

# ISO/IEC 9797-2:2002-06 (E)

## Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

---

<b>Contents</b>		<b>Page</b>
<b>1</b>	<b>Scope 1 2 Normative references 1 3 Terms and definitions 1 4 Symbols and notation 2 5 Requirements 3 6 MAC Algorithm 1 3 6.1 Description of MAC Algorithm 1 .....</b>	<b>4</b>
<b>6.1.1</b>	<b>Step 1 (key expansion) .....</b>	<b>4</b>
<b>6.1.2</b>	<b>Step 2 (modification of the constants and the IV ) .....</b>	<b>4</b>
<b>6.1.3</b>	<b>Step 3 (hashing operation) .....</b>	<b>4</b>
<b>6.1.4</b>	<b>Step 4 (output transformation) .....</b>	<b>4</b>
<b>6.1.5</b>	<b>Step 5 (truncation) .....</b>	<b>4</b>
<b>6.2</b>	<b>Efficiency .....</b>	<b>4</b>
<b>6.3</b>	<b>Computation of the constants .....</b>	<b>4</b>
<b>6.3.1</b>	<b>Dedicated Hash-Function 1 .....</b>	<b>5</b>
<b>6.3.2</b>	<b>Dedicated Hash-Function 2 .....</b>	<b>5</b>
<b>6.3.3</b>	<b>Dedicated Hash-Function 3 .....</b>	<b>5</b>
<b>7</b>	<b>MAC Algorithm 2 5 7.1 Description of MAC Algorithm 2 .....</b>	<b>6</b>
<b>7.1.1</b>	<b>Step 1 (key expansion) .....</b>	<b>6</b>
<b>7.1.2</b>	<b>Step 2 (hashing operation) .....</b>	<b>6</b>
<b>7.1.3</b>	<b>Step 3 (output transformation) .....</b>	<b>6</b>
<b>7.1.4</b>	<b>Step 4 (truncation) .....</b>	<b>6</b>
<b>7.2</b>	<b>Efficiency .....</b>	<b>6</b>
<b>8</b>	<b>MAC Algorithm 3 6 8.1 Description of MAC Algorithm 3 .....</b>	<b>6</b>
<b>8.1.1</b>	<b>Step 1 (key expansion) .....</b>	<b>6</b>
<b>8.1.2</b>	<b>Step 2 (modification of the constants and the IV ) .....</b>	<b>7</b>
<b>8.1.3</b>	<b>Step 3 (padding) .....</b>	<b>7</b>
<b>8.1.4</b>	<b>Step 4 (application of the round-function) .....</b>	<b>7</b>
<b>8.1.5</b>	<b>Step 5 (truncation) .....</b>	<b>7</b>
<b>8.2</b>	<b>Efficiency .....</b>	<b>7</b>