IEC 62541-7

Edition 3.0 2020-06
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

OPC unified architecture – Part 7: Profiles

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-8562-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 12
1 Scope 15
2 Normative references 15
3 Terms, definitions, and ~~conventions~~ abbreviated terms 16
3.1 Terms and definitions 16
3.2 Abbreviated terms 17
4 Overview 17
4.1 General 17
4.2 ConformanceUnit 18
4.3 Profiles 18
4.4 Profile Categories 19
5 Conformance Units 19
5.1 Overview 19
5.2 Services 20
5.3 Transport and communication related features 30
5.4 Information Model and AddressSpace related features 42
5.5 Miscellaneous 62
6 Profiles 64
6.1 Overview 64
6.2 Profile list 64
6.3 Conventions for Profile definitions 71
6.4 Profile versioning 71
6.5 Applications 71
6.6 Profile tables 73
6.6.1 General 73
6.6.2 Core Server Facet 73
6.6.3 Core 2017 Server Facet 73
6.6.4 Sessionless Server Facet 74
6.6.5 Reverse Connect Server Facet 75
6.6.6 Base Server Behaviour Facet 75
6.6.7 Request State Change Server Facet 75
6.6.8 Subnet Discovery Server Facet 75
6.6.9 Global Certificate Management Server Facet 76
6.6.10 Authorization Service Server Facet 76
6.6.11 KeyCredential Service Server Facet 76
6.6.12 Attribute WriteMask Server Facet 76
6.6.13 File Access Server Facet 77
6.6.14 Documentation Server Facet 77
6.6.15 Embedded DataChange Subscription Server Facet 77
6.6.16 Standard DataChange Subscription Server Facet 78
6.6.17 Standard DataChange Subscription 2017 Server Facet 78
6.6.18 Enhanced DataChange Subscription Server Facet 78
6.6.19 Enhanced DataChange Subscription 2017 Server Facet 78
6.6.20 Durable Subscription Server Facet 79
6.6.21 Data Access Server Facet 79
6.6.22 ComplexType Server Facet 79

6.6.23 ComplexType 2017 Server Facet 80
6.6.24 Standard Event Subscription Server Facet 80
6.6.25 Address Space Notifier Server Facet 81
6.6.26 A & C Base Condition Server Facet 81
6.6.27 A & C Refresh2 Server Facet 82
6.6.28 A & C Address Space Instance Server Facet 82
6.6.29 A & C Enable Server Facet 82
6.6.30 A & C AlarmMetrics Server Facet 82
6.6.31 A & C Alarm Server Facet 83
6.6.32 A & C Acknowledgeable Alarm Server Facet 83
6.6.33 A & C Exclusive Alarming Server Facet 84
6.6.34 A & C Non-Exclusive Alarming Server Facet 84
6.6.35 A & C Previous Instances Server Facet 84
6.6.36 A & C Dialog Server Facet 85
6.6.37 A & C CertificateExpiration Server Facet 85
6.6.38 A & E Wrapper Facet 85
6.6.39 Method Server Facet 86
6.6.40 Auditing Server Facet 86
6.6.41 Node Management Server Facet 87
6.6.42 User Role Base Server Facet 87
6.6.43 User Role Management Server Facet 87
6.6.44 State Machine Server Facet 88
6.6.45 Client Redundancy Server Facet 88
6.6.46 Redundancy Transparent Server Facet 88
6.6.47 Redundancy Visible Server Facet 89
6.6.48 Historical Raw Data Server Facet 89
6.6.49 Historical Aggregate Server Facet 89
6.6.50 Historical Data AtTime Server Facet 90
6.6.51 Historical Access Modified Data Server Facet 91
6.6.52 Historical Annotation Server Facet 91
6.6.53 Historical Data Insert Server Facet 91
6.6.54 Historical Data Update Server Facet 91
6.6.55 Historical Data Replace Server Facet 92
6.6.56 Historical Data Delete Server Facet 92
6.6.57 Historical Access Structured Data Server Facet 92
6.6.58 Base Historical Event Server Facet 92
6.6.59 Historical Event Update Server Facet 93
6.6.60 Historical Event Replace Server Facet 93
6.6.61 Historical Event Insert Server Facet 93
6.6.62 Historical Event Delete Server Facet 93
6.6.63 Aggregate Subscription Server Facet 94
6.6.64 Nano Embedded Device Server Profile 95
6.6.65 Nano Embedded Device 2017 Server Profile 95
6.6.66 Micro Embedded Device Server Profile 95
6.6.67 Micro Embedded Device 2017 Server Profile 95
6.6.68 Embedded UA Server Profile 95
6.6.69 Embedded 2017 UA Server Profile 96
6.6.70 Standard UA Server Profile 96
6.6.71 Standard 2017 UA Server Profile 96

6.6.72 Core Client Facet 97
6.6.73 Core 2017 Client Facet 97
6.6.74 Sessionless Client Facet 98
6.6.75 Reverse Connect Client Facet 98
6.6.76 Base Client Behaviour Facet 98
6.6.77 Discovery Client Facet 98
6.6.78 Subnet Discovery Client Facet 99
6.6.79 Global Discovery Client Facet 99
6.6.80 Global Certificate Management Client Facet 99
6.6.81 KeyCredential Service Client Facet 99
6.6.82 Access Token Request Client Facet 100
6.6.83 AddressSpace Lookup Client Facet 100
6.6.84 Request State Change Client Facet 100
6.6.85 File Access Client Facet 101
6.6.86 Entry-Level Support 2015 Client Facet 101
6.6.87 Multi-Server Client Connection Facet 101
6.6.88 Documentation – Client 101
6.6.89 Attribute Read Client Facet 102
6.6.90 Attribute Write Client Facet 102
6.6.91 DataChange Subscriber Client Facet 102
6.6.92 Durable Subscription Client Facet 103
6.6.93 DataAccess Client Facet 103
6.6.94 Event Subscriber Client Facet 104
6.6.95 Base Event Processing Client Facet 104
6.6.96 Notifier and Source Hierarchy Client Facet 105
6.6.97 A & C Base Condition Client Facet 105
6.6.98 A & C Refresh2 Client Facet 105
6.6.99 A & C Address Space Instance Client Facet 106
6.6.100 A & C Enable Client Facet 106
6.6.101 A & C AlarmMetrics Client Facet 106
6.6.102 A & C Alarm Client Facet 106
6.6.103 A & C Exclusive Alarming Client Facet 107
6.6.104 A & C Non-Exclusive Alarming Client Facet 107
6.6.105 A & C Previous Instances Client Facet 108
6.6.106 A & C Dialog Client Facet 108
6.6.107 A & C CertificateExpiration Client Facet 108
6.6.108 A & E Proxy Facet 109
6.6.109 Method Client Facet 110
6.6.110 Auditing Client Facet 110
6.6.111 Node Management Client Facet 110
6.6.112 Advanced Type Programming Client Facet 110
6.6.113 User Role Management Client Facet 111
6.6.114 State Machine Client Facet 111
6.6.115 Diagnostic Client Facet 111
6.6.116 Redundant Client Facet 112
6.6.117 Redundancy Switch Client Facet 112
6.6.118 Historical Access Client Facet 112
6.6.119 Historical Data AtTime Client Facet 112
6.6.120 Historical Aggregate Client Facet 112

6.6.121 Historical Annotation Client Facet 114
6.6.122 Historical Access Modified Data Client Facet 114
6.6.123 Historical Data Insert Client Facet 114
6.6.124 Historical Data Update Client Facet 114
6.6.125 Historical Data Replace Client Facet 114
6.6.126 Historical Data Delete Client Facet 115
6.6.127 Historical Access Client Server Timestamp Facet 115
6.6.128 Historical Structured Data Access Client Facet 115
6.6.129 Historical Structured Data AtTime Client Facet 115
6.6.130 Historical Structured Data Modified Client Facet 116
6.6.131 Historical Structured Data Insert Client Facet 116
6.6.132 Historical Structured Data Update Client Facet 116
6.6.133 Historical Structured Data Replace Client Facet 116
6.6.134 Historical Structured Data Delete Client Facet 116
6.6.135 Historical Events Client Facet 117
6.6.136 Historical Event Insert Client Facet 117
6.6.137 Historical Event Update Client Facet 117
6.6.138 Historical Event Replace Client Facet 117
6.6.139 Historical Event Delete Client Facet 118
6.6.140 Aggregate Subscriber Client Facet 118
6.6.141 Standard UA Client Profile 119
6.6.142 Standard UA Client 2017 Profile 119
6.6.143 UA-TCP UA-SC UA-Binary 120
6.6.144 HTTPS UA-Binary 120
6.6.145 HTTPS UA-XML 121
~~SOAP-HTTP WS-SC UA XML ..... ~~
~~SOAP-HTTP WS-SC UA Binary ..... ~~
~~SOAP-HTTP WS-SC UA XML-UA Binary ..... ~~
6.6.146 HTTPS UA-JSON 121
6.6.147 WSS UA-SC UA-Binary 122
6.6.148 WSS UA-JSON 122
6.6.149 Security User Access Control Full 122
6.6.150 Security User Access Control Base 123
6.6.151 Security Time Synchronization 123
6.6.152 Best Practice – Audit Events 123
6.6.153 Best Practice – Alarm Handling 123
6.6.154 Best Practice – Random Numbers 124
6.6.155 Best Practice – Timeouts 124
6.6.156 Best Practice – Administrative Access 124
6.6.157 Best Practice – Strict Message Handling 124
6.6.158 Best Practice – Audit Events Client 125
~~TransportSecurity – TLS 1.0 ..... ~~
~~TransportSecurity – TLS 1.1 ..... ~~
6.6.159 TransportSecurity – TLS 1.2 126
6.6.160 TransportSecurity – TLS 1.2 with PFS 126
6.6.161 SecurityPolicy – None 126
6.6.162 SecurityPolicy – Basic128Rsa15 127
6.6.163 SecurityPolicy – Basic256 127
6.6.164 SecurityPolicy [A] – Aes128-Sha256-RsaOaep 128

