

# DIN CEN/TS 15480-2:2012-09 (E)

## Identification card systems - European Citizen Card - Part 2: Logical data structures and security services ; English version CEN/TS 15480-2:2012

---

<b>Contents</b>		<b>Page</b>
Foreword .....		4
<b>1</b>	<b>Scope .....</b>	<b>5</b>
<b>2</b>	<b>Normative references .....</b>	<b>5</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>6</b>
<b>4</b>	<b>Abbreviations .....</b>	<b>7</b>
4.1	Abbreviations .....	7
4.2	Coding conventions and notation .....	9
<b>5</b>	<b>Data elements and data structures .....</b>	<b>10</b>
5.1	Supported data Structures .....	10
5.2	Access to data structures .....	10
5.3	Answer to reset (ATR) / answer to select (ATS) .....	11
5.4	General architecture and file supported .....	15
5.5	Selection of data structures .....	16
5.6	Access to files .....	17
<b>6</b>	<b>Basic card services .....</b>	<b>18</b>
6.1	General .....	18
6.2	Identification .....	18
6.3	User verification .....	20
6.4	Device authentication .....	20
6.5	Digital signature .....	23
6.6	Client/Server Authentication .....	24
6.7	Encryption key decipherment .....	24
<b>7</b>	<b>Extended card services .....</b>	<b>25</b>
7.1	General .....	25
7.2	Biometrics - on card matching .....	25
7.3	Passive Authentication .....	25
7.4	Basic Access Control .....	25
7.5	Active Authentication .....	25
7.6	Extended Access Control .....	26
7.7	Role authentication .....	26
7.8	Restricted Identification (RI) .....	27
7.9	Age, Validity or Auxiliary Data Verification .....	28
7.10	Modular Enhanced Role Authentication (mERA) .....	28
<b>Annex A (normative) Command set .....</b>		<b>29</b>
<b>A.1</b>	<b>CLASS byte coding .....</b>	<b>29</b>
<b>A.2</b>	<b>Command chaining mechanisms .....</b>	<b>29</b>
<b>A.3</b>	<b>Extended length mechanism .....</b>	<b>30</b>
<b>A.4</b>	<b>Logical channels .....</b>	<b>31</b>
<b>A.5</b>	<b>Short and extended length fields .....</b>	<b>31</b>
<b>A.6</b>	<b>Status words .....</b>	<b>31</b>
<b>A.7</b>	<b>Command set .....</b>	<b>32</b>

<b>Annex B (normative) Cryptographic Information Application</b>	<b>54</b>
<b>B.1 Description</b>	<b>54</b>
<b>B.2 CIA data organisation</b>	<b>63</b>
<b>Annex C (normative) Mandatory features</b>	<b>83</b>
<b>C.1 General</b>	<b>83</b>
<b>C.2 Data elements and data structures</b>	<b>83</b>
<b>DIN CEN/TS 15480-2 (DIN SPEC 91130-2):2012-09 CEN/TS 15480-2:2012 (E) C.3 Card services</b>	<b>84</b>
<b>C.4 Command set</b>	<b>84</b>
<b>C.5 Device Authentication and Key Derivation</b>	<b>85</b>
<b>C.6 Digital signature</b>	<b>85</b>
<b>C.7 Client/Server Authentication</b>	<b>86</b>
<b>C.8 Encryption Key Decipherment</b>	<b>86</b>
<b>Annex D (informative) Optional features</b>	<b>87</b>
<b>D.1 General</b>	<b>87</b>
<b>D.2 Data elements and data structures</b>	<b>87</b>
<b>D.3 Card services</b>	<b>88</b>
<b>D.4 Command set</b>	<b>88</b>
<b>D.5 Device Authentication and Key Derivation</b>	<b>89</b>
<b>D.6 Digital signature</b>	<b>89</b>
<b>Annex E (informative) Application Profiles</b>	<b>90</b>
<b>E.1 General</b>	<b>90</b>
<b>E.2 Application Profile 1: ICAO Application with EAC features</b>	<b>90</b>
<b>E.3 Application Profile 2: Travel Document Application</b>	<b>96</b>
<b>E.4 Application Profile 3: eID Application</b>	<b>101</b>
<b>E.5 Application Profile 4: Digital Signature Application</b>	<b>111</b>
<b>E.6 Application Profile 5: eServices Application using a trusted third party</b>	<b>121</b>
<b>E.7 Application Profile 6: Health Insurance Application</b>	<b>136</b>
<b>E.8 Application Profile 7: Combined eID and signature application</b>	<b>152</b>
<b>E.9 Application Profile 8: Multi-Service application</b>	<b>156</b>
<b>Annex F (informative) Access rules in expanded format</b>	<b>161</b>
<b>F.1 Object protection by access rules in expanded format</b>	<b>161</b>
<b>F.2 Access rules in expanded format</b>	<b>161</b>
<b>F.3 Security attribute referencing expanded format</b>	<b>162</b>
<b>F.4 Security attribute template for physical interfaces</b>	<b>163</b>
<b>Annex G (informative) Example of data structure: the Security Data Objects concept</b>	<b>164</b>
<b>G.1 SDO concept</b>	<b>164</b>
<b>Bibliography</b>	<b>176</b>