

1/7

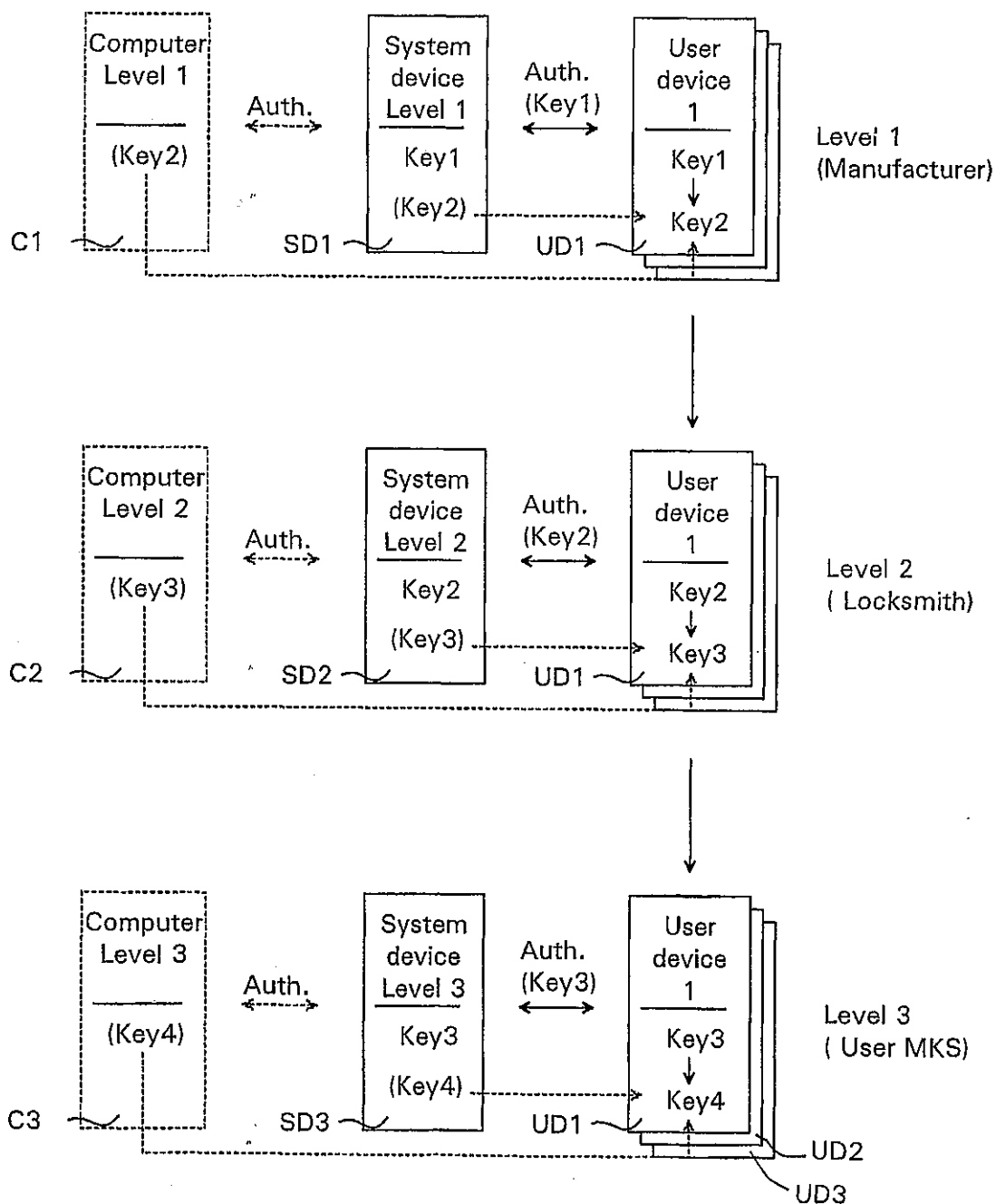


Fig. 1

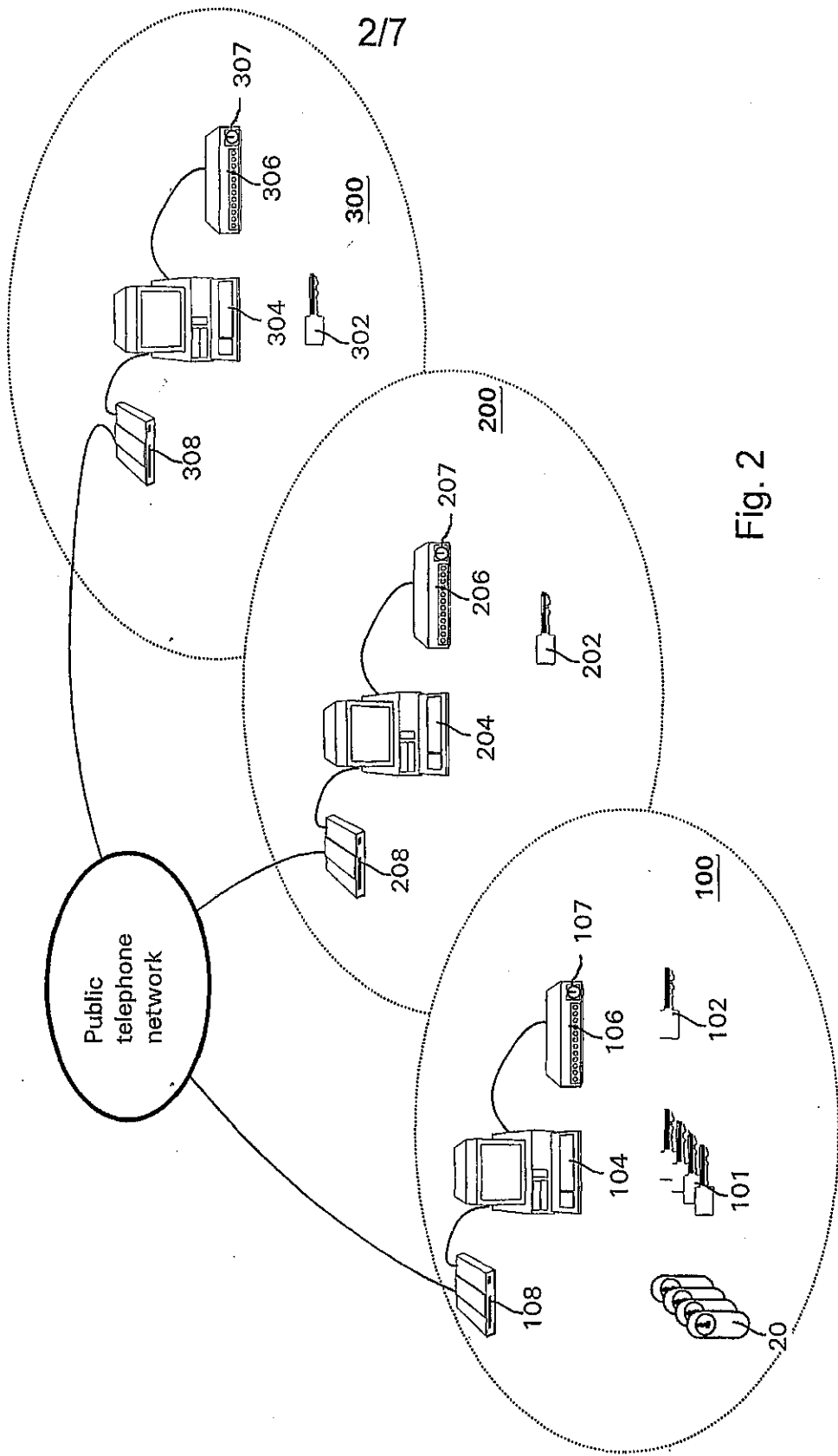


Fig. 2

3/7

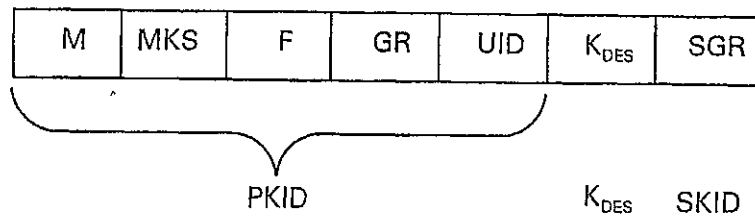


Fig. 3a

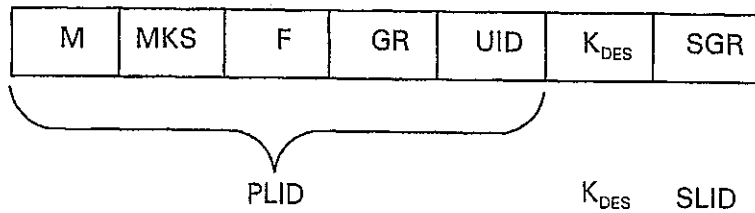
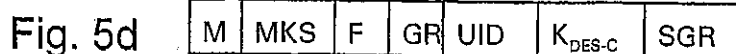
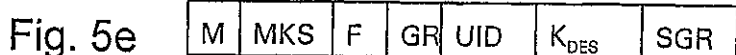


