

# ISO/IEC 7816-8:2019-08 (E)

## Identification cards - Integrated circuit cards - Part 8: Commands and mechanisms for security operations

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Abbreviated terms .....</b>	<b>2</b>
<b>5</b>	<b>Interindustry commands for security operations .....</b>	<b>3</b>
5.1	General .....	3
5.2	generate asymmetric key pair command .....	3
5.3	perform security operation command .....	7
5.3.1	General .....	7
5.3.2	compute cryptographic checksum operation .....	10
5.3.3	compute digital signature operation .....	10
5.3.4	hash operation .....	10
5.3.5	verify cryptographic checksum operation .....	11
5.3.6	verify digital signature operation .....	11
5.3.7	verify certificate operation .....	12
5.3.8	encipher operation .....	13
5.3.9	decipher operation .....	13
<b>Annex A (informative) Examples of operations related to digital signature .....</b>		<b>14</b>
<b>Annex B (informative) Examples of certificates interpreted by the card .....</b>		<b>20</b>
<b>Annex C (informative) Examples of asymmetric key transfer .....</b>		<b>24</b>
<b>Annex D (informative) Alternatives to achieve the reversible change of security context .....</b>		<b>27</b>
<b>Annex E (informative) Example of uses for generate asymmetric key pair command .....</b>		<b>29</b>
<b>Bibliography .....</b>		<b>35</b>