6.6.165 SecurityPolicy [B] – Basic256Sha256 128
6.6.166 SecurityPolicy – Aes256-Sha256-RsaPss 129
6.6.167 User Token – Anonymous Facet 129
6.6.168 User Token – User Name Password Server Facet 130
6.6.169 User Token – X509 Certificate Server Facet 130
6.6.170 User Token – Issued Token Server Facet 130
6.6.171 User Token – Issued Token Windows Server Facet 130
6.6.172 User Token – JWT Server Facet 131
6.6.173 User Token – User Name Password Client Facet 131
6.6.174 User Token – X509 Certificate Client Facet 131
6.6.175 User Token – Issued Token Client Facet 131
6.6.176 User Token – Issued Token Windows Client Facet 131
6.6.177 User Token – JWT Client Facet 132
6.6.178 Global Discovery Server Profile 132
6.6.179 Global Discovery Server 2017 Profile 132
6.6.180 Global Discovery and Certificate Management Server 132
6.6.181 Global Discovery and Certificate Mgmt 2017 Server 133
6.6.182 Global Certificate Management Client Profile 133
6.6.183 Global Certificate Management Client 2017 Profile 133
6.6.184 Global Service Authorization Request Server Facet 133
6.6.185 Global Service KeyCredential Pull Facet 134
6.6.186 Global Service KeyCredential Push Facet 134
Bibliography 135

Figure 1 – Profile – ConformanceUnit – TestCases 18
Figure 2 – HMI Client sample 72
Figure 3 – Embedded Server sample 72
Figure 4 – Standard UA Server sample 73

Table 1 – Profile Categories 19
Table 2 – Conformance Groups 20
Table 3 – Discovery Services 21
Table 4 – Session Services 22
Table 5 – Node Management Services 24
Table 6 – View Services 24
Table 7 – Attribute Services 25
Table 8 – Method Services 26
Table 9 – Monitored Item Services 27
Table 10 – Subscription Services 29
Table 11 – Security 31
Table 12 – Protocol and Encoding 42
Table 13 – Base Information 43
Table 14 – Address Space Model 46
Table 15 – Data Access 48
Table 16 – Alarms and Conditions 49
Table 17 – Historical Access 52

Table 18 – Aggregates 55
Table 19 – Auditing 61
Table 20 – Redundancy 61
Table 21 – Global Discovery Server 62
Table 22 – Miscellaneous 63
Table 23 – Profile list 65
Table 24 – Core 2017 Server Facet 74
Table 25 – Sessionless Server Facet 74
Table 26 – Reverse Connect Server Facet 75
Table 27 – Base Server Behaviour Facet 75
Table 28 – Request State Change Server Facet 75
Table 29 – Subnet Discovery Server Facet 75
Table 30 – Global Certificate Management Server Facet 76
Table 31 – Authorization Service Server Facet 76
Table 32 – KeyCredential Service Server Facet 76
Table 33 – Attribute WriteMask Server Facet 76
Table 34 – File Access Server Facet 77
Table 35 – Documentation Server Facet 77
Table 36 – Embedded DataChange Subscription Server Facet 77
Table 37 – Standard DataChange Subscription 2017 Server Facet 78
Table 38 – Enhanced DataChange Subscription 2017 Server Facet 79
Table 39 – Durable Subscription Server Facet 79
Table 40 – Data Access Server Facet 79
Table 41 – ComplexType 2017 Server Facet 80
Table 42 – Standard Event Subscription Server Facet 81
Table 43 – Address Space Notifier Server Facet 81
Table 44 – A & C Base Condition Server Facet 82
Table 45 – A & C Refresh2 Server Facet 82
Table 46 – A & C Address Space Instance Server Facet 82
Table 47 – A & C Enable Server Facet 82
Table 48 – A & C AlarmMetrics Server Facet 83
Table 49 – A & C Alarm Server Facet 83
Table 50 – A & C Acknowledgeable Alarm Server Facet 84
Table 51 – A & C Exclusive Alarming Server Facet 84
Table 52 – A & C Non-Exclusive Alarming Server Facet 84
Table 53 – A & C Previous Instances Server Facet 85
Table 54 – A & C Dialog Server Facet 85
Table 55 – A & C CertificateExpiration Server Facet 85
Table 56 – A & E Wrapper Facet 86
Table 57 – Method Server Facet 86
Table 58 – Auditing Server Facet 87
Table 59 – Node Management Server Facet 87
Table 60 – User Role Base Server Facet 87

Table 61 – User Role Management Server Facet 88
Table 62 – State Machine Server Facet 88
Table 63 – Client Redundancy Server Facet 88
Table 64 – Redundancy Transparent Server Facet 88
Table 65 – Redundancy Visible Server Facet 89
Table 66 – Historical Raw Data Server Facet 89
Table 67 – Historical Aggregate Server Facet 90
Table 68 – Historical Data AtTime Server Facet 91
Table 69 – Historical Access Modified Data Server Facet 91
Table 70 – Historical Annotation Server Facet 91
Table 71 – Historical Data Insert Server Facet 91
Table 72 – Historical Data Update Server Facet 92
Table 73 – Historical Data Replace Server Facet 92
Table 74 – Historical Data Delete Server Facet 92
Table 75 – Historical Access Structured Data Server Facet 92
Table 76 – Base Historical Event Server Facet 93
Table 77 – Historical Event Update Server Facet 93
Table 78 – Historical Event Replace Server Facet 93
Table 79 – Historical Event Insert Server Facet 93
Table 80 – Historical Event Delete Server Facet 93
Table 81 – Aggregate Subscription Server Facet 94
Table 82 – Nano Embedded Device 2017 Server Profile 95
Table 83 – Micro Embedded Device 2017 Server Profile 95
Table 84 – Embedded 2017 UA Server Profile 96
Table 85 – Standard 2017 UA Server Profile 97
Table 86 – Core 2017 Client Facet 97
Table 87 – Sessionless Client Facet 98
Table 88 – Reverse Connect Client Facet 98
Table 89 – Base Client Behaviour Facet 98
Table 90 – Discovery Client Facet 99
Table 91 – Subnet Discovery Client Facet 99
Table 92 – Global Discovery Client Facet 99
Table 93 – Global Certificate Management Client Facet 99
Table 94 – KeyCredential Service Client Facet 100
Table 95 – Access Token Request Client Facet 100
Table 96 – AddressSpace Lookup Client Facet 100
Table 97 – Request State Change Client Facet 100
Table 98 – File Access Client Facet 101
Table 99 – Entry Level Support 2015 Client Facet 101
Table 100 – Multi-Server Client Connection Facet 101
Table 101 – Documentation – Client 102
Table 102 – Attribute Read Client Facet 102
Table 103 – Attribute Write Client Facet 102

Table 104 – DataChange Subscriber Client Facet 103
Table 105 – Durable Subscription Client Facet 103
Table 106 – DataAccess Client Facet 104
Table 107 – Event Subscriber Client Facet 104
Table 108 – Base Event Processing Client Facet 105
Table 109 – Notifier and Source Hierarchy Client Facet 105
Table 110 – A & C Base Condition Client Facet 105
Table 111 – A & C Refresh2 Client Facet 106
Table 112 – A & C Address Space Instance Client Facet 106
Table 113 – A & C Enable Client Facet 106
Table 114 – A & C AlarmMetrics Client Facet 106
Table 115 – A & C Alarm Client Facet 107
Table 116 – A & C Exclusive Alarming Client Facet 107
Table 117 – A & C Non-Exclusive Alarming Client Facet 108
Table 118 – A & C Previous Instances Client Facet 108
Table 119 – A & C Dialog Client Facet 108
Table 120 – A & C CertificateExpiration Client Facet 108
Table 121 – A & E Proxy Facet 109
Table 122 – Method Client Facet 110
Table 123 – Auditing Client Facet 110
Table 124 – Node Management Client Facet 110
Table 125 – Advanced Type Programming Client Facet 111
Table 126 – User Role Management Client Facet 111
Table 127 – State Machine Client Facet 111
Table 128 – Diagnostic Client Facet 111
Table 129 – Redundant Client Facet 112
Table 130 – Redundancy Switch Client Facet 112
Table 131 – Historical Access Client Facet 112
Table 132 – Historical Data AtTime Client Facet 112
Table 133 – Historical Aggregate Client Facet 113
Table 134 – Historical Annotation Client Facet 114
Table 135 – Historical Access Modified Data Client Facet 114
Table 136 – Historical Data Insert Client Facet 114
Table 137 – Historical Data Update Client Facet 114
Table 138 – Historical Data Replace Client Facet 115
Table 139 – Historical Data Delete Client Facet 115
Table 140 – Historical Access Client Server Timestamp Facet 115
Table 141 – Historical Structured Data Access Client Facet 115
Table 142 – Historical Structured Data AtTime Client Facet 115
Table 143 – Historical Structured Data Modified Client Facet 116
Table 144 – Historical Structured Data Insert Client Facet 116
Table 145 – Historical Structured Data Update Client Facet 116
Table 146 – Historical Structured Data Replace Client Facet 116

