

# ISO/IEC TR 21000-11:2004-11 (E)

## Information technology - Multimedia framework (MPEG-21) - Part 11: Evaluation Tools for Persistent Association Technologies

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vii
<b>1</b>	<b>Scope .....</b>	<b>1</b>
1.1	Introduction .....	1
1.3	Organisation of the Document .....	1
<b>2</b>	<b>Terms and Abbreviations .....</b>	<b>2</b>
2.1	Terms and Definitions .....	2
2.1.1	Computational Performance .....	2
2.1.2	Fingerprinting .....	2
2.1.3	Impairment .....	2
2.1.4	Perceptibility .....	3
2.1.5	Persistent Association .....	3
2.1.6	Persistent Association Tool .....	3
2.1.7	PAT Evaluation Configuration .....	3
2.1.8	Robustness .....	3
2.1.9	Survivability .....	3
2.1.10	Watermarking .....	4
2.1.11	Feature Extraction .....	4
2.2	Terms not used in this Technical Report .....	4
2.3	Abbreviations .....	4
<b>3</b>	<b>(Persistent) Association Technologies .....</b>	<b>4</b>
3.1	Introduction .....	4
3.2	Headers .....	5
3.3	Digital Signatures .....	6
3.4	Fingerprinting .....	7
3.5	Watermarking .....	8
<b>4</b>	<b>Use Cases for Persistent Association .....</b>	<b>9</b>
4.1	Introduction .....	9
4.2	Rights and Content Management .....	9
4.3	Audio Content Tracking and Reporting .....	9
4.4	Internet Audio Content Services .....	9
4.5	Anti-Piracy Investigation and Enforcement .....	9
4.6	Authentication and Integrity .....	10
4.7	Value Added Services .....	10
<b>5</b>	<b>Considerations for the Evaluation of Persistent Association Tools .....</b>	<b>10</b>
<b>6</b>	<b>Characteristic Parameters of Persistent Association Technologies .....</b>	<b>11</b>
6.1	Introduction .....	11
6.2	Fingerprint Size .....	11
6.3	Watermark Payload .....	12
6.4	Granularity .....	12
6.5	Perceptibility .....	12
6.6	Robustness .....	13
6.7	Reliability .....	13
6.8	Computational Performance .....	14

<b>7</b>	<b>Issues in Persistent Association</b>	<b>15</b>
<b>7.1</b>	<b>Robustness to Malicious Attacks</b>	<b>16</b>
<b>7.1.1</b>	<b>Impairment Attacks</b>	<b>16</b>
<b>7.1.2</b>	<b>Synchronisation Attacks</b>	<b>16</b>
<b>7.1.3</b>	<b>Cryptographic Factors</b>	<b>16</b>
<b>7.2</b>	<b>Scalability</b>	<b>17</b>
<b>7.2.1</b>	<b>Scalability of Fingerprinting</b>	<b>17</b>
<b>7.2.2</b>	<b>Scalability of Watermarking</b>	<b>18</b>
<b>7.3</b>	<b>Interactions</b>	<b>18</b>
<b>8</b>	<b>Evaluation Methods for Persistent Association Technologies</b>	<b>18</b>
<b>8.1</b>	<b>Introduction</b>	<b>18</b>
<b>8.2</b>	<b>Generic Framework and Methodology for Evaluation of PAT</b>	<b>18</b>
<b>8.3</b>	<b>PAT Evaluation Configuration</b>	<b>20</b>
<b>8.4</b>	<b>Generic PAT Evaluation Process</b>	<b>20</b>
<b>8.5</b>	<b>Evaluation of Reliability</b>	<b>21</b>
<b>8.6</b>	<b>Evaluation of Perceptibility</b>	<b>22</b>
<b>8.7</b>	<b>Evaluation of Payload/Size</b>	<b>23</b>
<b>8.8</b>	<b>Evaluation of Robustness</b>	<b>24</b>
<b>8.9</b>	<b>Evaluation of Granularity</b>	<b>25</b>
<b>8.10</b>	<b>Evaluation of Computational Performance</b>	<b>26</b>
<b>8.11</b>	<b>Automation of Evaluations</b>	<b>27</b>
	<b>Bibliography</b>	<b>31</b>