

# Key Flow — Version 0.3

Command.. ..Nano	CAM	Card
01 01 .. ..28 (0D)	Change Provider ID (Very Rare) PP+ 00+ EMK + PRID + SIG	<p>PRID</p> <p>PMK</p> <p>Prov00</p> <p>Prov10</p> <p>Key (kn)</p> <p>00</p> <p>01</p> <p>02</p> <p>03</p> <p>..</p> <p>..</p> <p>0F</p> <p>10</p> <p>11</p>
01 01 .. .. 10 (xx)	Key Update (approx every 60~30 sec) (1 or more (kn+ EPK)) + SIG	<p>PK</p> <p>Key Algo</p> <p>DATE + PMK</p> <p>EPK</p> <p>Sig Algo</p> <p>00</p> <p>01</p> <p>02</p> <p>03</p> <p>..</p> <p>..</p> <p>0F</p> <p>10</p> <p>11</p>
01 05 .. .. 78 (12)	Entitlement (approx every 10 sec) kn + i + EK <sub>1</sub> + EK <sub>2</sub> + SIG If DK <sub>i</sub> is correct, then Pictures!	<p>DK<sub>i</sub></p> <p>Key Algo</p> <p>DATE + PK<sub>kn</sub></p> <p>EK<sub>i</sub></p> <p>Sig Algo</p> <p>00</p> <p>01</p> <p>02</p> <p>03</p> <p>..</p> <p>..</p> <p>0F</p> <p>10</p> <p>11</p>
	<b>Code Bytes Meaning</b> PP 1 00=Prov00,11=Prov10 PRID 3 ProviderID EMK 8 Encrypted Master Key HMK 10 Hex Master Key PMK 8 Plain Master Key SIG 5 Signature	<b>Code Bytes Meaning</b> EPK 8 Encrypted Plain Key PK 8 Plain Key kn 1 Key number i 1 Selects EK <sub>1</sub> or EK <sub>2</sub> EK 8 Encrypted Key DK 8 Decrypted Key
		<b>Notes:</b> SigAlgo not included in DPSC (Wafer) cards. CoCo and ChID changes not shown. Read in conjunction with “Activate” by 007.4, “MOSC Compendium” by KuBand, and “Newbies Guide for Experimenting with Smartcards” by KuBand