Implementing EMV™ and PKI in Brazil

Jorge F. Krug
(jorge_krug@banrisul.com.br)
Senior IT Security Executive
Banrisul S.A.
www.banrisul.com.br

Daniel F. Nunes de Oliveira
(daniel.oliveira@smartcon.com.br)
Business Development Director
Smartcon Consultancy Ltd.
www.smartcon.com.br
Presentation Overview

- About Banrisul and Smartcon
- Quick overview of Brazilian market
- Banrisul’s strategy towards EMV and PKI
- Implementation and card acceptance infrastructure
- Conclusions
About Banrisul and Smartcon
About Banrisul (banrisul.com.br)

Key facts:
- 2.9 Million clients
- Net Profit 2007: US$ 535.90 Million (+154%)
- Total Equity 2007: US$ 1.63 Billion (+30.9%)
- The most widely recognized financial institution brand name in its region (southern Brazil)
- Biggest Return Over Equity (ROE) amongst Brazilian financial institutions
- Recent Initial Public Offering (IPO)

Banricompras:
Banrisul’s own debit network
- 40,000 affiliated merchants
- 47 Million transactions per year

Distribution channels:

(2) “IstoÉ Dinheiro” Magazine (2007)

Current exchange rate in Feb/2008: 1 USD (US$) = 1.71 BRL (R$)
About Banrisul (banrisul.com.br)

Key facts:

- **2,9 Million** clients
- **Net Profit 2007:** US$ 535,90 Million (+154%)
- **Total Equity 2007:** US$ 1,63 Billion (+30,9%)
- The most widely recognized financial institution brand name in its region (southern Brazil)
- Biggest Return Over Equity (ROE) amongst Brazilian financial institutions
- Recent Initial Public Offering (IPO)

**Branches & ATM:**

- 419 Branches
- 278 Mini-branches
- 380 External ATM rooms
- 286 Million transactions per year (70 % unattended)

**Distribution channels:**


(2) “IstoÉ Dinheiro” Magazine (2007)

Current exchange rate in Feb/2008: 1USD (US$) = 1,71 BRL (R$)
About Banrisul (banrisul.com.br)

Key facts:

- **2,9 Million** clients
- **Net Profit 2007:** US$ 535,90 Million (+154%)
- **Total Equity 2007:** US$ 1,63 Billion (+30,9%)
- **The most widely recognized financial institution brand name in its region**¹ (southern Brazil)
- **Biggest Return Over Equity (ROE) among Brazilian financial institutions**²
- **Recent Initial Public Offering (IPO)**

Internet Banking (Home and Office Banking):

- **158 Million transactions per year**

Distribution channels:

(2) “IstoÉ Dinheiro” Magazine (2007)

Current exchange rate in Feb/2008: 1 USD (US$) = 1,71 BRL (R$)
About Smartcon (smartcon.com.br)

EMV and PKI specialists that provide a range of products and services, including:

- **MULTOS Applications:**
  - EMV for private-label applications
  - VSDC and qVSDC applications
  - PKI applications (including Biometric PKI)
  - Public Transport SAM (Secure Access Module)

- **PC middleware:**
  - EMV for terminals (EMV Kernel)
  - PC *Middleware* for PKI cards (CSP/PKCS#11)
  - EMV Authorization Libraries for hosts
Quick overview about Brazilian market
Brazilian card growth 2006-2007

Source: ABECS (Brazilian Credit and Services Companies Association) Report April 2008
## Payment methods (1997-2017*)

<table>
<thead>
<tr>
<th></th>
<th>1997</th>
<th>2007</th>
<th>2017*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>60%</td>
<td>60%</td>
<td>51%</td>
</tr>
<tr>
<td>Cards</td>
<td>6%</td>
<td>20%</td>
<td>38%</td>
</tr>
<tr>
<td>Checks</td>
<td>23%</td>
<td>8%</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
<td>12%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Source: ABECS (Brazilian Credit and Services Companies Association) Report April 2008

*2017: estimated
Banrisul’s strategy towards EMV and PKI
Fighting fraud requires coordinated actions, otherwise only fraud targets change (and not fraud numbers!)
Banrisul strategy towards EMV and PKI

Ammo used by Banrisul to fight fraud:

- Software agents: plug-ins at clients computer to inhibit Trojan horses and spyware
- Transaction Monitoring
- Cooperation with local and international police to identify and dismantle cyber-crime networks
- Hardware defences: Chip cards with EMV and PKI technology

Key part of Banrisul’s strategy!
The EMV world

Why EMV?