Table 147 – Historical Structured Data Delete Client Facet 117
Table 148 – Historical Events Client Facet 117
Table 149 – Historical Event Insert Client Facet 117
Table 150 – Historical Event Update Client Facet 117
Table 151 – Historical Event Replace Client Facet 117
Table 152 – Historical Event Delete Client Facet 118
Table 153 – Aggregate Subscriber Client Facet 118
Table 154 – Standard UA Client 2017 Profile 120
Table 155 – UA-TCP UA-SC UA-Binary 120
Table 156 – HTTPS UA-Binary 120
Table 157 – HTTPS UA-XML 121
Table 158 – HTTPS UA-JSON 121
Table 159 – WSS UA-SC UA-Binary 122
Table 160 – WSS UA-JSON 122
Table 161 – Security User Access Control Full 123
Table 162 – Security User Access Control Base 123
Table 163 – Security Time Synchronization 123
Table 164 – Best Practice – Audit Events 123
Table 165 – Best Practice – Alarm Handling 124
Table 166 – Best Practice – Random Numbers 124
Table 167 – Best Practice – Timeouts 124
Table 168 – Best Practice – Administrative Access 124
Table 169 – Best Practice – Strict Message Handling 124
Table 170 – Best Practice – Audit Events Client 125
Table 171 – TransportSecurity – TLS 1.2 126
Table 172 – TransportSecurity – TLS 1.2 with PFS 126
Table 173 – SecurityPolicy – None 127
Table 174 – SecurityPolicy [A] – Aes128-Sha256-RsaOaep 128
Table 175 – SecurityPolicy [B] – Basic256Sha256 129
Table 176 – SecurityPolicy – Aes256-Sha256-RsaPss 129
Table 177 – User Token – Anonymous Facet 130
Table 178 – User Token – User Name Password Server Facet 130
Table 179 – User Token – X509 Certificate Server Facet 130
Table 180 – User Token – Issued Token Server Facet 130
Table 181 – User Token – Issued Token Windows Server Facet 130
Table 182 – User Token – JWT Server Facet 131
Table 183 – User Token – User Name Password Client Facet 131
Table 184 – User Token – X509 Certificate Client Facet 131
Table 185 – User Token – Issued Token Client Facet 131
Table 186 – User Token – Issued Token Windows Client Facet 132
Table 187 – User Token – JWT Client Facet 132
Table 188 – Global Discovery Server 2017 Profile 132
Table 189 – Global Discovery and Certificate Mgmt 2017 Server 133

Table 190 – Global Certificate Management Client 2017 Profile 133
Table 191 – Global Service Authorization Request Server Facet 133
Table 192 – Global Service KeyCredential Pull Facet 134
Table 193 – Global Service KeyCredential Push Facet 134

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC UNIFIED ARCHITECTURE –

Part 7: Profiles

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

International Standard IEC 62541-7 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) new functional Profiles:
   - profiles for global discovery and global certificate management;
   - profiles for global KeyCredential management and global access token management;
   - facet for durable subscriptions;
   - standard UA Client Profile;
   - profiles for administration of user roles and permissions.
b) new transport Profiles:
   - HTTPS with JSON encoding;
   - secure WebSockets (WSS) with binary or JSON encoding;
   - reverse connectivity.
c) new security Profiles:
   - transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy);
   - securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15);
   - securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP);
   - user Token JWT (Jason Web Token).
d) deprecated Security Profiles (due to broken algorithms):
   - securityPolicy – Basic128Rsa15 (broken algorithm Sha1);
   - securityPolicy – Basic256 (broken algorithm Sha1);
   - transportSecurity – TLS 1.0 (broken algorithm RC4);
   - transportSecurity – TLS 1.1 (broken algorithm RC4).
e) deprecated Transport (missing support on most platforms):
   - SOAP/HTTP with WS-SecureConversation (all encodings).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65E/707/FDIS	65E/725/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

Throughout this document and the other parts of the IEC 62541 series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in the "Terms and definition" clause in one of the parts of the IEC 62541 series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms and names* are, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published under the general title *OPC Unified Architecture*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

OPC UNIFIED ARCHITECTURE –

Part 7: Profiles

1 Scope

This part of IEC 62541 ~~describes~~ defines the OPC Unified Architecture (OPC UA) *Profiles*. The *Profiles* in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs. This could equally as well refer to test tools provided by another organization or a test lab provided by another organization. What is important is the concept of automated tool-based testing versus lab-based testing. The scope of this standard includes defining functionality that can only be tested in a lab and defining the grouping of functionality that is to be used when testing OPC UA products either in a lab or using automated tools. The definition of actual *TestCases* is not within the scope of this document, but the general categories of TestCases are within the scope of this document.

Most OPC UA applications will conform to several, but not all, of the *Profiles*.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TR 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security Model*

IEC 62541-3, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-8, *OPC Unified Architecture – Part 8: Data Access*

IEC 62541-9, *OPC Unified Architecture – Part 9: Alarms and Conditions*

IEC 62541-11[1], *OPC Unified Architecture – Part 11: Historical Access*

IEC 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

IEC 62541-13[1], *OPC Unified Architecture – Part 13: Aggregates*

[1] To be published.

Compliance Part 8 UA Server: OPC Test Lab Specification: Part 8 – UA Server
http://www.opcfoundation.org/Test/Part8/

Compliance Part 9 UA Client: OPC Test Lab Specification: Part 9 – UA Client
http://www.opcfoundation.org/Test/Part9/

IEC 62541-7

Edition 3.0 2020-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

OPC unified architecture – Part 7: Profiles

Architecture unifiée OPC – Partie 7: Profils



IEC 62541-7:2020-06(en-fr)

CONTENTS

FOREWORD 12
1 Scope 15
2 Normative references 15
3 Terms, definitions, and abbreviated terms 16
3.1 Terms and definitions 16
3.2 Abbreviated terms 17
4 Overview 17
4.1 General 17
4.2 ConformanceUnit 18
4.3 Profiles 18
4.4 Profile Categories 19
5 Conformance Units 19
5.1 Overview 19
5.2 Services 20
5.3 Transport and communication related features 30
5.4 Information Model and AddressSpace related features 38
5.5 Miscellaneous 55
6 Profiles 57
6.1 Overview 57
6.2 Profile list 57
6.3 Conventions for Profile definitions 64
6.4 Profile versioning 64
6.5 Applications 64
6.6 Profile tables 66
6.6.1 General 66
6.6.2 Core Server Facet 66
6.6.3 Core 2017 Server Facet 66
6.6.4 Sessionless Server Facet 67
6.6.5 Reverse Connect Server Facet 67
6.6.6 Base Server Behaviour Facet 68
6.6.7 Request State Change Server Facet 68
6.6.8 Subnet Discovery Server Facet 68
6.6.9 Global Certificate Management Server Facet 68
6.6.10 Authorization Service Server Facet 69
6.6.11 KeyCredential Service Server Facet 69
6.6.12 Attribute WriteMask Server Facet 69
6.6.13 File Access Server Facet 69
6.6.14 Documentation Server Facet 70
6.6.15 Embedded DataChange Subscription Server Facet 70
6.6.16 Standard DataChange Subscription Server Facet 70
6.6.17 Standard DataChange Subscription 2017 Server Facet 71
6.6.18 Enhanced DataChange Subscription Server Facet 71
6.6.19 Enhanced DataChange Subscription 2017 Server Facet 71
6.6.20 Durable Subscription Server Facet 71
6.6.21 Data Access Server Facet 72
6.6.22 ComplexType Server Facet 72

6.6.23 ComplexType 2017 Server Facet 72
6.6.24 Standard Event Subscription Server Facet 73
6.6.25 Address Space Notifier Server Facet 74
6.6.26 A & C Base Condition Server Facet 74
6.6.27 A & C Refresh2 Server Facet 74
6.6.28 A & C Address Space Instance Server Facet 74
6.6.29 A & C Enable Server Facet 75
6.6.30 A & C AlarmMetrics Server Facet 75
6.6.31 A & C Alarm Server Facet 75
6.6.32 A & C Acknowledgeable Alarm Server Facet 76
6.6.33 A & C Exclusive Alarming Server Facet 76
6.6.34 A & C Non-Exclusive Alarming Server Facet 77
6.6.35 A & C Previous Instances Server Facet 77
6.6.36 A & C Dialog Server Facet 77
6.6.37 A & C CertificateExpiration Server Facet 78
6.6.38 A & E Wrapper Facet 78
6.6.39 Method Server Facet 79
6.6.40 Auditing Server Facet 79
6.6.41 Node Management Server Facet 80
6.6.42 User Role Base Server Facet 80
6.6.43 User Role Management Server Facet 80
6.6.44 State Machine Server Facet 81
6.6.45 Client Redundancy Server Facet 81
6.6.46 Redundancy Transparent Server Facet 81
6.6.47 Redundancy Visible Server Facet 82
6.6.48 Historical Raw Data Server Facet 82
6.6.49 Historical Aggregate Server Facet 82
6.6.50 Historical Data AtTime Server Facet 83
6.6.51 Historical Access Modified Data Server Facet 84
6.6.52 Historical Annotation Server Facet 84
6.6.53 Historical Data Insert Server Facet 84
6.6.54 Historical Data Update Server Facet 84
6.6.55 Historical Data Replace Server Facet 85
6.6.56 Historical Data Delete Server Facet 85
6.6.57 Historical Access Structured Data Server Facet 85
6.6.58 Base Historical Event Server Facet 85
6.6.59 Historical Event Update Server Facet 86
6.6.60 Historical Event Replace Server Facet 86
6.6.61 Historical Event Insert Server Facet 86
6.6.62 Historical Event Delete Server Facet 86
6.6.63 Aggregate Subscription Server Facet 87
6.6.64 Nano Embedded Device Server Profile 88
6.6.65 Nano Embedded Device 2017 Server Profile 88
6.6.66 Micro Embedded Device Server Profile 88
6.6.67 Micro Embedded Device 2017 Server Profile 88
6.6.68 Embedded UA Server Profile 88
6.6.69 Embedded 2017 UA Server Profile 89
6.6.70 Standard UA Server Profile 89
6.6.71 Standard 2017 UA Server Profile 89

