Enough to go to the Moon (and back)
JavaCard™ Technology

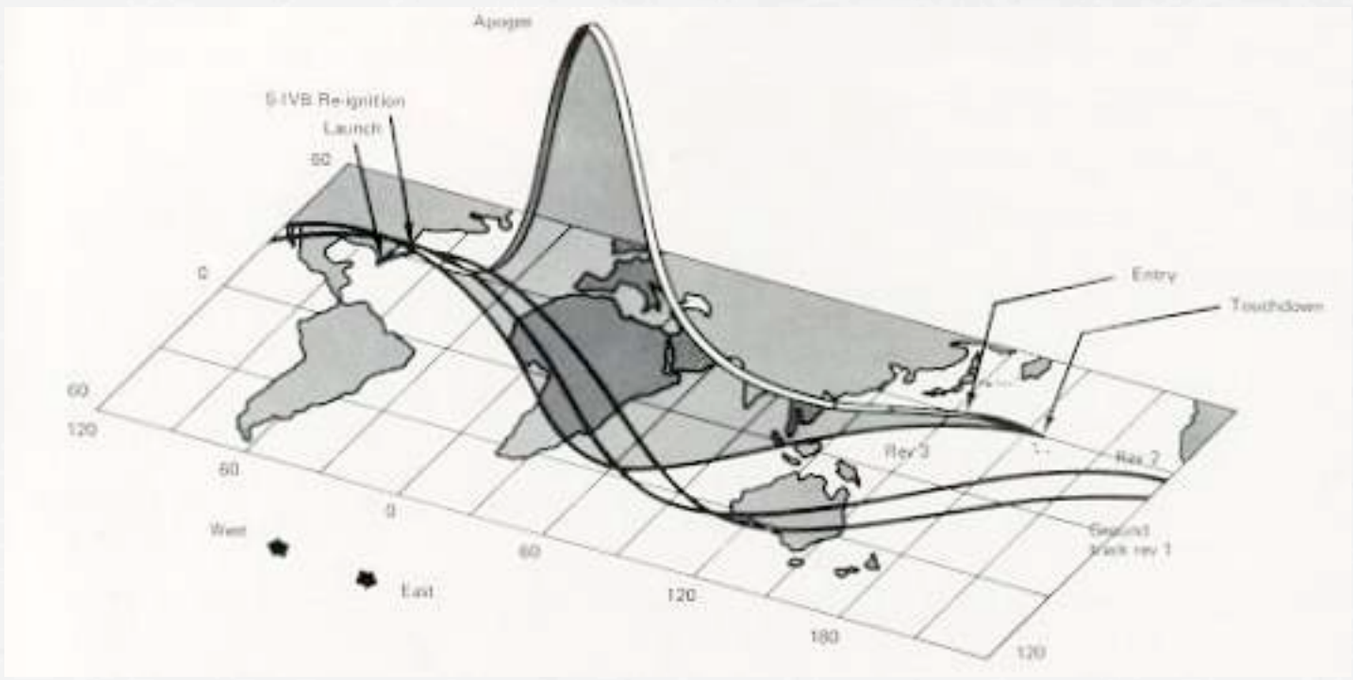
Dr. Thorsten Kramp, Thomas Weigold
IBM Zurich Research Laboratory

{thk,twe}@zurich.ibm.com

IBM®

Flight Plan

- SmartCard Technology
- JavaCard Technology
- IBM JCOP
- Demo
- Outlook



SmartCard Hardware

CPU
8-32 Bit

Crypto-
Units

I/O
- 800 Kbps

RAM
1-8 KB

EEPROM
4-72 KB

ROM
- 200 KB

IBM

Tamper Resistance

- Shielding against microprobing
- Sensors (glitch, light, temperature, …)
- Randomized chip layout
- Randomized clock
- Unified power consumption
- Memory encryption

IBM

Apollo 11 GC

- 2-Mhz CPU
- 16 Bit Word Length
- 2 KB RAM
- 36 KB ROM

- http://www.apollosaturn.com/gnc.htm
  http://www.digitalmist.com/plethorama/apollogc.htm

IBM

Smart “cards” in the Wild

IBM

Proprietary vs...

