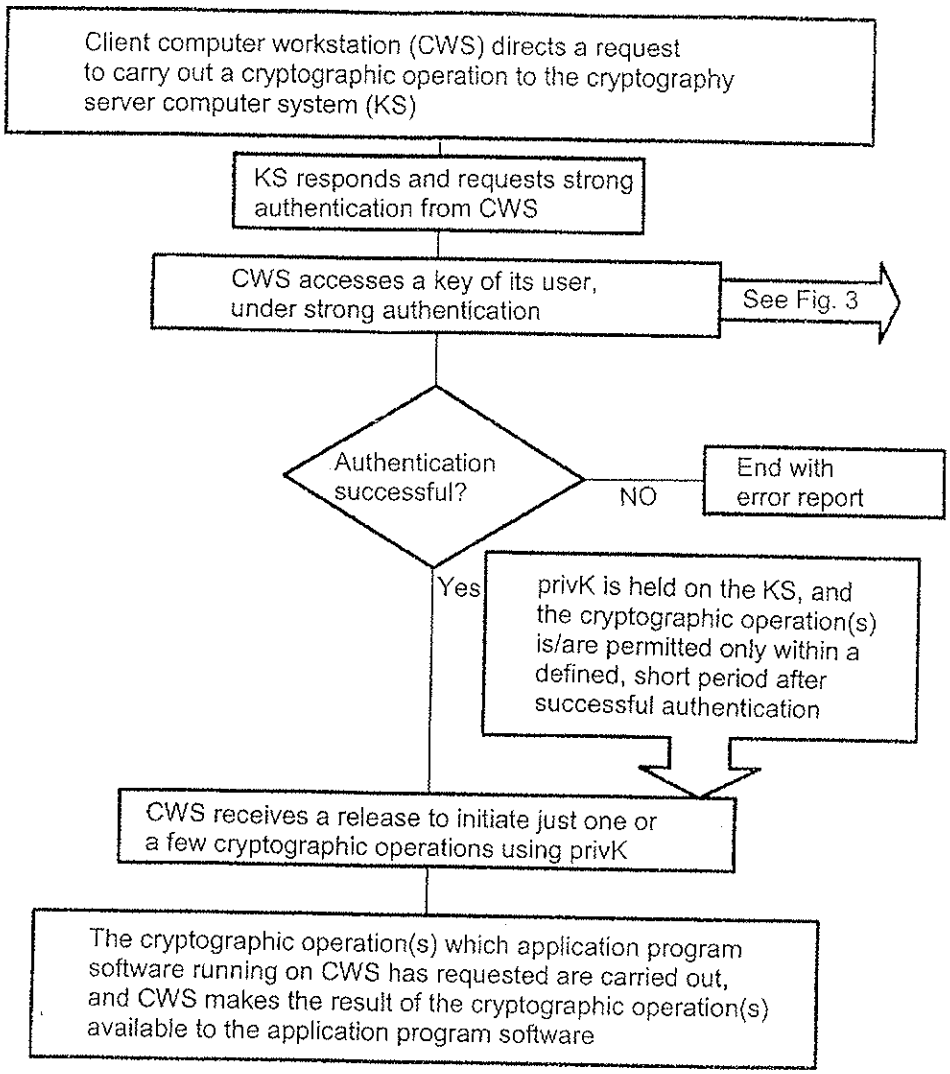

Client computer workstation (CWS) directs a request to carry out a cryptographic operation to the cryptography server computer system (KS)
KS responds and requests strong authentication from CWS
CWS accesses a key of its user, under strong authentication
See Fig. 3
Authentication successful?
NO
End with error report
Yes
privK is held on the KS, and the cryptographic operation(s) is/are permitted only within a defined, short period after successful authentication
CWS receives a release to initiate just one or a few cryptographic operations using privK
The cryptographic operation(s) which application program software running on CWS has requested are carried out, and CWS makes the result of the cryptographic operation(s) available to the application program software