6.6.72 Core Client Facet 90
6.6.73 Core 2017 Client Facet 90
6.6.74 Sessionless Client Facet 90
6.6.75 Reverse Connect Client Facet 90
6.6.76 Base Client Behaviour Facet 91
6.6.77 Discovery Client Facet 91
6.6.78 Subnet Discovery Client Facet 91
6.6.79 Global Discovery Client Facet 92
6.6.80 Global Certificate Management Client Facet 92
6.6.81 KeyCredential Service Client Facet 92
6.6.82 Access Token Request Client Facet 92
6.6.83 AddressSpace Lookup Client Facet 93
6.6.84 Request State Change Client Facet 93
6.6.85 File Access Client Facet 93
6.6.86 Entry Level Support 2015 Client Facet 94
6.6.87 Multi-Server Client Connection Facet 94
6.6.88 Documentation – Client 94
6.6.89 Attribute Read Client Facet 94
6.6.90 Attribute Write Client Facet 95
6.6.91 DataChange Subscriber Client Facet 95
6.6.92 Durable Subscription Client Facet 96
6.6.93 DataAccess Client Facet 96
6.6.94 Event Subscriber Client Facet 97
6.6.95 Base Event Processing Client Facet 97
6.6.96 Notifier and Source Hierarchy Client Facet 98
6.6.97 A & C Base Condition Client Facet 98
6.6.98 A & C Refresh2 Client Facet 98
6.6.99 A & C Address Space Instance Client Facet 99
6.6.100 A & C Enable Client Facet 99
6.6.101 A & C AlarmMetrics Client Facet 99
6.6.102 A & C Alarm Client Facet 99
6.6.103 A & C Exclusive Alarming Client Facet 100
6.6.104 A & C Non-Exclusive Alarming Client Facet 100
6.6.105 A & C Previous Instances Client Facet 101
6.6.106 A & C Dialog Client Facet 101
6.6.107 A & C CertificateExpiration Client Facet 101
6.6.108 A & E Proxy Facet 102
6.6.109 Method Client Facet 103
6.6.110 Auditing Client Facet 103
6.6.111 Node Management Client Facet 103
6.6.112 Advanced Type Programming Client Facet 103
6.6.113 User Role Management Client Facet 104
6.6.114 State Machine Client Facet 104
6.6.115 Diagnostic Client Facet 104
6.6.116 Redundant Client Facet 105
6.6.117 Redundancy Switch Client Facet 105
6.6.118 Historical Access Client Facet 105
6.6.119 Historical Data AtTime Client Facet 105
6.6.120 Historical Aggregate Client Facet 105

6.6.121 Historical Annotation Client Facet 107
6.6.122 Historical Access Modified Data Client Facet 107
6.6.123 Historical Data Insert Client Facet 107
6.6.124 Historical Data Update Client Facet 107
6.6.125 Historical Data Replace Client Facet 107
6.6.126 Historical Data Delete Client Facet 108
6.6.127 Historical Access Client Server Timestamp Facet 108
6.6.128 Historical Structured Data Access Client Facet 108
6.6.129 Historical Structured Data AtTime Client Facet 108
6.6.130 Historical Structured Data Modified Client Facet 109
6.6.131 Historical Structured Data Insert Client Facet 109
6.6.132 Historical Structured Data Update Client Facet 109
6.6.133 Historical Structured Data Replace Client Facet 109
6.6.134 Historical Structured Data Delete Client Facet 109
6.6.135 Historical Events Client Facet 110
6.6.136 Historical Event Insert Client Facet 110
6.6.137 Historical Event Update Client Facet 110
6.6.138 Historical Event Replace Client Facet 110
6.6.139 Historical Event Delete Client Facet 111
6.6.140 Aggregate Subscriber Client Facet 111
6.6.141 Standard UA Client Profile 112
6.6.142 Standard UA Client 2017 Profile 112
6.6.143 UA-TCP UA-SC UA-Binary 113
6.6.144 HTTPS UA-Binary 113
6.6.145 HTTPS UA-XML 114
6.6.146 HTTPS UA-JSON 114
6.6.147 WSS UA-SC UA-Binary 114
6.6.148 WSS UA-JSON 114
6.6.149 Security User Access Control Full 115
6.6.150 Security User Access Control Base 115
6.6.151 Security Time Synchronization 115
6.6.152 Best Practice – Audit Events 116
6.6.153 Best Practice – Alarm Handling 116
6.6.154 Best Practice – Random Numbers 116
6.6.155 Best Practice – Timeouts 116
6.6.156 Best Practice – Administrative Access 116
6.6.157 Best Practice – Strict Message Handling 117
6.6.158 Best Practice – Audit Events Client 117
6.6.159 TransportSecurity – TLS 1.2 117
6.6.160 TransportSecurity – TLS 1.2 with PFS 117
6.6.161 SecurityPolicy – None 118
6.6.162 SecurityPolicy – Basic128Rsa15 118
6.6.163 SecurityPolicy – Basic256 118
6.6.164 SecurityPolicy [A] – Aes128-Sha256-RsaOaep 118
6.6.165 SecurityPolicy [B] – Basic256Sha256 119
6.6.166 SecurityPolicy – Aes256-Sha256-RsaPss 119
6.6.167 User Token – Anonymous Facet 120
6.6.168 User Token – User Name Password Server Facet 120
6.6.169 User Token – X509 Certificate Server Facet 120

6.6.170 User Token – Issued Token Server Facet 121
6.6.171 User Token – Issued Token Windows Server Facet 121
6.6.172 User Token – JWT Server Facet 121
6.6.173 User Token – User Name Password Client Facet 121
6.6.174 User Token – X509 Certificate Client Facet 122
6.6.175 User Token – Issued Token Client Facet 122
6.6.176 User Token – Issued Token Windows Client Facet 122
6.6.177 User Token – JWT Client Facet 122
6.6.178 Global Discovery Server Profile 122
6.6.179 Global Discovery Server 2017 Profile 123
6.6.180 Global Discovery and Certificate Management Server 123
6.6.181 Global Discovery and Certificate Mgmt 2017 Server 123
6.6.182 Global Certificate Management Client Profile 123
6.6.183 Global Certificate Management Client 2017 Profile 123
6.6.184 Global Service Authorization Request Server Facet 124
6.6.185 Global Service KeyCredential Pull Facet 124
6.6.186 Global Service KeyCredential Push Facet 124
Bibliography 125

Figure 1 – Profile – ConformanceUnit – TestCases 18
Figure 2 – HMI Client sample 64
Figure 3 – Embedded Server sample 65
Figure 4 – Standard UA Server sample 65

Table 1 – Profile Categories 19
Table 2 – Conformance Groups 20
Table 3 – Discovery Services 21
Table 4 – Session Services 22
Table 5 – Node Management Services 23
Table 6 – View Services 24
Table 7 – Attribute Services 25
Table 8 – Method Services 26
Table 9 – Monitored Item Services 27
Table 10 – Subscription Services 29
Table 11 – Security 31
Table 12 – Protocol and Encoding 38
Table 13 – Base Information 39
Table 14 – Address Space Model 41
Table 15 – Data Access 42
Table 16 – Alarms and Conditions 43
Table 17 – Historical Access 46
Table 18 – Aggregates 49
Table 19 – Auditing 54
Table 20 – Redundancy 54
Table 21 – Global Discovery Server 55

Table 22 – Miscellaneous 56
Table 23 – Profile list 58
Table 24 – Core 2017 Server Facet 67
Table 25 – Sessionless Server Facet 67
Table 26 – Reverse Connect Server Facet 68
Table 27 – Base Server Behaviour Facet 68
Table 28 – Request State Change Server Facet 68
Table 29 – Subnet Discovery Server Facet 68
Table 30 – Global Certificate Management Server Facet 69
Table 31 – Authorization Service Server Facet 69
Table 32 – KeyCredential Service Server Facet 69
Table 33 – Attribute WriteMask Server Facet 69
Table 34 – File Access Server Facet 70
Table 35 – Documentation Server Facet 70
Table 36 – Embedded DataChange Subscription Server Facet 70
Table 37 – Standard DataChange Subscription 2017 Server Facet 71
Table 38 – Enhanced DataChange Subscription 2017 Server Facet 71
Table 39 – Durable Subscription Server Facet 72
Table 40 – Data Access Server Facet 72
Table 41 – ComplexType 2017 Server Facet 73
Table 42 – Standard Event Subscription Server Facet 73
Table 43 – Address Space Notifier Server Facet 74
Table 44 – A & C Base Condition Server Facet 74
Table 45 – A & C Refresh2 Server Facet 74
Table 46 – A & C Address Space Instance Server Facet 75
Table 47 – A & C Enable Server Facet 75
Table 48 – A & C AlarmMetrics Server Facet 75
Table 49 – A & C Alarm Server Facet 76
Table 50 – A & C Acknowledgeable Alarm Server Facet 76
Table 51 – A & C Exclusive Alarming Server Facet 77
Table 52 – A & C Non-Exclusive Alarming Server Facet 77
Table 53 – A & C Previous Instances Server Facet 77
Table 54 – A & C Dialog Server Facet 78
Table 55 – A & C CertificateExpiration Server Facet 78
Table 56 – A & E Wrapper Facet 79
Table 57 – Method Server Facet 79
Table 58 – Auditing Server Facet 80
Table 59 – Node Management Server Facet 80
Table 60 – User Role Base Server Facet 80
Table 61 – User Role Management Server Facet 81
Table 62 – State Machine Server Facet 81
Table 63 – Client Redundancy Server Facet 81
Table 64 – Redundancy Transparent Server Facet 81

