

Abbreviations

AES	Advanced Encryption Standard
APDU	application protocol data unit
ASCII	American Standard Code for Information Interchange
CBC	cipher block chaining
CEN	<i>Comité Européen de Normalisation</i>
CHV	cardholder verification
CLK	clock
CPU	Central processing unit
CS	chip select
CW	control words
DES	Data Encryption Standard
DSA	digital signature algorithm
DSS	Digital Signature Standard
ECB	electronic codebook
EEPROM	electrically erasable programmable read-only memory
EMV	Europay, MasterCard, Visa
ENG	enable gate
EPROM	erasable programmable read only memory
GND	ground
GSM	Global System for Mobile Communications
HEX	hexadecimal
I/O	input/output
I ² C	inter-integrated circuit
IDEA	international data encryption algorithm
IEC	International Electro-technical Commission
IEC	International Electro-technical Commission
ISO	International Organization for Standardization
NPU	numeric processing unit
OC	output control
OE	output enable
PC	personal computer
PIN	personal identification number
PUK	personal unblocking key

RAM	random-access memory
RF	radio frequency
RIPE-MD	RACE integrity primitives evaluation message digest
ROM	read-only memory
RSA	Rivest, Shamir and Adleman cryptographic algorithm
RST	reset
SCQL	structured card query language
SIM	subscriber identity module
SQL	structured query language
TS	technical specification
UICC	universal integrated circuit card
USIM	universal subscriber identity module
Vcc	supply voltage