

# DIN EN 419212-3:2017-11 (E)

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols; English version EN 419212-3:2017

---

<b>Contents</b>	<b>Page</b>
European foreword.....	5
Introduction .....	6
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions .....	7
4 Symbols and abbreviations .....	15
5 Management Summary .....	18
5.1 Motivation.....	18
5.2 What is in behind?.....	19
5.3 Use Cases .....	20
5.4 Privacy and Security.....	21
5.5 Overview - EU Directive and Regulation.....	21
5.6 Facts and Figures.....	22
Annex A (normative) Algorithm Identifiers — Coding and specification .....	23
Table A.1 — AlgIDs.....	24
Table A.2 — Coding of byte 3 and 4 (for hash calculation - byte 2 = '01' to '0F').....	24
Table A.3 — Coding of byte 3 (for digital signature computation - byte 2 = '1x') .....	25
Table A.4 — Coding of byte 4 (for digital signature computation - byte 2 = '1x') .....	25
Table A.5 — Coding of byte 3 (for C/S authentication - byte 2 = '2x').....	25
Table A.6 — Coding of byte 4 (for C/S authentication - byte 2 = '2x').....	25
Table A.7 — Coding of byte 3 (for key decipherment - byte 2 = '3x').....	26
Table A.8 — Coding of byte 4 (for key decipherment - byte 2 = '3x').....	26
Table A.9 — Coding of byte 3 (for authentication protocol - byte 2 = '4x').....	26
Table A.10 — Coding of byte 4 (for authentication protocol - byte 2 = '4x') .....	28
Table A.11 — Coding of byte 3 (for digital signature verification - byte 2 = '9x').....	28
Table A.12 — Coding of byte 4 (for digital signature verification - byte 2 = '9x').....	28
Table A.13 — Coding of byte 3 (for role authentication - byte 2 = 'Ax').....	29
Table A.14 — Coding of byte 3 (for privacy features - byte 2 = 'Cx') .....	29
Table A.15 — Coding of byte 4 (for role authentication - byte 2 = 'Ax').....	29
Table A.16 — Coding of byte 4 (for privacy feature - byte 2 = 'Cx') .....	29
Table A.17 — 1-byte Algorithm-ID coding.....	30
Annex B (informative) OID values.....	32
B.1 OIDs for certificate signatures.....	32
Table B.1 — Object identifier values related to a public key in a certificate.....	32
B.2 OIDs for key transport protocol.....	32