Table 65 – Redundancy Visible Server Facet 82
Table 66 – Historical Raw Data Server Facet 82
Table 67 – Historical Aggregate Server Facet 83
Table 68 – Historical Data AtTime Server Facet 84
Table 69 – Historical Access Modified Data Server Facet 84
Table 70 – Historical Annotation Server Facet 84
Table 71 – Historical Data Insert Server Facet 84
Table 72 – Historical Data Update Server Facet 85
Table 73 – Historical Data Replace Server Facet 85
Table 74 – Historical Data Delete Server Facet 85
Table 75 – Historical Access Structured Data Server Facet 85
Table 76 – Base Historical Event Server Facet 86
Table 77 – Historical Event Update Server Facet 86
Table 78 – Historical Event Replace Server Facet 86
Table 79 – Historical Event Insert Server Facet 86
Table 80 – Historical Event Delete Server Facet 86
Table 81 – Aggregate Subscription Server Facet 87
Table 82 – Nano Embedded Device 2017 Server Profile 88
Table 83 – Micro Embedded Device 2017 Server Profile 88
Table 84 – Embedded 2017 UA Server Profile 89
Table 85 – Standard 2017 UA Server Profile 89
Table 86 – Core 2017 Client Facet 90
Table 87 – Sessionless Client Facet 90
Table 88 – Reverse Connect Client Facet 91
Table 89 – Base Client Behaviour Facet 91
Table 90 – Discovery Client Facet 91
Table 91 – Subnet Discovery Client Facet 92
Table 92 – Global Discovery Client Facet 92
Table 93 – Global Certificate Management Client Facet 92
Table 94 – KeyCredential Service Client Facet 92
Table 95 – Access Token Request Client Facet 93
Table 96 – AddressSpace Lookup Client Facet 93
Table 97 – Request State Change Client Facet 93
Table 98 – File Access Client Facet 93
Table 99 – Entry Level Support 2015 Client Facet 94
Table 100 – Multi-Server Client Connection Facet 94
Table 101 – Documentation – Client 94
Table 102 – Attribute Read Client Facet 95
Table 103 – Attribute Write Client Facet 95
Table 104 – DataChange Subscriber Client Facet 96
Table 105 – Durable Subscription Client Facet 96
Table 106 – DataAccess Client Facet 97
Table 107 – Event Subscriber Client Facet 97

Table 108 – Base Event Processing Client Facet 98
Table 109 – Notifier and Source Hierarchy Client Facet 98
Table 110 – A & C Base Condition Client Facet 98
Table 111 – A & C Refresh2 Client Facet 99
Table 112 – A & C Address Space Instance Client Facet 99
Table 113 – A & C Enable Client Facet 99
Table 114 – A & C AlarmMetrics Client Facet 99
Table 115 – A & C Alarm Client Facet 100
Table 116 – A & C Exclusive Alarming Client Facet 100
Table 117 – A & C Non-Exclusive Alarming Client Facet 101
Table 118 – A & C Previous Instances Client Facet 101
Table 119 – A & C Dialog Client Facet 101
Table 120 – A & C CertificateExpiration Client Facet 101
Table 121 – A & E Proxy Facet 102
Table 122 – Method Client Facet 103
Table 123 – Auditing Client Facet 103
Table 124 – Node Management Client Facet 103
Table 125 – Advanced Type Programming Client Facet 104
Table 126 – User Role Management Client Facet 104
Table 127 – State Machine Client Facet 104
Table 128 – Diagnostic Client Facet 104
Table 129 – Redundant Client Facet 105
Table 130 – Redundancy Switch Client Facet 105
Table 131 – Historical Access Client Facet 105
Table 132 – Historical Data AtTime Client Facet 105
Table 133 – Historical Aggregate Client Facet 106
Table 134 – Historical Annotation Client Facet 107
Table 135 – Historical Access Modified Data Client Facet 107
Table 136 – Historical Data Insert Client Facet 107
Table 137 – Historical Data Update Client Facet 107
Table 138 – Historical Data Replace Client Facet 108
Table 139 – Historical Data Delete Client Facet 108
Table 140 – Historical Access Client Server Timestamp Facet 108
Table 141 – Historical Structured Data Access Client Facet 108
Table 142 – Historical Structured Data AtTime Client Facet 108
Table 143 – Historical Structured Data Modified Client Facet 109
Table 144 – Historical Structured Data Insert Client Facet 109
Table 145 – Historical Structured Data Update Client Facet 109
Table 146 – Historical Structured Data Replace Client Facet 109
Table 147 – Historical Structured Data Delete Client Facet 110
Table 148 – Historical Events Client Facet 110
Table 149 – Historical Event Insert Client Facet 110
Table 150 – Historical Event Update Client Facet 110

Table 151 – Historical Event Replace Client Facet 110
Table 152 – Historical Event Delete Client Facet 111
Table 153 – Aggregate Subscriber Client Facet 111
Table 154 – Standard UA Client 2017 Profile 113
Table 155 – UA-TCP UA-SC UA-Binary 113
Table 156 – HTTPS UA-Binary 113
Table 157 – HTTPS UA-XML 114
Table 158 – HTTPS UA-JSON 114
Table 159 – WSS UA-SC UA-Binary 114
Table 160 – WSS UA-JSON 115
Table 161 – Security User Access Control Full 115
Table 162 – Security User Access Control Base 115
Table 163 – Security Time Synchronization 115
Table 164 – Best Practice – Audit Events 116
Table 165 – Best Practice – Alarm Handling 116
Table 166 – Best Practice – Random Numbers 116
Table 167 – Best Practice – Timeouts 116
Table 168 – Best Practice – Administrative Access 117
Table 169 – Best Practice – Strict Message Handling 117
Table 170 – Best Practice – Audit Events Client 117
Table 171 – TransportSecurity – TLS 1.2 117
Table 172 – TransportSecurity – TLS 1.2 with PFS 118
Table 173 – SecurityPolicy – None 118
Table 174 – SecurityPolicy [A] – Aes128-Sha256-RsaOaep 119
Table 175 – SecurityPolicy [B] – Basic256Sha256 119
Table 176 – SecurityPolicy – Aes256-Sha256-RsaPss 120
Table 177 – User Token – Anonymous Facet 120
Table 178 – User Token – User Name Password Server Facet 120
Table 179 – User Token – X509 Certificate Server Facet 120
Table 180 – User Token – Issued Token Server Facet 121
Table 181 – User Token – Issued Token Windows Server Facet 121
Table 182 – User Token – JWT Server Facet 121
Table 183 – User Token – User Name Password Client Facet 121
Table 184 – User Token – X509 Certificate Client Facet 122
Table 185 – User Token – Issued Token Client Facet 122
Table 186 – User Token – Issued Token Windows Client Facet 122
Table 187 – User Token – JWT Client Facet 122
Table 188 – Global Discovery Server 2017 Profile 123
Table 189 – Global Discovery and Certificate Mgmt 2017 Server 123
Table 190 – Global Certificate Management Client 2017 Profile 124
Table 191 – Global Service Authorization Request Server Facet 124

Table 192 – Global Service KeyCredential Pull Facet 124
Table 193 – Global Service KeyCredential Push Facet..... 124

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC UNIFIED ARCHITECTURE –

Part 7: Profiles

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62541-7 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) new functional Profiles:
   - profiles for global discovery and global certificate management;
   - profiles for global KeyCredential management and global access token management;
   - facet for durable subscriptions;
   - standard UA Client Profile;

- profiles for administration of user roles and permissions.

b) new transport Profiles:
   - HTTPS with JSON encoding;
   - secure WebSockets (WSS) with binary or JSON encoding;
   - reverse connectivity.

c) new security Profiles:
   - transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy);
   - securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15);
   - securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP);
   - user Token JWT (Jason Web Token).

d) deprecated Security Profiles (due to broken algorithms):
   - securityPolicy – Basic128Rsa15 (broken algorithm Sha1);
   - securityPolicy – Basic256 (broken algorithm Sha1);
   - transportSecurity – TLS 1.0 (broken algorithm RC4);
   - transportSecurity – TLS 1.1 (broken algorithm RC4).

e) deprecated Transport (missing support on most platforms):
   - SOAP/HTTP with WS-SecureConversation (all encodings).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65E/707/FDIS	65E/725/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

Throughout this document and the other parts of the IEC 62541 series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in the "Terms and definition" clause in one of the parts of the IEC 62541 series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms and names* are, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published under the general title *OPC Unified Architecture*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

OPC UNIFIED ARCHITECTURE –

Part 7: Profiles

1 Scope

This part of IEC 62541 defines the OPC Unified Architecture (OPC UA) *Profiles*. The *Profiles* in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs. This could equally as well refer to test tools provided by another organization or a test lab provided by another organization. What is important is the concept of automated tool-based testing versus lab-based testing. The scope of this standard includes defining functionality that can only be tested in a lab and defining the grouping of functionality that is to be used when testing OPC UA products either in a lab or using automated tools. The definition of actual *TestCases* is not within the scope of this document, but the general categories of TestCases are within the scope of this document.

Most OPC UA applications will conform to several, but not all, of the *Profiles*.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TR 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security Model*

IEC 62541-3, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-8, *OPC Unified Architecture – Part 8: Data Access*

IEC 62541-9, *OPC Unified Architecture – Part 9: Alarms and Conditions*

IEC 62541-11, *OPC Unified Architecture – Part 11: Historical Access*

IEC 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

IEC 62541-13, *OPC Unified Architecture – Part 13: Aggregates*

Compliance Part 8 UA Server: OPC Test Lab Specification: Part 8 – UA Server
http://www.opcfoundation.org/Test/Part8/

Compliance Part 9 UA Client: OPC Test Lab Specification: Part 9 – UA Client
http://www.opcfoundation.org/Test/Part9/

SOMMAIRE

AVANT-PROPOS 136
1 Domaine d'application 139
2 Références normatives 139
3 Termes, définitions et termes abrégés 140
3.1 Termes et définitions 140
3.2 Termes abrégés 141
4 Vue d'ensemble 141
4.1 Généralités 141
4.2 ConformanceUnit 142
4.3 Profils 142
4.4 Catégories de profils 143
5 Unités de Conformité 143
5.1 Vue d'ensemble 143
5.2 Services 144
5.3 Caractéristiques relatives au transport et à la communication 155
5.4 Modèle d'information et caractéristiques relatives à l'AddressSpace 164
5.5 Divers 182
6 Profils 184
6.1 Vue d'ensemble 184
6.2 Liste des profils 184
6.3 Conventions applicables aux définitions des profils 191
6.4 Versionnage des Profils 191
6.5 Applications 191
6.6 Tableaux de Profils 193
6.6.1 Généralités 193
6.6.2 Facette Serveur principal 193
6.6.3 Facette Serveur 2017 principal 193
6.6.4 Facette Serveur Sans session 194
6.6.5 Facette Serveur Connexion inversée 195
6.6.6 Facette Serveur Comportement de base du serveur 195
6.6.7 Facette Serveur Demande modification d'état 195
6.6.8 Facette Serveur Découverte sous-réseau 195
6.6.9 Facette Serveur Gestion globale des certificats 196
6.6.10 Facette Serveur Service d'autorisation 196
6.6.11 Facette Serveur Service KeyCredential 196
6.6.12 Facette Serveur Attribut WriteMask 196
6.6.13 Facette Serveur Accès fichier 197
6.6.14 Facette Serveur Documentation 197
6.6.15 Facette Serveur Abonnement intégré aux DataChanges 197
6.6.16 Facette Serveur Abonnement normalisé aux DataChanges 198
6.6.17 Facette Serveur 2017 Abonnement normalisé aux DataChanges 198
6.6.18 Facette Serveur Abonnement amélioré aux DataChanges 198
6.6.19 Facette Serveur 2017 Abonnement amélioré aux DataChanges 199
6.6.20 Facette Serveur Abonnement durable 199
6.6.21 Facette Serveur Accès aux données 199
6.6.22 Facette Serveur ComplexType 200