Fig. 2

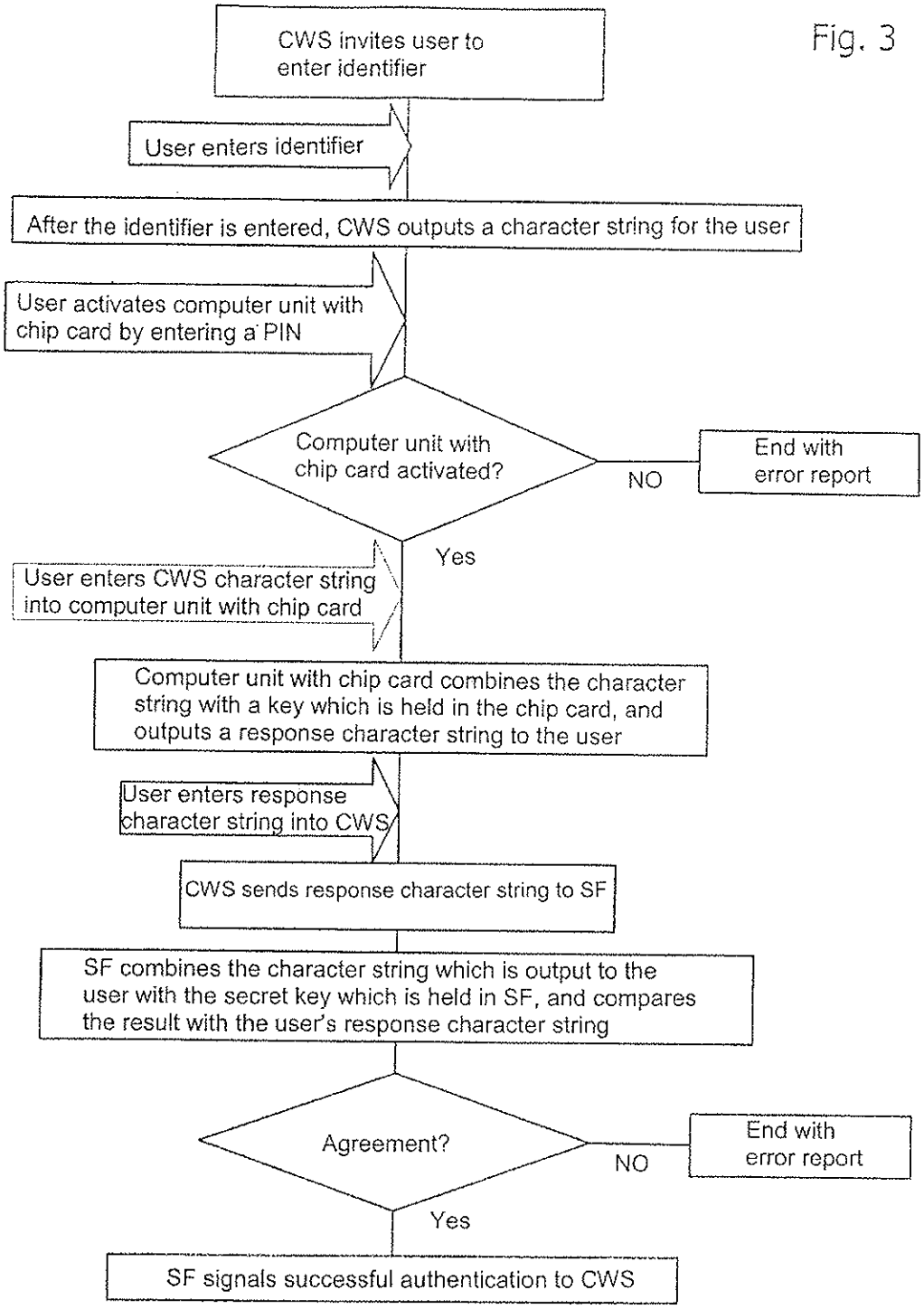
Fig. 2a

Cryptographic operations	
Signing a hash value	Decrypting a key
	Secret key
	Private key
	A/symmetrical key

Legitimation means used for strong authentication are
* Alpha/numeric character strings (4 to 20 characters)
* Valid for a short time (0.2 to 5 min)
* Valid only once
* Dynamically generated

Fig. 2b

Fig. 3


CWS invites user to enter identifier
User enters identifier
After the identifier is entered, CWS outputs a character string for the user
User activates computer unit with chip card by entering a PIN
Computer unit with chip card activated?
NO
End with error report
Yes
User enters CWS character string into computer unit with chip card
Computer unit with chip card combines the character string with a key which is held in the chip card, and outputs a response character string to the user
User enters response character string into CWS
CWS sends response character string to SF
SF combines the character string which is output to the user with the secret key which is held in SF, and compares the result with the user's response character string
Agreement?
NO
End with error report
Yes
SF signals successful authentication to CWS