

# DIN EN 419212-5:2018-06 (E)

## Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService; English version EN 419212-5:2018

---

<b>Contents</b>	<b>Page</b>
European foreword.....	4
Introduction .....	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions .....	6
4 Abbreviations and notation.....	6
5 Additional Service Selection.....	6
6 Client/Server Authentication .....	10
6.1 General.....	10
6.2 Client/Server protocols .....	10
6.3 Steps preceding the client/server authentication .....	11
6.4 Padding format .....	11
6.4.1 PKCS #1 v 1-5 Padding.....	11
6.4.2 PKCS #1 V 2.x (PSS) Padding.....	12
6.4.3 Building the DSI on ECDSA .....	13
6.5 Client/Server protocol .....	13
6.5.1 General.....	13
6.5.2 Step 1 — Read certificate .....	14
6.5.3 Step 2 — Set signing key for client/server internal authentication .....	15
6.5.4 Step 3 — Internal authentication .....	16
6.5.5 Client/Server authentication execution flow.....	18
6.5.6 Command data field for the client server authentication .....	19
7 Role Authentication.....	20
7.1 Role Authentication of the card .....	20
7.2 Role Authentication of the server .....	20
7.3 Symmetrical external authentication.....	20
7.3.1 Protocol .....	20
7.3.2 Description of the cryptographic mechanisms .....	24
7.3.3 Role description.....	25
7.4 Asymmetric external authentication .....	25
7.4.1 Protocol based on RSA.....	25
8 Symmetric key transmission between a remote server and the ICC.....	28
8.1 Steps preceding the key transport.....	28
8.2 Key encryption with RSA .....	28
8.2.1 General.....	28
8.2.2 PKCS#1 v1.5 padding.....	30
8.2.3 OAEP padding.....	30
8.2.4 Execution flow .....	31
8.3 Diffie-Hellman key exchange for key encipherment.....	33
8.3.1 General.....	33
8.3.2 Execution flow .....	35

<b>9</b>	<b>Signature verification .....</b>	<b>37</b>
<b>9.1</b>	<b>General.....</b>	<b>37</b>
<b>9.2</b>	<b>Signature verification execution flow.....</b>	<b>37</b>
<b>9.2.1</b>	<b>General .....</b>	<b>37</b>
<b>9.2.2</b>	<b>Step 1: Receive Hash.....</b>	<b>37</b>
<b>9.2.3</b>	<b>Step 2: Select verification key .....</b>	<b>39</b>
<b>9.2.4</b>	<b>Step 3: Verify digital signature .....</b>	<b>39</b>
<b>10</b>	<b>Certificates for additional services .....</b>	<b>40</b>
<b>10.1</b>	<b>File structure.....</b>	<b>40</b>
<b>10.2</b>	<b>File structure.....</b>	<b>41</b>
<b>10.3</b>	<b>EF.C_X509.CH.DS.....</b>	<b>41</b>
<b>10.4</b>	<b>EF.C.CH.AUT .....</b>	<b>41</b>
<b>10.5</b>	<b>EF.C.CH.KE.....</b>	<b>42</b>
<b>10.6</b>	<b>Reading Certificates and the public key of CAs.....</b>	<b>42</b>
<b>11</b>	<b>APDU data structures.....</b>	<b>42</b>
<b>11.1</b>	<b>Algorithm Identifiers.....</b>	<b>42</b>
<b>11.2</b>	<b>General .....</b>	<b>42</b>
<b>11.3</b>	<b>CRTs.....</b>	<b>43</b>
<b>11.3.1</b>	<b>General .....</b>	<b>43</b>
<b>11.3.2</b>	<b>CRT DST for selection of ICC's private client/server auth. key .....</b>	<b>43</b>
<b>11.3.3</b>	<b>CRT AT for selection of ICC's private client/server auth. key.....</b>	<b>43</b>
<b>11.3.4</b>	<b>CRT CT for selection of ICC's private key.....</b>	<b>44</b>
<b>11.3.5</b>	<b>CRT DST for selection of IFD's public key (signature verification) .....</b>	<b>44</b>
	<b>Annex A (informative) Security Service Descriptor Templates.....</b>	<b>45</b>
	<b>Annex B (informative) Example of DF.CIA .....</b>	<b>51</b>
	<b>Bibliography .....</b>	<b>58</b>