Fig. 3b



M-software

M-software
M-keyD-software
D-keyC-software
C-key

4/7

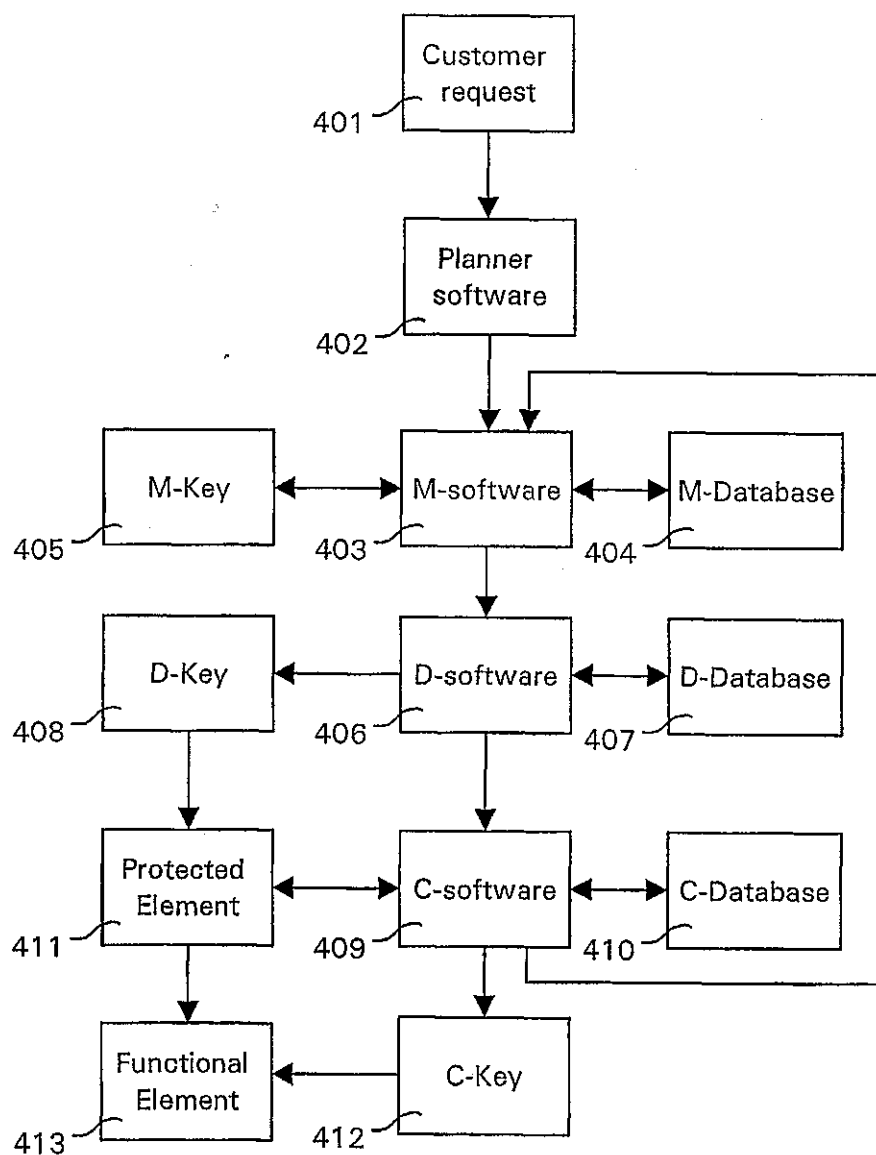


Fig. 4

5/7

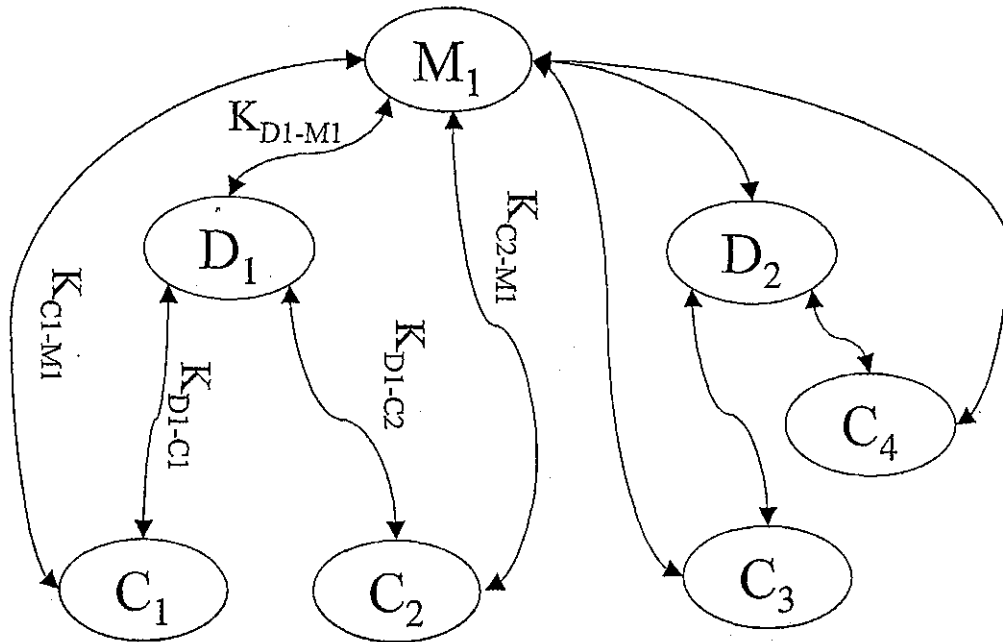


Fig. 6

6/7

