

# ISO/IEC 29167-11:2023-02 (E)

## Information technology - Automatic identification and data capture techniques - Part 11: Crypto suite PRESENT-80 security services for air interface communications

<b>Contents</b>		<b>Page</b>
<b>Foreword</b>		v
<b>Introduction</b>		vi
<b>1</b>	<b>Scope</b>	<b>1</b>
<b>2</b>	<b>Normative references</b>	<b>1</b>
<b>3</b>	<b>Terms, definitions, symbols and abbreviated terms</b>	<b>1</b>
	3.1 Terms and definitions	1
	3.2 Symbols	2
	3.3 Abbreviated terms	3
<b>4</b>	<b>Conformance</b>	<b>3</b>
	4.1 Air interface protocol specific information	3
	4.2 Interrogator conformance and requirements	3
	4.3 Tag conformance and requirements	3
<b>5</b>	<b>Introduction of the PRESENT-80 cryptographic suite</b>	<b>4</b>
<b>6</b>	<b>Parameter and variable definitions</b>	<b>4</b>
<b>7</b>	<b>Crypto suite state diagram</b>	<b>4</b>
<b>8</b>	<b>Initialization and resetting</b>	<b>5</b>
<b>9</b>	<b>Authentication</b>	<b>5</b>
	9.1 Introduction	5
	9.2 Message and response formatting	5
	9.3 Tag authentication: AuthMethod "00"	6
	9.3.1 General	6
	9.3.2 TAM1 message	6
	9.3.3 Intermediate Tag processing	7
	9.3.4 TAM1 response	8
	9.3.5 Final Interrogator processing	8
	9.4 Interrogator authentication: AuthMethod "01"	9
	9.4.1 General	9
	9.4.2 IAM1 message	9
	9.4.3 Intermediate Tag processing #1	9
	9.4.4 IAM1 response	10
	9.4.5 Intermediate Interrogator processing	10
	9.4.6 IAM2 message	10
	9.4.7 Intermediate Tag processing #2	10
	9.4.8 IAM2 response	11
	9.4.9 Final Interrogator processing	11
	9.5 Mutual authentication: AuthMethod "10"	11
	9.5.1 General	11
	9.5.2 MAM1 message	12
	9.5.3 Intermediate Tag processing #1	12
	9.5.4 MAM1 response	12
	9.5.5 Intermediate Interrogator processing	13
	9.5.6 MAM2 message	13
	9.5.7 Intermediate Tag processing #2	13
	9.5.8 MAM2 response	14
	9.5.9 Final Interrogator processing	14
<b>10</b>	<b>Communication</b>	<b>14</b>

<b>11</b>	<b>Key table and Key update</b>	<b>14</b>
<b>Annex A</b>	<b>(normative) Crypto suite state transition table</b>	<b>15</b>
<b>Annex B</b>	<b>(normative) Errors and error handling</b>	<b>16</b>
<b>Annex C</b>	<b>(informative) Description of PRESENT</b>	<b>17</b>
<b>Annex D</b>	<b>(informative) Test vectors</b>	<b>22</b>
<b>Annex E</b>	<b>(normative) Protocol specific information</b>	<b>24</b>
<b>Bibliography</b>		<b>27</b>