- File-System-Based
- Programming in assembly and/or C
- Vendor Lock-In
  - OS & applications from single vendor
  - Moving to another vendor becomes cost/time intensive

IBM

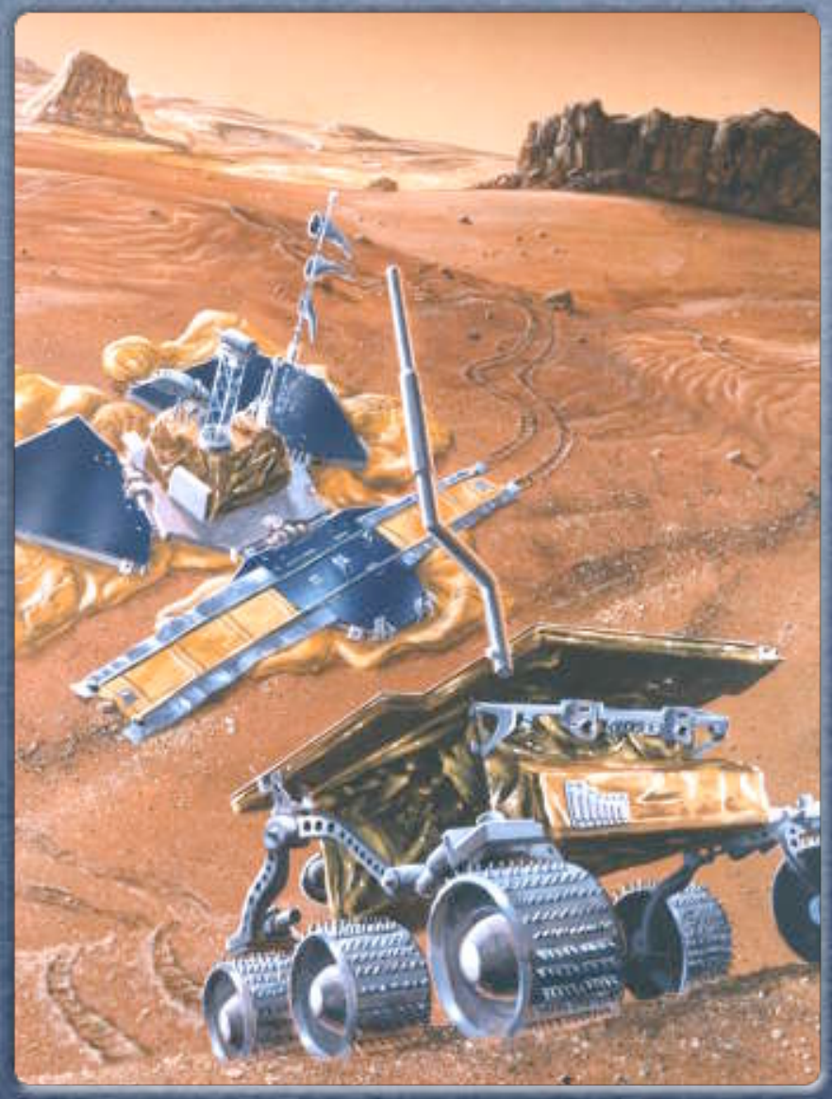
...Open

- Hardware abstraction (VM)
- High-level programming language
  - Object-oriented
- Open Standards
- PC Model: Hardware/OS/Applications

IBM

JavaCard*
(& Global Platform)