<b>Table B.2 — Object identifier values for the key transport protocol.....</b>	<b>33</b>
<b>B.3 OIDs for device authentication with privacy .....</b>	<b>33</b>
<b>Table B.3 — Object identifier values for device authentication with privacy .....</b>	<b>33</b>
<b>B.4 OIDs for password based mechanisms .....</b>	<b>34</b>
<b>Table B.4 — PACE OIDs .....</b>	<b>34</b>
<b>B.5 OIDs for mEAC protocol.....</b>	<b>34</b>
<b>B.5.1 OIDs for Chip Device Authentication .....</b>	<b>34</b>
<b>Table B.5 — Chip Device Authentication (DES/AES).....</b>	<b>34</b>
<b>B.5.2 OIDs for Terminal Device Authentication.....</b>	<b>35</b>
<b>Table B.6 — Terminal Authentication (RSA/ECDSA).....</b>	<b>35</b>
<b>B.6 OIDs for privacy protocols.....</b>	<b>36</b>
<b>B.6.1 OIDs for Restricted Identification.....</b>	<b>36</b>
<b>Table B.7 — OIDs for Restricted Identification.....</b>	<b>36</b>
<b>Table B.8 — OIDs for use in certificate extension.....</b>	<b>36</b>
<b>B.6.2 OIDs for Restricted Identification.....</b>	<b>36</b>
<b>Table B.9 — OIDs for use in auxiliary data verification.....</b>	<b>36</b>
<b>B.7 OIDs for mEAC based eServices - OIDs for Terminal Device Authentication in mEAC- based eServices .....</b>	<b>36</b>
<b>Table B.10 — OID values for the mEAC Terminal Authentication.....</b>	<b>36</b>
<b>B.8 OIDs for the PCA mechanism .....</b>	<b>37</b>
<b>Table B.11 — OID for the PCA mechanism.....</b>	<b>37</b>
<b>Annex C (informative) Build scheme for object identifiers defined by EN 419212 .....</b>	<b>38</b>
<b>Figure C.1 — Build scheme for mEAC OIDs.....</b>	<b>39</b>
<b>Annex D (informative) Tutorial on Signature Technology .....</b>	<b>40</b>
<b>D.1 General .....</b>	<b>40</b>
<b>D.2 Signatures and keys .....</b>	<b>41</b>
<b>Table D.1 — Generating RSA keys.....</b>	<b>42</b>
<b>D.3 Signing documents .....</b>	<b>42</b>
<b>D.4 About certificates.....</b>	<b>43</b>
<b>D.5 The “chain of trust” .....</b>	<b>44</b>
<b>D.6 Multi step signature generation.....</b>	<b>44</b>
<b>D.6.1 General .....</b>	<b>44</b>
<b>D.6.2 Device authentication protocols .....</b>	<b>44</b>
<b>D.6.3 Secure Messaging.....</b>	<b>45</b>
<b>D.6.4 Password based device authentication .....</b>	<b>45</b>
<b>D.6.5 PIN entry .....</b>	<b>45</b>
<b>D.7 Signing the document.....</b>	<b>46</b>

<b>Annex E (informative) Guide to the EN 419212 .....</b>	<b>47</b>
<b>E.1 From EN 14890 to EN 419212.....</b>	<b>47</b>
<b>E.2 The EU Regulation 910/2014 and the Directive 1999/93/EU.....</b>	<b>48</b>
<b>E.3 Secure Elements (SE) .....</b>	<b>48</b>
<b>E.4 Specific protection required for contactless integrated circuits .....</b>	<b>49</b>
<b>E.4.1 General.....</b>	<b>49</b>
<b>E.4.2 Eavesdropping attacks .....</b>	<b>49</b>
<b>E.4.3 Skimming attack.....</b>	<b>49</b>
<b>E.4.4 Relay attack.....</b>	<b>49</b>
<b>E.4.5 Denial of Service (DoS) attack .....</b>	<b>49</b>
<b>E.4.6 Countermeasures .....</b>	<b>50</b>
<b>E.5 The Human-Machine Interface.....</b>	<b>50</b>
<b>E.6 Communications with the ICC and with the user .....</b>	<b>50</b>
<b>E.7 Information that should be initially communicated by the ICC to the IFD .....</b>	<b>51</b>
<b>E.8 User agreement using PINs.....</b>	<b>51</b>
<b>E.9 PIN unlocking.....</b>	<b>52</b>
<b>E.10 PIN change .....</b>	<b>52</b>
<b>E.11 User agreement using biometric information .....</b>	<b>52</b>
<b>E.12 User control using a local display and a local keyboard .....</b>	<b>52</b>
<b>E.13 Card applications .....</b>	<b>53</b>
<b>E.13.1 General.....</b>	<b>53</b>
<b>E.13.2 eSign card application .....</b>	<b>53</b>
<b>E.13.3 Device authentication mechanisms.....</b>	<b>53</b>
<b>E.13.4 Document Decryption mechanisms .....</b>	<b>53</b>
<b>E.14 Signature-/Seal functions.....</b>	<b>53</b>
<b>E.14.1 General.....</b>	<b>53</b>
<b>E.14.2 Digital signature/seal creation .....</b>	<b>54</b>
<b>E.14.3 Digital signature verification.....</b>	<b>54</b>
<b>E.14.4 Identification and authentication service.....</b>	<b>54</b>
<b>Bibliography.....</b>	<b>56</b>