6.6.23 Facette Serveur 2017 ComplexType 200
6.6.24 Facette Serveur Abonnement normalisé aux événements 200
6.6.25 Facette Serveur Notification de l'espace d'adressage 201
6.6.26 Facette Serveur A & C Condition de base 201
6.6.27 Facette Serveur A & C Refresh2 202
6.6.28 Facette Serveur A & C Instance de l'espace d'adressage 202
6.6.29 Facette Serveur A & C Activation 202
6.6.30 Facette Serveur A & C AlarmMetrics 203
6.6.31 Facette Serveur A & C Alarme 203
6.6.32 Facette Serveur A & C Alarme acquittable 203
6.6.33 Facette Serveur A & C Alarme exclusive 204
6.6.34 Facette Serveur A & C Alarme non exclusive 204
6.6.35 Facette Serveur A & C Instances précédentes 205
6.6.36 Facette Serveur A & C Dialogue 205
6.6.37 Facette Serveur A & C CertificateExpiration 205
6.6.38 Facette Conteneur A & E 206
6.6.39 Facette Serveur Méthode 206
6.6.40 Facette Serveur Audit 207
6.6.41 Facette Serveur Gestion des nœuds 207
6.6.42 Facette Serveur Rôle de base utilisateur 207
6.6.43 Facette Serveur Gestion des rôles d'utilisateurs 208
6.6.44 Facette Serveur Diagramme d'état 208
6.6.45 Facette Serveur Redondance client 208
6.6.46 Facette Serveur Redondance transparente 209
6.6.47 Facette Serveur Redondance visible 209
6.6.48 Facette Serveur Données brutes historiques 209
6.6.49 Facette Serveur Agrégat historique 209
6.6.50 Facette Serveur Données historiques à temps 210
6.6.51 Facette Serveur Accès à l'historique Données modifiées 211
6.6.52 Facette Serveur Annotation Historique 211
6.6.53 Facette Serveur Insertion Données historiques 211
6.6.54 Facette Serveur Mise à Jour Données historiques 211
6.6.55 Facette Serveur Remplacement données historiques 212
6.6.56 Facette Serveur Suppression données historiques 212
6.6.57 Facette Serveur Accès à l'historique Données structurées 212
6.6.58 Facette Serveur Evénement Historique de base 213
6.6.59 Facette Serveur Mise à jour Evénement historique 213
6.6.60 Facette Serveur Remplacement Evénement historique 213
6.6.61 Facette Serveur Insertion Evénement historique 213
6.6.62 Facette Serveur Suppression Evénement historique 213
6.6.63 Facette Serveur Abonnement aux agrégats 214
6.6.64 Profil Serveur à dispositif nano-intégré 215
6.6.65 Profil Serveur 2017 Dispositif Nano-Intégré 215
6.6.66 Profil Serveur Dispositif Micro-Intégré 215
6.6.67 Profil Serveur 2017 Dispositif Micro-Intégré 215
6.6.68 Profil Serveur UA intégré 216
6.6.69 Profil Serveur UA 2017 intégré 216
6.6.70 Profil Serveur UA normalisé 216
6.6.71 Profil Serveur UA 2017 normalisé 216

6.6.72 Facette Client principal 217
6.6.73 Facette Client 2017 principal 217
6.6.74 Facette Client Sans Session 218
6.6.75 Facette *Client* Connexion inversée 218
6.6.76 Facette Client Comportement de base 218
6.6.77 Facette Client Découverte 219
6.6.78 Facette Client Découverte Sous-Réseau 219
6.6.79 Facette Client Découverte Globale 219
6.6.80 Facette Client Gestion Globale des Certificats 219
6.6.81 Facette Client Service KeyCredential 220
6.6.82 Facette Client Demande de jeton d'accès 220
6.6.83 Facette Client Consultation de l'AddressSpace 220
6.6.84 Facette Client Demande de Modification d'Etat 221
6.6.85 Facette Client Accès Fichier 221
6.6.86 Facette Client 2015 Prise en Charge Entrée de Gamme 221
6.6.87 Facette Client Connexion Multi-Serveur 222
6.6.88 Documentation – Client 222
6.6.89 Facette Client Attribut Lecture 222
6.6.90 Facette Client Attribut Ecriture 223
6.6.91 Facette Client Abonné aux DataChanges 223
6.6.92 Facette Client Abonnement durable 224
6.6.93 Facette Client DataAccess 224
6.6.94 Facette Client Abonné aux Evénements 225
6.6.95 Facette Client Traitement des Evénements de base 225
6.6.96 Facette Client Hiérarchie de Notification et de Source 226
6.6.97 Facette Client A & C Condition de base 226
6.6.98 Facette Client A & C Refresh2 226
6.6.99 Facette Client A & C Instance de l'Espace d'adressage 227
6.6.100 Facette Client A & C Activer 227
6.6.101 Facette Client A & C AlarmMetrics 227
6.6.102 Facette Client A & C Alarme 227
6.6.103 Facette Client A & C Alarme exclusive 228
6.6.104 Facette Client A & C Alarme non exclusive 228
6.6.105 Facette Client A & C Instances précédentes 229
6.6.106 Facette Client A & C Dialogue 229
6.6.107 Facette Client A & C CertificateExpiration 229
6.6.108 Facette Proxy A & E 230
6.6.109 Facette Client Méthode 231
6.6.110 Facette Client Audit 231
6.6.111 Facette Client Gestion des Nœuds 231
6.6.112 Facette Client Programmation de type avancé 231
6.6.113 Facette Client Gestion des Rôles d'Utilisateurs 232
6.6.114 Facette Client Diagramme d'état 232
6.6.115 Facette Client Diagnostic 232
6.6.116 Facette Client Redondant 233
6.6.117 Facette Client Commutateur de redondance 233
6.6.118 Facette Client Accès à l'historique 233
6.6.119 Facette Client Données Historiques AtTime 233
6.6.120 Facette Client Agrégat Historique 233

6.6.121 Facette Client Annotation Historique 235
6.6.122 Facette Client Accès à l'historique Données Modifiées 235
6.6.123 Facette Client Insertion Données Historiques 235
6.6.124 Facette Client Mise à Jour Données Historiques 235
6.6.125 Facette Client Remplacement données historiques 235
6.6.126 Facette Client Supprimer données structurées historiques 236
6.6.127 Facette Client Accès à l'historique Horodatage Serveur 236
6.6.128 Facette Client Accès données structurées historiques 236
6.6.129 Facette Client Données structurées historiques AtTime 236
6.6.130 Facette Client Données structurées historiques modifiées 237
6.6.131 Facette Client Insérer données structurées historiques 237
6.6.132 Facette Client Mettre à Jour données structurées historiques 237
6.6.133 Facette Client Remplacer données structurées historiques 237
6.6.134 Facette Client Supprimer données structurées historiques 238
6.6.135 Facette Client Evénements Historiques 238
6.6.136 Facette Client Insertion Evénements Historiques 238
6.6.137 Facette Client Mise à Jour Evénements Historiques 238
6.6.138 Facette Client Remplacement Evénements Historiques 238
6.6.139 Facette Client Suppression Evénements Historiques 239
6.6.140 Facette Client Abonnement aux Agrégats 239
6.6.141 profil client UA normalisé; 240
6.6.142 Profil 2017 Client UA normalisé 240
6.6.143 Profil UA binaire UA-TCP UA-SC 241
6.6.144 Profil UA binaire HTTPS 241
6.6.145 Protocole de transport XML UA HTTPS 242
6.6.146 Protocole de transport UA JSON HTTPS 242
6.6.147 Profil UA binaire WSS UA-SC 242
6.6.148 Protocole de transport UA JSON WSS 242
6.6.149 Sécurité utilisateur Contrôle accès complet 243
6.6.150 Sécurité utilisateur Contrôle accès de base 243
6.6.151 Synchronisation Temporelle Sécurité 243
6.6.152 Meilleures pratiques – Evénements d'audit 244
6.6.153 Meilleures pratiques – Gestion d'alarmes 244
6.6.154 Meilleures pratiques – Nombres aléatoires 244
6.6.155 Meilleures pratiques – Temporisations 244
6.6.156 Meilleures pratiques – Accès administratif 244
6.6.157 Meilleures pratiques – Gestion stricte des messages 245
6.6.158 Meilleures pratiques – Client Evénements d'audit 245
6.6.159 Profil TransportSecurity – TLS 1.2 245
6.6.160 Profil TransportSecurity – TLS 1.2 avec PFS 245
6.6.161 SecurityPolicy – None 246
6.6.162 SecurityPolicy – Basic128Rsa15 246
6.6.163 SecurityPolicy – Basic256 246
6.6.164 SecurityPolicy [A] – Aes128-Sha256-RsaOaep 246
6.6.165 SecurityPolicy [B] – Basic256Sha256) 247
6.6.166 SecurityPolicy – Aes256-Sha256-RsaPss 248
6.6.167 Facette Jeton Utilisateur – Anonyme 248
6.6.168 Facette Serveur Jeton utilisateur – Nom d'utilisateur Mot de passe 248
6.6.169 Facette Serveur Jeton utilisateur – Certificat X509 249