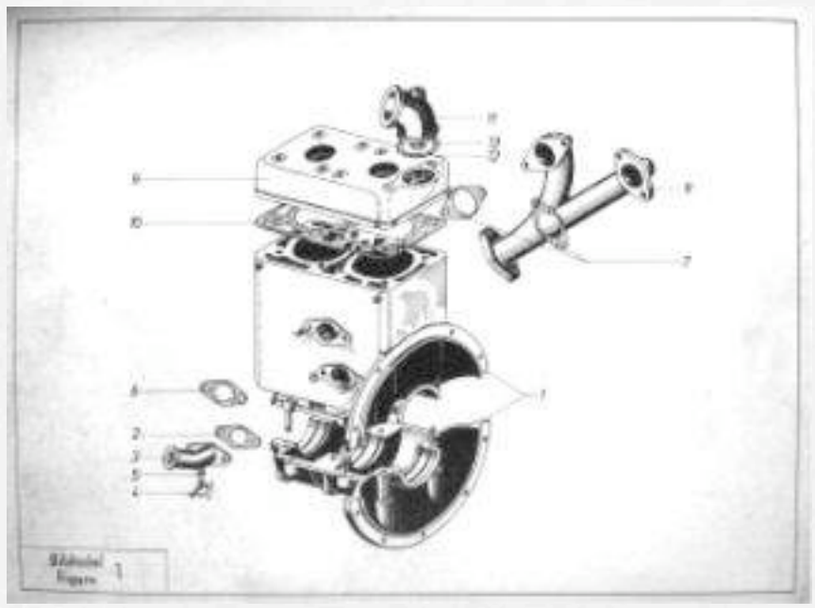
“The Master Plan”



IBM®

*JavaCard is a trademark of Sun Microsystems Inc. in the United States and other Countries.

JavaCard VM



- Extended memory model
- Transactions
- No threads (but multi application)
- Java Programming Language
  - Subset: No `float`, optional `int`

IBM

JavaCard Security

