

# ISO/IEC 29167-17:2015-06 (E)

## Information technology - Automatic identification and data capture techniques - Part 17: Crypto suite crypt toGPS security services for air interface communications

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Conformance .....</b>	<b>1</b>
2.1	Claiming conformance .....	1
2.2	Interrogator conformance and obligations .....	1
2.3	Tag conformance and obligations .....	1
<b>3</b>	<b>Normative references .....</b>	<b>2</b>
<b>4</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>5</b>	<b>Symbols and abbreviated terms .....</b>	<b>5</b>
5.1	Symbols .....	5
5.2	Abbreviated terms .....	6
<b>6</b>	<b>Cipher introduction .....</b>	<b>6</b>
<b>7</b>	<b>Parameter definitions .....</b>	<b>7</b>
<b>8</b>	<b>State diagram .....</b>	<b>8</b>
<b>9</b>	<b>Initialization and resetting .....</b>	<b>8</b>
<b>10</b>	<b>Authentication .....</b>	<b>9</b>
10.1	Introduction .....	9
10.2	Tag authentication: CCR variant (Method "00" = TAM1) .....	10
10.3	Tag authentication: NTS variant (Method "01" = TAM2) .....	12
10.3.1	CCR variant (Method "00" = TAM1) .....	15
10.3.2	NTS variant (Method "01" = TAM2) .....	19
<b>11</b>	<b>Communication .....</b>	<b>23</b>
<b>12</b>	<b>Key table and key update .....</b>	<b>23</b>
<b>Annex A (normative) State transition tables .....</b>		<b>24</b>
<b>Annex B (normative) Error codes and error handling .....</b>		<b>25</b>
<b>Annex C (normative) Cipher description .....</b>		<b>27</b>
<b>Annex D (informative) Test vectors .....</b>		<b>28</b>
<b>Annex E (normative) Protocol specific .....</b>		<b>35</b>
<b>Bibliography .....</b>		<b>38</b>