6.6.170 Facette Serveur Jeton utilisateur – Jeton émis 249
6.6.171 Facette Serveur Windows Jeton utilisateur – Jeton émis 249
6.6.172 Facette Serveur Jeton utilisateur – JWT 249
6.6.173 Facette Client Jeton Utilisateur – Nom d'Utilisateur Mot de Passe 250
6.6.174 Facette Client Jeton Utilisateur – Certificat X509 250
6.6.175 Facette Client Jeton Utilisateur – Jeton Emis 250
6.6.176 Facette Client Windows Jeton Utilisateur – Jeton Emis 250
6.6.177 Facette Client Jeton Utilisateur – JWT 250
6.6.178 Profil Serveur Découverte Globale 251
6.6.179 Profil 2017 Serveur Découverte Globale 251
6.6.180 Serveur Découverte Globale et Gestion des Certificats 251
6.6.181 Serveur 2017 Découverte Globale et Gestion des Certificats 251
6.6.182 Profil Client Gestion Globale des Certificats 252
6.6.183 Profil 2017 Client Gestion Globale des Certificats 252
6.6.184 Facette Serveur Demande d'autorisation Service global 252
6.6.185 Facette Pull KeyCredential Service Global 252
6.6.186 Facette Push KeyCredential Service Global 253
Bibliographie 254

Figure 1 – Profil – ConformanceUnits – TestCases 142
Figure 2 – Echantillon Client IHM 191
Figure 3 – Échantillon Serveur intégré 192
Figure 4 – Echantillon Serveur UA normalisé 193

Tableau 1 – Catégories de profils 143
Tableau 2 – Groupes de Conformité 144
Tableau 3 – Services Découverte 145
Tableau 4 – Services Session 147
Tableau 5 – Services Gestion des Nœuds 148
Tableau 6 – Services Vue 149
Tableau 7 – Services Attribut 150
Tableau 8 – Services Méthode 151
Tableau 9 – Services Eléments surveillés 152
Tableau 10 – Services Abonnement 154
Tableau 11 – Sécurité 156
Tableau 12 – Protocole et codage 163
Tableau 13 – Informations de base 164
Tableau 14 – Modèle d'espace d'adressage 167
Tableau 15 – Accès aux données 169
Tableau 16 – Alarmes et conditions 170
Tableau 17 – Accès à l'historique 173
Tableau 18 – Agrégats 176
Tableau 19 – Audit 181
Tableau 20 – Redondance 181
Tableau 21 – Serveur "Découverte" Global 182

Tableau 22 – Divers 183
Tableau 23 – Liste des Profils 185
Tableau 24 – Facette Serveur 2017 principal 194
Tableau 25 – Facette Serveur Sans session 194
Tableau 26 – Facette Serveur Connexion inversée 195
Tableau 27 – Facette Serveur Comportement de base du serveur 195
Tableau 28 – Facette Serveur Demande modification d'état 195
Tableau 29 – Facette Serveur Découverte sous-Réseau 196
Tableau 30 – Facette Serveur Gestion globale des certificats 196
Tableau 31 – Facette Serveur Service d'autorisation 196
Tableau 32 – Facette Serveur Service KeyCredential 196
Tableau 33 – Facette Serveur Attribut WriteMask 197
Tableau 34 – Facette Serveur Accès fichier 197
Tableau 35 – Facette Serveur Documentation 197
Tableau 36 – Facette Serveur Abonnement intégré aux DataChanges 198
Tableau 37 – Facette Serveur 2017 Abonnement normalisé aux DataChanges 198
Tableau 38 – Facette Serveur 2017 Abonnement amélioré aux DataChanges 199
Tableau 39 – Facette Serveur Abonnement durable 199
Tableau 40 – Facette Serveur Accès aux données 200
Tableau 41 – Facette Serveur 2017 ComplexType 200
Tableau 42 – Facette Serveur Abonnement normalisé aux événements 201
Tableau 43 – Facette Serveur Notification de l'espace d'adressage 201
Tableau 44 – Facette Serveur A & C Condition de base 202
Tableau 45 – Facette Serveur A & C Refresh2 202
Tableau 46 – Facette Serveur A & C Instance Espace d'adressage 202
Tableau 47 – Facette Serveur A & C Activer 202
Tableau 48 – Facette Serveur A & C AlarmMetrics 203
Tableau 49 – Facette Serveur A & C Alarme 203
Tableau 50 – Facette Serveur A & C Alarme acceptable 204
Tableau 51 – Facette Serveur A & C Alarme exclusive 204
Tableau 52 – Facette Serveur A & C Alarme non exclusive 204
Tableau 53 – Facette Serveur A & C Instances précédentes 205
Tableau 54 – Facette Serveur A & C Dialogue 205
Tableau 55 – Facette Serveur A & C CertificateExpiration 205
Tableau 56 – Facette Conteneur A & E 206
Tableau 57 – Facette Serveur Méthode 207
Tableau 58 – Facette Serveur Audit 207
Tableau 59 – Facette Serveur Gestion des Nœuds 207
Tableau 60 – Facette Serveur Rôle de base Utilisateur 208
Tableau 61 – Facette Serveur Gestion des Rôles d'Utilisateurs 208
Tableau 62 – Facette Serveur Diagramme d'état 208
Tableau 63 – Facette Serveur Redondance Client 208
Tableau 64 – Facette Serveur Redondance transparente 209

Tableau 65 – Facette Serveur Redondance visible 209
Tableau 66 – Facette Serveur Données Brutes Historiques 209
Tableau 67 – Facette Serveur Agrégat Historique 210
Tableau 68 – Facette Serveur Données Historiques AtTime 211
Tableau 69 – Facette Serveur Accès à l'Historique Données Modifiées 211
Tableau 70 – Facette Serveur Annotation Historique 211
Tableau 71 – Facette Serveur Insertion Données Historiques 211
Tableau 72 – Facette Serveur Mise à Jour Données Historiques 212
Tableau 73 – Facette Serveur Remplacement données historiques 212
Tableau 74 – Facette Serveur Suppression données historiques 212
Tableau 75 – Facette Serveur Accès à l'historique données structurées 212
Tableau 76 – Facette Serveur Evénements Historiques de base 213
Tableau 77 – Facette Serveur Mise à Jour Evénements Historiques 213
Tableau 78 – Facette Serveur Remplacement Evénements Historiques 213
Tableau 79 – Facette Serveur Insertion Evénements Historiques 213
Tableau 80 – Facette Serveur Suppression Evénements Historiques 214
Tableau 81 – Facette Serveur Abonnement aux Agrégats 214
Tableau 82 – Profil Serveur 2017 à dispositif nano-intégré 215
Tableau 83 – Profil Serveur 2017 à dispositif micro-intégré 216
Tableau 84 – Profil Serveur UA 2017 intégré 216
Tableau 85 – Profil Serveur UA 2017 normalisé 217
Tableau 86 – Facette Client 2017 principal 217
Tableau 87 – Facette Client Sans Session 218
Tableau 88 – Facette Client Connexion inversée 218
Tableau 89 – Facette Comportement Client de base 218
Tableau 90 – Facette Client Découverte 219
Tableau 91 – Facette Client Découverte Sous-Réseau 219
Tableau 92 – Facette Client Découverte Globale 219
Tableau 93 – Facette Client Gestion Globale des Certificats 220
Tableau 94 – Facette Client Service KeyCredential 220
Tableau 95 – Facette Client Demande de jeton d'accès 220
Tableau 96 – Facette Client Consultation de l'AddressSpace 221
Tableau 97 – Facette Client Demande de Modification d'Etat 221
Tableau 98 – Facette Client Accès Fichier 221
Tableau 99 – Facette Client 2015 Prise en Charge Entrée de Gamme 222
Tableau 100 – Facette Client Connexion Multi-Serveur 222
Tableau 101 – Documentation – Client 222
Tableau 102 – Facette Client Attribut Lecture 223
Tableau 103 – Facette Client Attribut Ecriture 223
Tableau 104 – Facette Client Abonné aux DataChanges 224
Tableau 105 – Facette Client Abonnement durable 224
Tableau 106 – Facette Client DataAccess 225
Tableau 107 – Facette Client Abonné aux Evénements 225

Tableau 108 – Facette Client Traitement des Evénements de base 226
Tableau 109 – Facette Client Hiérarchie de Notification et de Source 226
Tableau 110 – Facette Client A & C Condition de base 226
Tableau 111 – Facette Client A & C Refresh2 227
Tableau 112 – Facette Client A & C Instance Espace d'adressage 227
Tableau 113 – Facette Client A & C Activer 227
Tableau 114 – Facette Client A & C AlarmMetrics 227
Tableau 115 – Facette Client A & C Alarme 228
Tableau 116 – Facette Client A & C Alarme exclusive 228
Tableau 117 – Facette Client A & C Alarme non exclusive 229
Tableau 118 – Facette Client A & C Instances précédentes 229
Tableau 119 – Facette Client A & C Dialogue 229
Tableau 120 – Facette Client A & C CertificateExpiration 229
Tableau 121 – Facette Proxy A & E 230
Tableau 122 – Facette Client Méthode 231
Tableau 123 – Facette Client Audit 231
Tableau 124 – Facette Client Gestion des Nœuds 231
Tableau 125 – Facette Client Programmation de type avancé 232
Tableau 126 – Facette Client Gestion des Rôles d'Utilisateurs 232
Tableau 127 – Facette Client Diagramme d'état 232
Tableau 128 – Facette Client Diagnostic 232
Tableau 129 – Facette Client Redondant 233
Tableau 130 – Facette Client Commutateur de redondance 233
Tableau 131 – Facette Client Accès à l'historique 233
Tableau 132 – Facette Client Données Historiques AtTime 233
Tableau 133 – Facette Client Agrégat Historique 234
Tableau 134 – Facette Client Annotation Historique 235
Tableau 135 – Facette Client Accès à l'Historique Données Modifiées 235
Tableau 136 – Facette Client Insertion Données Historiques 235
Tableau 137 – Facette Client Mise à Jour Données Historiques 235
Tableau 138 – Facette Client Remplacement données historiques 236
Tableau 139 – Facette Client Suppression données historiques 236
Tableau 140 – Facette Client Accès à l'historique Horodatage Serveur 236
Tableau 141 – Facette Client Accès données structurées historiques 236
Tableau 142 – Facette Client données structurées historiques AtTime 236
Tableau 143 – Facette Client données structurées historiques modifiées 237
Tableau 144 – Facette Client Insérer données structurées historiques 237
Tableau 145 – Facette Client Mettre à jour données structurées historiques 237
Tableau 146 – Facette Client Remplacer données structurées historiques 237
Tableau 147 – Facette Client Supprimer données structurées historiques 238
Tableau 148 – Facette Client Evénements Historiques 238