- sandboxing
- Firewall (applet isolation/sharing)
- Byte-code verification
  - Off-card (signed applets)
  - On-card verification on the horizon

IBM

Global Platform

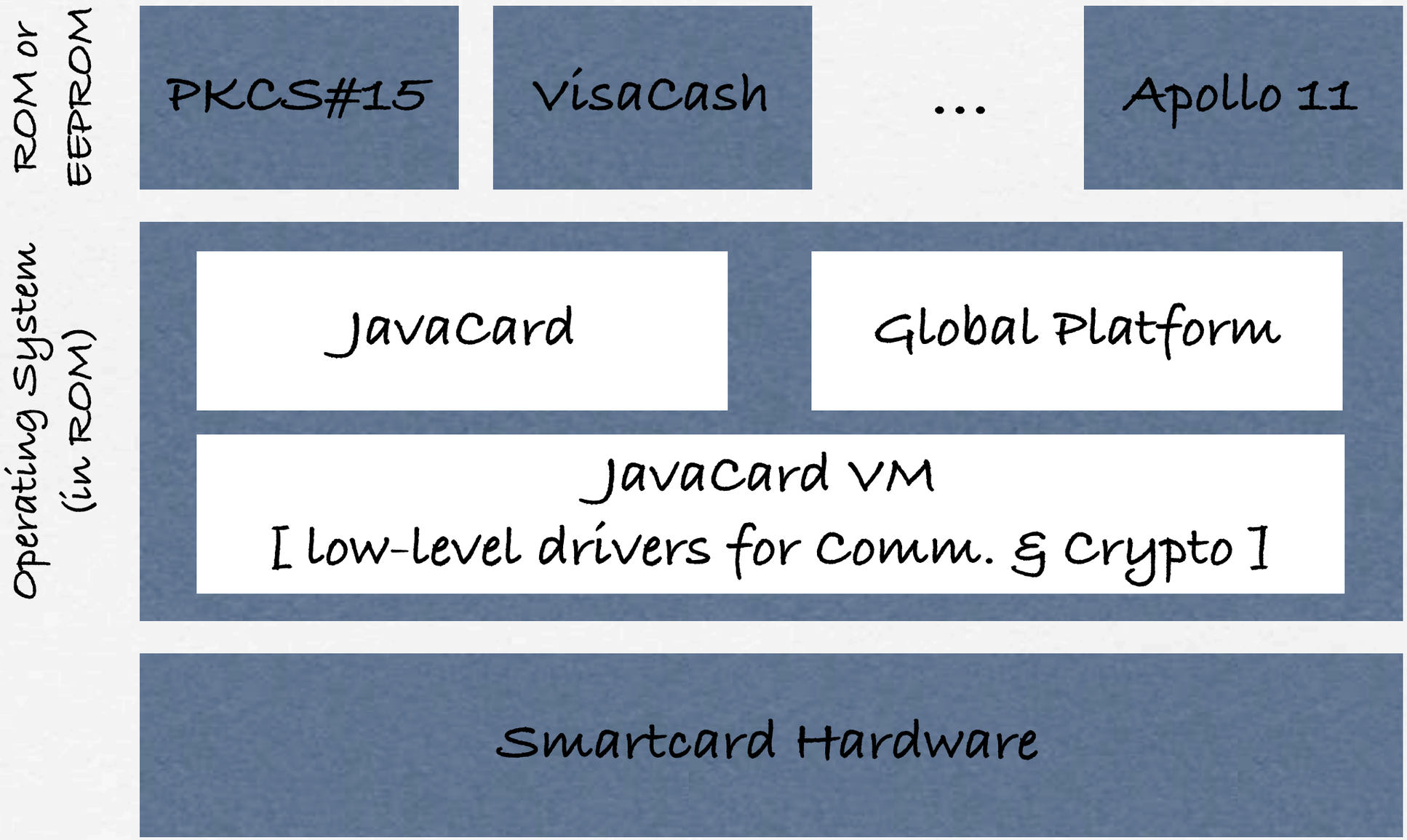
- Multi-Application Token-Security Framework
- Applet loading, installation, removal
- Secure Messaging
- Security Domains