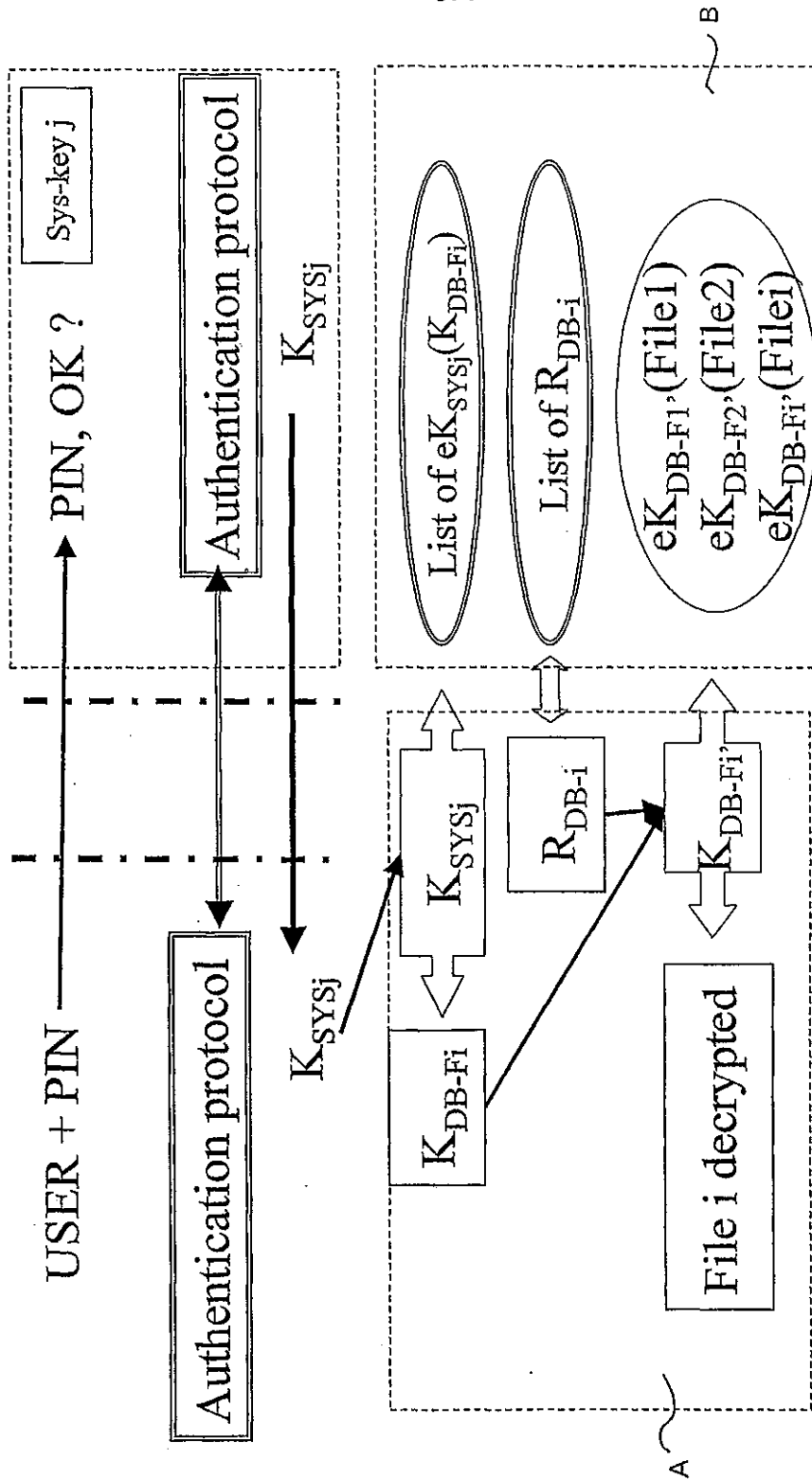


Fig. 7

	DB-file1	DB-file2	...	DB-filei
Sys-key1	$eeK_{SYS1}(K_{DB-F1})$	$eeK_{SYS1}(K_{DB-F2})$	...	$eeK_{SYS1}(K_{DB-Fi})$
Sys-key2	$eeK_{SYS2}(K_{DB-F1})$	$eeK_{SYS2}(K_{DB-F2})$	...	$eeK_{SYS2}(K_{DB-Fi})$
...	...	...	...	...
Sys-keyj	$eeK_{SYSj}(K_{DB-F1})$	$eeK_{SYSj}(K_{DB-F2})$	...	$eeK_{SYSj}(K_{DB-Fi})$

DB-file1	DB-file2	DB-filei
R_{DB-F1}	R_{DB-F2}	R_{DB-Fi}

Fig. 8