

# ISO/IEC TR 15443-1:2012-11 (E)

## Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts

---

Contents	Page
<b>Foreword .....</b>	<b>v</b>
<b>Introduction .....</b>	<b>vi</b>
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Abbreviated Terms .....</b>	<b>6</b>
<b>5 Concepts of security assurance .....</b>	<b>8</b>
<b>5.1 Security assurance .....</b>	<b>8</b>
<b>5.2 Assurance is distinguishable from confidence .....</b>	<b>9</b>
<b>5.3 The need for security assurance .....</b>	<b>9</b>
<b>5.4 Security assurance is intangible .....</b>	<b>10</b>
<b>5.5 Security assurance reduces security risk .....</b>	<b>10</b>
<b>5.6 Security assurance provided is related to the effort expended .....</b>	<b>10</b>
<b>5.7 Security assurance does not improve the product .....</b>	<b>11</b>
<b>5.8 Security assurance stakeholders .....</b>	<b>11</b>
<b>5.8.1 Those requiring confidence in SACA results .....</b>	<b>11</b>
<b>5.8.2 Approval and assurance authorities .....</b>	<b>11</b>
<b>5.9 Security assurance pervasiveness .....</b>	<b>12</b>
<b>5.9.1 Pass-through security assurance .....</b>	<b>14</b>
<b>5.9.2 Boundaries of deliverables .....</b>	<b>14</b>
<b>5.9.3 Transfer of deliverables .....</b>	<b>18</b>
<b>5.10 Organisational aspects of SACA .....</b>	<b>18</b>
<b>6 The structure of security assurance .....</b>	<b>19</b>
<b>6.1 Security assurance requirements specification .....</b>	<b>20</b>
<b>6.2 Security assurance cases .....</b>	<b>20</b>
<b>6.2.1 Developing a security assurance case .....</b>	<b>21</b>
<b>6.2.2 Communicating a security assurance case .....</b>	<b>21</b>
<b>6.3 Security assurance evidence .....</b>	<b>21</b>
<b>6.4 Security assurance claims .....</b>	<b>21</b>
<b>6.5 Security assurance arguments .....</b>	<b>22</b>
<b>7 SACA techniques .....</b>	<b>23</b>
<b>7.1 Techniques .....</b>	<b>23</b>
<b>7.1.1 Effectiveness (or evaluation) .....</b>	<b>24</b>
<b>7.1.2 Correctness (or conformance) .....</b>	<b>24</b>
<b>7.1.3 Predictive assurance .....</b>	<b>24</b>
<b>7.2 Selecting security assurance techniques .....</b>	<b>24</b>
<b>7.2.1 Optimisation considerations .....</b>	<b>25</b>
<b>8 SACA methods .....</b>	<b>26</b>
<b>8.1 Security Assurance Conformity Assessment (SACA) Methods .....</b>	<b>26</b>
<b>8.1.2 The composition of a security assurance conformance assessment method .....</b>	<b>27</b>
<b>8.1.3 Methods specific to security assurance .....</b>	<b>28</b>
<b>8.1.4 Methods not specific to security assurance .....</b>	<b>29</b>

<b>8.2</b>	<b>Approaches of SACA methods .....</b>	<b>29</b>
8.2.1	Approach types .....	29
8.2.2	Combining approaches .....	30
8.3	Coverage of life cycle phases .....	31
8.3.1	Security assurance conformity assessors .....	32
8.3.2	Efficiency of a SACA method .....	32
8.4	The relationship between security criteria and assessment methods .....	33
8.5	Security assurance ratings .....	33
8.6	SACA tools .....	34
8.7	Outputs from the application of SACA methods .....	34
<b>9</b>	<b>CASCO .....</b>	<b>35</b>
9.1	Standards supporting conformity assessment .....	35
<b>10</b>	<b>SACA Paradigms .....</b>	<b>36</b>
10.1	SACA schemes .....	36
10.2	SACA conformity assessment bodies .....	37
10.2.1	Type A conformity assessments .....	37
10.2.2	Second party conformity assessment bodies .....	37
10.2.3	Third party conformity assessment bodies .....	38
10.3	Example models of SACA paradigms .....	38
10.3.1	Common Criteria .....	38
10.3.2	The Cryptographic Module Validation Program (CMVP) .....	39
10.3.3	The Payment Card Industry .....	40
<b>11</b>	<b>Aspects of the composition of security assurance .....</b>	<b>41</b>
11.1	Developing an assurance case in a compositional setting .....	42
11.1.1	General problems of composition .....	43
11.1.2	General aspects of composition re-use .....	43
11.1.3	Composition using different assurance techniques .....	44
11.2	Types of composition .....	44
11.2.1	Layering .....	44
11.2.2	Network .....	46
11.2.3	Component .....	48
11.3	Further activities .....	49
<b>Bibliography .....</b>	<b>50</b>	