JC/GP Standard APIs

- JavaCard
  - Applet Base, Communication, ...
  - Crypto: Ciphers, Digests, Key Mgmt
- Global Platform
  - Secure Messaging

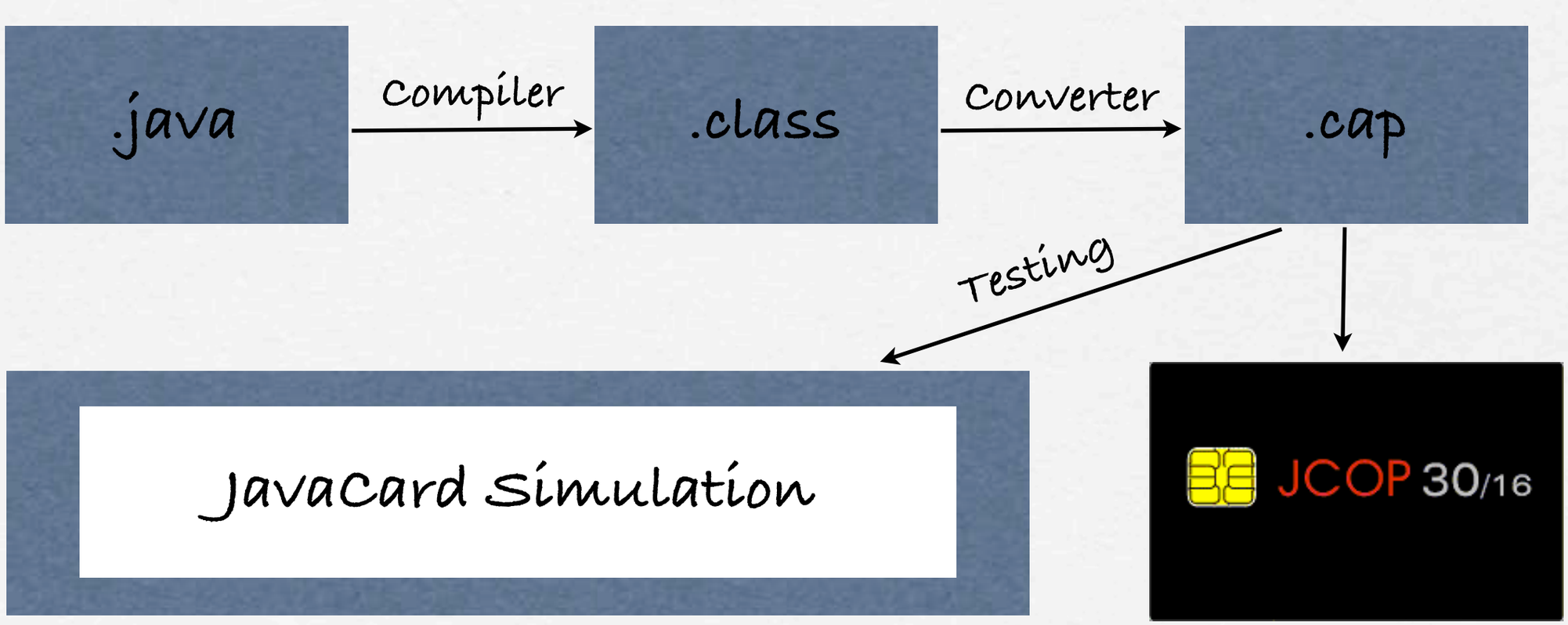
IBM

JC/GP Architecture



JavaCard Development

- very close to Java development



IBM

JCOP Debug - UBSign.java - Eclipse Platform

File Edit Source Refactor Navigate Search Project Run Window Help

Debug

<terminated> UBSign [IBM JCOP Card Simulator]
<terminated> IBM JCOP 20
<terminated> UBSign [IBM JCOP Card Simulator]
<terminated> IBM JCOP 20
UBSign [IBM JCOP Card Simulator]
JCOP Debug Target
System Thread [JCOP Main Thread] (Suspended (breakpoint at line 1
UBSign.process(APDU) line: 157
IBM JCOP 20

Variables

byte[] outLength= byte[2] (id=35084)
byte[] outRange= byte[2] (id=35075)
byte pinChanged= 0 [0x0]
boolean[] pinOk= boolean[2] (id=35136)
Signature sig= Signature (id=35119)
byte timeout= 0 [0x0]
APDU apdu= APDU (id=11710)
byte[] buf= byte[261] (id=2)
byte[] [0..99]
byte[] [100..199]
byte[] [200..260]

Variables Breakpoints Memory Information

JCOP Shell

```
Card Manager AID   :  A000000003000000
Card Manager state :  OP_READY

    Application:  SELECTABLE (--------) 0F55425369676E
    Load File  :      LOADED (--------) A0000000620001   (java.lar
    Load File  :      LOADED (--------) A0000000620101   (javacard
    Load File  :      LOADED (--------) A0000000620102   (javacard