Tableau 149 – Facette Client Insertion Evénements Historiques 238
Tableau 150 – Facette Client Mise à Jour Evénements Historiques 238
Tableau 151 – Facette Client Remplacement Evénements Historiques 239
Tableau 152 – Facette Client Suppression Evénements Historiques 239
Tableau 153 – Facette Client Abonné aux Agrégats 239
Tableau 154 – Profil 2017 Client UA normalisé 241
Tableau 155 – Profil UA binaire UA-TCP UA-SC 241
Tableau 156 – Profil USA binaire HTTPS 241
Tableau 157 – Protocole de transport XML UA HTTPS 242
Tableau 158 – Protocole de transport UA JSON HTTPS 242
Tableau 159 – Profil UA binaire WSS UA-SC 242
Tableau 160 – Protocole de transport UA JSON WSS 243
Tableau 161 – Sécurité utilisateur Contrôle accès complet 243
Tableau 162 – Sécurité utilisateur Contrôle accès de base 243
Tableau 163 – Synchronisation Temporelle Sécurité 243
Tableau 164 – Meilleures pratiques – Evénements d'audit 244
Tableau 165 – Meilleures pratiques – Gestion d'alarmes 244
Tableau 166 – Meilleures pratiques – Nombres aléatoires 244
Tableau 167 – Meilleures pratiques – Temporisations 244
Tableau 168 – Meilleures pratiques – Accès administratif 245
Tableau 169 – Meilleures pratiques – Gestion stricte des messages 245
Tableau 170 – Meilleures pratiques – Client Evénements d'audit 245
Tableau 171 – Profil TransportSecurity – TLS 1.2 245
Tableau 172 – Profil TransportSecurity – TLS 1.2 avec PFS 246
Tableau 173 – SecurityPolicy – None 246
Tableau 174 – SecurityPolicy [A] – Aes128-Sha256-RsaOaep 247
Tableau 175 – SecurityPolicy [B] – Basic256Sha256) 247
Tableau 176 – SecurityPolicy – Aes256-Sha256-RsaPss 248
Tableau 177 – Facette Jeton Utilisateur – Anonyme 248
Tableau 178 – Facette Serveur Jeton Utilisateur – Nom d'utilisateur Mot de passe 248
Tableau 179 – Facette Serveur Jeton Utilisateur – Certificat X509 249
Tableau 180 – Facette Serveur Jeton Utilisateur – Jeton Emis 249
Tableau 181 – Facette Serveur Windows Jeton Utilisateur – Jeton Emis 249
Tableau 182 – Facette Serveur Jeton Utilisateur – JWT 249
Tableau 183 – Facette Client Jeton Utilisateur – Nom d'Utilisateur Mot de Passe 250
Tableau 184 – Facette Client Jeton Utilisateur – Certificat X509 250
Tableau 185 – Facette Client Jeton Utilisateur – Jeton Emis 250
Tableau 186 – Facette ClientWindows Jeton Utilisateur – Jeton Emis 250
Tableau 187 – Facette Client Jeton Utilisateur – JWT 251
Tableau 188 – Profil 2017 Serveur Découverte Globale 251
Tableau 189 – Serveur 2017 Découverte Globale et Gestion des Certificats 252
Tableau 190 – Profil 2017 Client Gestion Globale des Certificats 252
Tableau 191 – Facette Serveur Demande d'autorisation Service global 252

Tableau 192 – Facette Pull KeyCredential Service Global 253
Tableau 193 – Facette Push KeyCredential Service Global 253

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ARCHITECTURE UNIFIÉE OPC –

Partie 7: Profils

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62541-7 a été établie par le sous-comité 65E: Les dispositifs et leur intégration dans les systèmes de l'entreprise, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette troisième édition annule et remplace la deuxième édition parue en 2015. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) ajout de nouveaux profils fonctionnels:
   - profils pour la découverte globale et la gestion globale des certificats;
   - profils pour la gestion globale de KeyCredential et pour la gestion globale des jetons d'accès;

- facette pour les abonnements durables;
- profil client UA normalisé;
- profils pour l'administration des rôles et permissions des utilisateurs.

b) ajout de nouveaux profils de transport:
- HTTPS avec codage JSON;
- Secure WebSockets (WSS) avec codage binaire ou JSON;
- connectivité inversée.

c) ajout de nouveaux profils de sécurité:
- TransportSecurity – TLS 1.2 avec PFS (confidentialité persistante);
- SecurityPolicy [A] – Aes128-Sha256-RsaOaep (en remplacement de Base128Rsa15);
- SecurityPolicy – Aes256-Sha256-RsaPss ajoute la confidentialité persistante pour UA TCP);
- jeton d'utilisateur JWT (Jason Web Token).

d) spécification des profils de sécurité déconseillés (en raison des algorithmes cassés):
- SecurityPolicy – Basic128Rsa15 (algorithme Sha1 cassé);
- SecurityPolicy – Basic256 (algorithme Sha1 cassé);
- TransportSecurity – TLS 1.0 (algorithme RC4 cassé);
- TransportSecurity – TLS 1.1 (algorithme RC4 cassé).

e) transport déconseillé (absence de prise en charge sur la plupart des plateformes):
- SOAP/HTTP avec WS-SecureConversation (tous les codages).

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65E/707/FDIS	65E/725/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Dans l'ensemble du présent document et dans les autres parties de la série IEC 62541, certaines conventions de document sont utilisées:

Le format *italique* est utilisé pour mettre en évidence un terme défini ou une définition qui apparaît à l'article "Termes et définitions" dans l'une des parties de la série IEC 62541.

Le format *italique* est également utilisé pour mettre en évidence le nom d'un paramètre d'entrée ou de sortie de service, ou le nom d'une structure ou d'un élément de structure habituellement défini dans les tableaux.

Par ailleurs, les *termes* et les *noms en italique* sont, à quelques exceptions près, écrits en camel-case (pratique qui consiste à joindre, sans espace, les éléments des mots ou expressions composés, la première lettre de chaque élément étant en majuscule). Par exemple, le terme défini est *AddressSpace* et non Espace d'adressage. Cela permet de mieux comprendre qu'il existe une définition unique pour *AddressSpace*, et non deux définitions distinctes pour Espace et pour Adressage.

Une liste de toutes les parties de la série IEC 62541, publiées sous le titre général *Architecture unifiée OPC*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

ARCHITECTURE UNIFIÉE OPC –

Partie 7: Profils

1 Domaine d'application

La présente partie de l'IEC 62541 définit les *Profils* de l'architecture unifiée OPC (OPC UA). Les *Profils* du présent document permettent de classer les caractéristiques en fonction des essais de produits OPC UA et de la nature des essais (via un outil ou en laboratoire). Cela inclut les essais effectués à l'aide de l'outil d'essai de conformité CTT OPC UA développé par la Fondation OPC (outil d'essai autonome), ainsi que les essais réalisés par des laboratoires de certification indépendants de cette même fondation. Le présent document peut également faire référence aux outils d'essai ou au laboratoire d'essai d'un autre organisme. Dans le cas présent, l'élément important est le concept qui oppose les essais fondés sur un outil automatisé et les essais en laboratoire. Le domaine d'application de la présente norme inclut la définition d'une fonctionnalité qui ne peut être soumise à l'essai qu'en laboratoire, ainsi que la définition du regroupement des fonctionnalités à utiliser durant les essais de produits OPC UA effectués en laboratoire ou à l'aide d'outils automatisés. La définition des *TestCases* réels ne relève pas du domaine d'application du présent document, mais les catégories de *TestCases* générales relèvent du domaine d'application du présent document.

La plupart des applications OPC UA sont conformes à plusieurs *Profils*, mais pas à l'ensemble des *Profils*.

2 Références normatives

Les documents ci-après sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TR 62541-1*, OPC Unified Architecture – Part 1: Overview and Concepts* (disponible en anglais seulement)

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security Model* (disponible en anglais seulement)

IEC 62541-3, *Architecture unifiée OPC – Partie 3: Modèle d'espace d'adressage*

IEC 62541-4, *Architecture unifiée OPC – Partie 4: Services*

IEC 62541-5, *Architecture unifiée OPC – Partie 5: Modèle d'information*

IEC 62541-6, *Architecture unifiée OPC – Partie 6: Mappings*

IEC 62541-8, *Architecture unifiée OPC – Partie 8: Accès aux données*

IEC 62541-9, *Architecture unifiée OPC – Partie 9: Alarmes et conditions*

IEC 62541-11, *Architecture unifiée OPC – Partie 11: Accès à l'historique*

IEC 62541-12, *Architecture unifiée OPC – Partie 12: Services globaux et de découverte*

IEC 62541-13, *Architecture unifiée OPC – Partie 13: Agrégats*

Compliance Part 8 UA Server: OPC Test Lab Specification: Part 8 – UA Server
http://www.opcfoundation.org/Test/Part8/

Compliance Part 9 UA Client: OPC Test Lab Specification: Part 9 – UA Client
http://www.opcfoundation.org/Test/Part9/