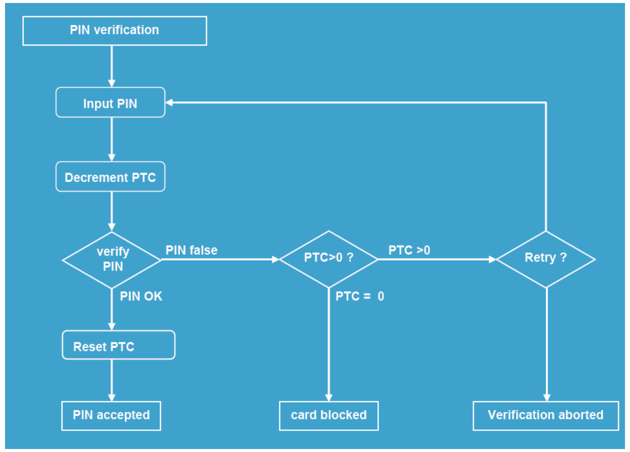
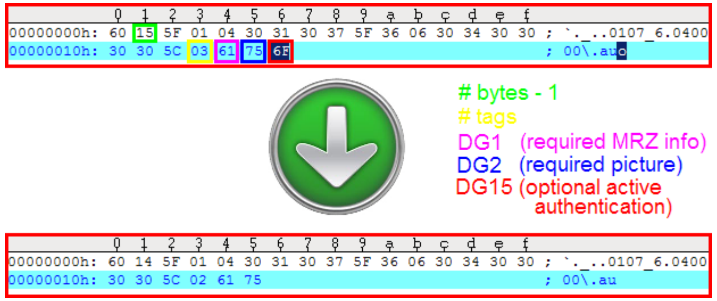
REMOTE ATTACKS

- Goal is to find a weakness in the software
- Cryptanalysis
  - e.g. weakness in the SHA-1
- Protocol analysis
  - e.g. contactless ISO 14443
- Cryptographic API
  - e.g. Java Card API
- Security API
  - e.g. financial API or ICAO
- Man in the middle attack

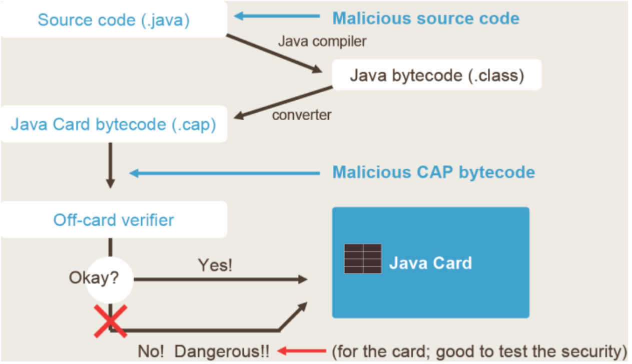




```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 60 15 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; `._..0107_6.0400
00000010h: 30 30 5C 03 61 75 6F                            ; 00\.auo
```

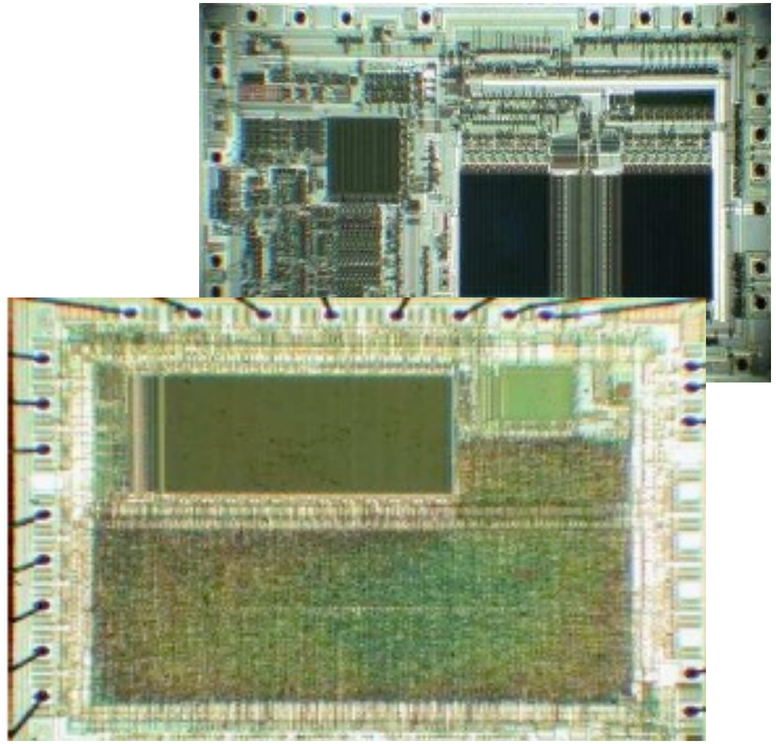
# bytes - 1
# tags
DG1 (required MRZ info)
DG2 (required picture)
DG15 (optional active authentication)

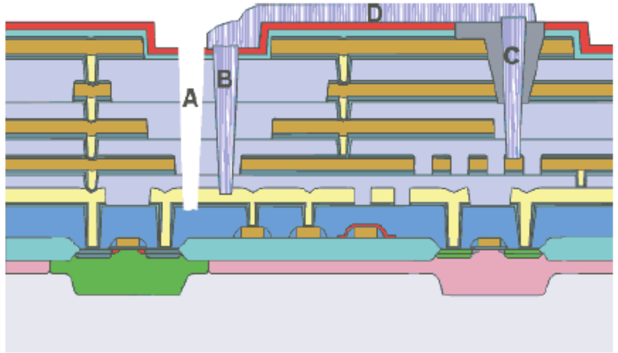
```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 60 14 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; `._..0107_6.0400
00000010h: 30 30 5C 02 61 75                               ; 00\.au
```



COUNTER MEASURES – HARDWARE

- Sensors (Voltage, Clock, Temperature, Light)
- Filters (protection against spikes/glitches)
- Independent internal clock (not the reader CLK)
- Single Fault Injection (SFI) detection mechanisms
- Passive and active shields
- Glue logic (hard to reverse engineer circuitry)
- Handshaking circuit
- Dense multi layer technology
- Bus and memory encryption
- Virtual addressing (SW address != HW address)
- Hardware error detection (checksums)
- True random number generator (RNG)
- Noise generation (against side channel attacks)
- Pre-silicon power analysis
- ...





COUNTER MEASURES – SOFTWARE – OS

- Sensitive information encrypted (keys, pins)
- Double executions (e.g. encrypt → decrypt for verification)
- Checksums
- Program flow verification
- Unpredictable timing (e.g. random NOP)
- Defined API access (Java Card)
  - No direct access to HW platform, HAL (assembler), C
  - Prevent buffer overflow
  - Prevent wrong offset ..
- Firewall mechanisms (between JC Applets and native applications)
- Read after write
- Exception counters
- Executed code verification (for Java Card: bytecode verification)
- Zeroing o f keys and pins
- …