    Load File  :      LOADED (--------) A0000000620201   (javacard
    Load File  :      LOADED (--------) A0000000030000   (visa.ope
    Load File  :      LOADED (--------) 0F5542536967
cm>  change-pin 3 1234
 => 80 24 00 03 08 68 B0 8D 10 3A 43 04 B4            .$...h...:C
 (10 msec)
 <= 90 00                                             ..
Status: No Error
cm>  /send 00a4040007f55425369676e
 => 00 A4 04 00 07 0F 55 42 53 69 67 6E               ......UBSig
 (20 msec)
 <= 90 00                                             ..
Status: No Error
cm>  i-u 255
 => 80 50 00 00 08 56 0D 95 20 69 A5 85 C4 00         .P...V.. i..
 (10 msec)
 <= 00 00 31 48 12 34 56 78 98 76 FF 01 50 57 16 48   ..1H.4Vx.v..PW.H
    B0 A0 12 62 1C D0 5D E3 41 E0 68 50 90 00         ...b..].A.hP..
Status: No Error
cm>  e-a enc
 => 84 82 03 00 10 03 2F BB 20 AD C0 81 77 DA D8 D9   ....../. ...w...
    49 E6 C4 1B 13                                    I....
 (30 msec)
 <= 90 00                                             ..
Status: No Error
cm>  send 80f0000023000000000001020304050607080090a0b0c0d0e0f444553
 => 84 F0 00 00 30 06 7B 91 CF 76 57 AB 3F C0 26 26   ....0.{..vW.?.&&
    6B 0E 25 C3 46 12 9B BF 6A E9 BD F9 DC 26 D4 3E   k.%.F...j....&.>
    1B 8D 0A 03 B0 F4 52 8F DD E0 29 31 37 85 FD 40   ......R...)17..@
    1A BB A3 68 8E                                    ...h.
cm>
```

Package Explorer

UBSign
src
com.ibm.ubsign
UBSign.java
JCOP_HOME/apis/JCOP20/api.zip - C:
scripts

Package Explorer JCOP Explorer

CAP File Properties

	Size
Package: com.ibm.ubsign	
Package AID: 0f5542536967	
Built:6/16/03 9:32:08 AM CEST	
Component sizes	
Classes	12
Methods	900
Statics	10
RefLocs	115
Constant pool	170
Package Sizes	
Download	162
Runtime code	944
Runtime data	54

CAP File Properties Properties

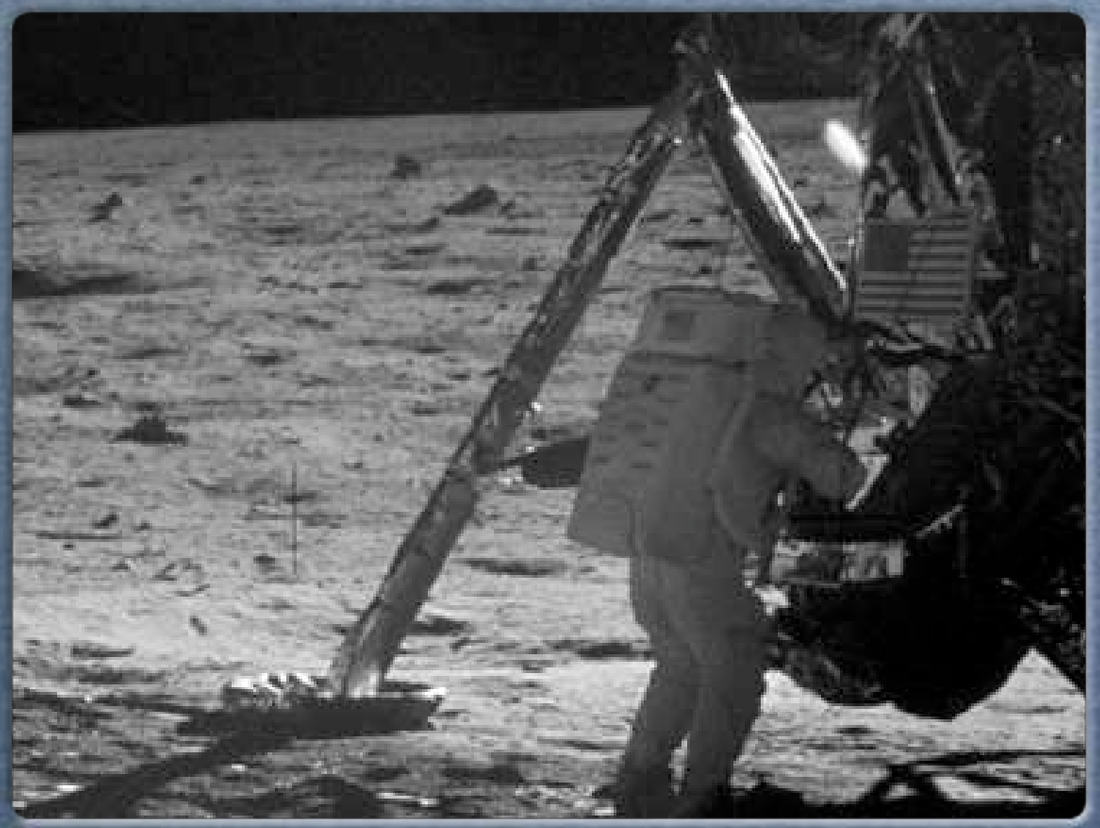
Welcome | Welcome | UBSign.java | ubsign-init.jcsh

```
            // send response
            apdu.setOutgoingAndSend(ISO7816.OFFSET_CDATA,buf[ISO7
            break;
          case VOP_EXTERNAL_AUTHENTICATE:
            // secure channel with encryption required
            if ((domain == null) || (buf[ISO7816.OFFSET_P1] != (b
              ISOException.throwIt(ISO7816.SW_CONDITIONS_NOT_SATI

            domain.verifyExternalAuthenticate(channel,apdu);

                                  // no explicit response
            break;
          case PERSONALISE:
            if (domain == null)
              ISOException.throwIt(ISO7816.SW_SECURITY_STATUS_NOT_

            domain.unwrap(channel,apdu);

            // personalise counter, pin change flag, 3DES key, la
            // timeout, out range, and out length
            highCounter = buf[ISO7816.OFFSET_CDATA];
            lowCounter = Util.getShort(buf,(short)(ISO7816.OFFSET_
            pinChanged  = buf[(short)(ISO7816.OFFSET_CDATA+3)];

            key = (DESKey)KeyBuilder.buildKey(KeyBuilder.TYPE_DES,
            key.setKey(buf,(short)(ISO7816.OFFSET_CDATA+4));
            sig.init(key,Signature.MODE_SIGN);

            language     = Util.getShort(buf,(short)(ISO7816.OFFSE
            timeout      = buf[ISO7816.OFFSET_CDATA+22];
            outRange[0]  = buf[ISO7816.OFFSET_CDATA+23];
            outRange[1]  = buf[ISO7816.OFFSET_CDATA+24];
            outLength[0] = buf[ISO7816.OFFSET_CDATA+25];
            outLength[1] = buf[ISO7816.OFFSET_CDATA+26];

            if (buf[ISO7816.OFFSET_LC] > 0x1b)
              Util.arrayCopyNonAtomic(buf,(short)(ISO7816.OFFSET_C
                                      (short)(buf[ISO7816.OFFSET_L

            OPSystem.setCardContentState(OPSystem.APPLET_PERSONALI

            // no explicit response
```

Console [JCOP Debug Target]

```
IBM JCOP card simulator (built: May 28 2003  16:24:39)
```

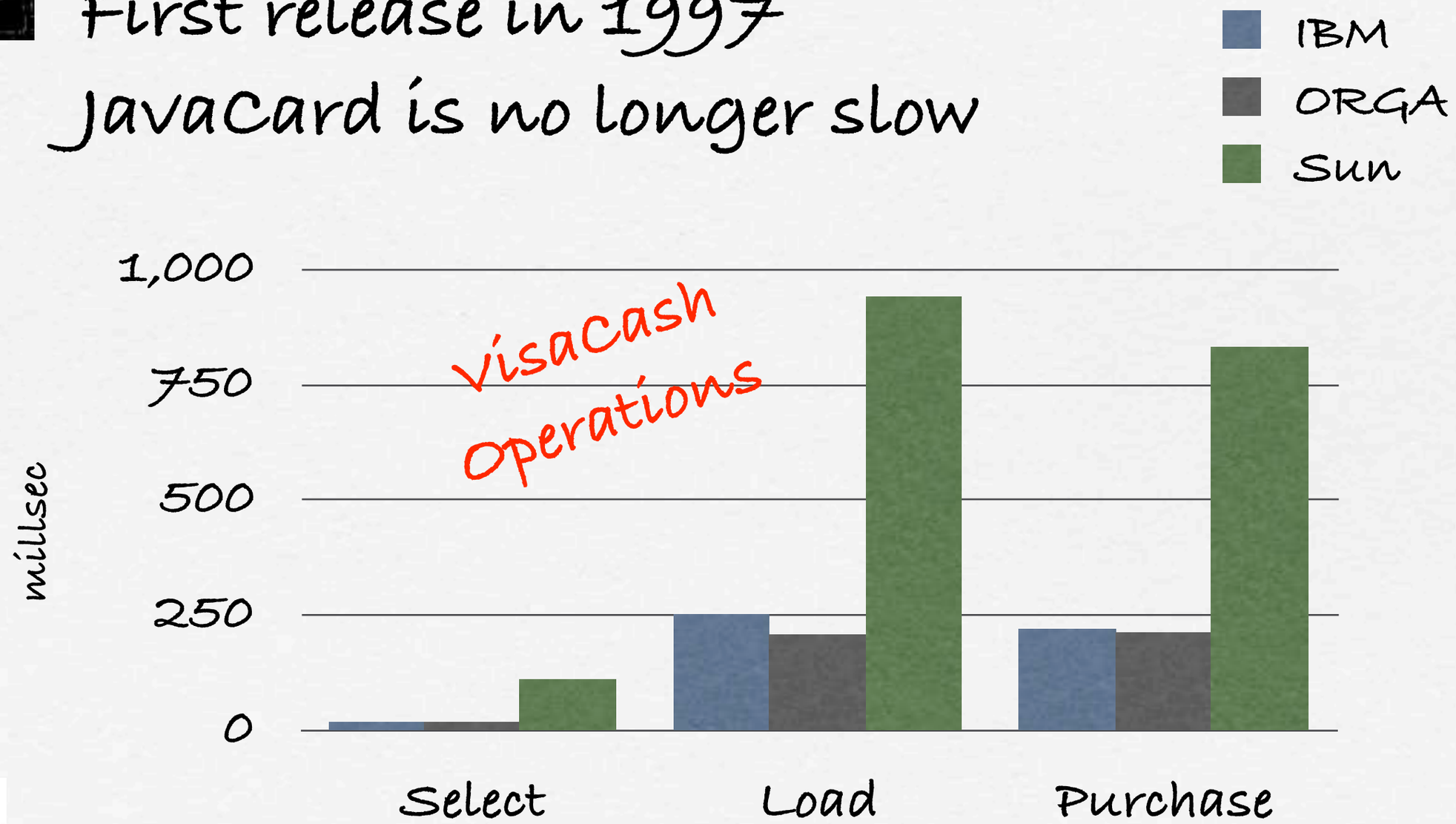
Writable | Insert | 157 : 25



IBM JCOP

JCOP History

- First release in 1997
  JavaCard is no longer slow



IBM

JCOP History

- First release in 1997
  JavaCard is no longer slow

IBM

JCOP Variants Today

- JCOP 10 (DES)
- JCOP 20 (RSA) [id]
- JCOP 30 (dual interface) [bio]
- JCOPsim (SWIM)

IBM

JCOP Memory Usage

	ROM available	EEPROM available
JCOP 10/16	16 KB	15 KB
JCOP 20/8	16 KB	7 KB
JCOP 20/16	24 KB	15 KB
JCOP 20/32	56 KB	31 KB
JCOP 30/16	20 KB	14 KB

JCOP Crypto Performance

	3DES CBC	1024 Bit Private	1024 Bit Public
JCOP 10	20 ms	n/a	n/a
JCOP 20	20 ms	290 ms	80 ms
JCOP 30	11 ms	230 ms	45 ms

JCOP RSA Key Generation

	512 Bit RSA CRT	1024 Bit RSA CRT
JCOP 20	2.2 secs	6.9 secs
JCOP 30	2.1 secs	6.1 secs

Demo

IBM®

Outlook

Next JavaCard

- Hardware
  - Moore's Law
  - More Interfaces (e.g., USB)
- Software
  - Remote Method Invocations (RMI)
  - Additional Crypto (e.g., ECC)

Questions?

javacard@zurich.ibm.com

IBM®