- *De facto* standard for chip-based debit and credit transactions → more than 6.3 million terminals\(^1\) and 441.6 million cards\(^2\)
- Technological platform of choice for hundreds of issuers around the world
- Clear and well-defined certification process (EMV TA) → unprecedented interoperability
- Advanced debit and credit features such as risk management and support for off-line transactions (including pre-authorized debit)

Sources:
1,2: EMVCo. Newsletter (December/2006)

*Question: Could EMV alone, address all Banrisul’s clients needs?*
Banrisul strategy towards EMV and PKI

Why can’t we do everything using EMV?
EMV is great for debit and credit transactions but does not offer some of the benefits of PKI, including:

- Legal validity in Brazil: “ICP-Brasil”: Important especially for high value Internet transactions

Card usage in typical non-banking PC scenarios (products) like:

- e-contract signing
- Secure e-mail
- Secure access to 3rd party services (e-gov included)
- Workstation Logon
- Workflow applications
PKI
The PKI world

ICP-Brasil

- PKI scheme defined and regulated by Brazilian government;
- Grants legal validity to documents (e-mails, e-contracts, etc) digitally signed under the programme rules;
- Strict mechanisms for physically validating the user’s identity before issuing a certificate.
- By using his or hers ICP-Brasil certificate, a user can contract new products without going to a branch.
- The majority of Brazilian Banks plan to or already use “ICP-Brasil” to secure their Internet Banking portals and other on-line channels.

**AC-RS** is a 2nd level ICP-Brasil compliant CA established by Rio Grande do Sul state with the aid of Banrisul
Banrisul strategy towards EMV and PKI

Why can’t we do everything with PKI alone?
PKI is highly flexible but lacks the interoperability and simplicity of the payment industry’s *de facto* debit and credit standard: EMV

Accepting PKI cards at EMV terminals is a difficult task.
- How to deploy the complex PKI middleware (CSP/PKCS#11)?
- How to handle alphanumeric passwords?

Millions of EMV terminals have been already deployed worldwide, ready to accept **EMV** cards!
- Almost *none* of these terminals can handle PKI cards

There is no PKI-based standard for debit & credit. For example, if you want to issue a chip-based MasterCard/Visa branded credit card today, there is just one option: EMV
Implementation and overview of card acceptance infrastructure
Capturing EMV and PKI transactions

- **Cashiers** (PC + PINPad)
- **Workstations** (PC + PC/SC smart card reader)
- **ATMs** (Linux PC + EMV L1 Reader + EMV L2 Software)
- **Internet Channels**
  - **Workstations** (PC + PC/SC smart card reader)
- **Commercial Network**
  - **PC-based WebTerminal** (PC + PIN Pad)
  - **Autonomous Terminal** (FPOS)
Capturing EMV and PKI transactions

- **Branches**
  - Cashiers (PC + PINPad)
  - Linux PC + EMV L1 Reader + EMV L2 Software
- **ATMs**
- **Workstations** (PC + PC/SC smart card reader)
- **Internet Channels**
  - Internet Banking
- **Commercial Network**
  - PC-based WebTerminal (PC + PIN Pad)
  - Autonomous Terminal (FPOS)

**EMV**

**PKI**

Capturing EMV and PKI transactions
## Terminal Network infrastructure

<table>
<thead>
<tr>
<th></th>
<th>PC/SC Readers</th>
<th>PIN Pads</th>
<th>FPOS</th>
<th>ATMs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target environment</strong></td>
<td>Home/Office</td>
<td>Branches &amp; point of sale</td>
<td>Point of sale</td>
<td>Branches / Outdoor</td>
</tr>
<tr>
<td><strong>Internal Software</strong></td>
<td>Simple (comm. protocol only)</td>
<td>Communication protocol and EMV Level II Kernel</td>
<td>EMV Level II Kernel, communication with an online host, Payment software</td>
<td>EMV Level II Kernel, communication with an online host, Payment software</td>
</tr>
<tr>
<td><strong>Comm. Interface</strong></td>
<td>Vast majority: USB</td>
<td>Serial, USB</td>
<td>Serial, USB, GPRS, Ethernet, Dial-up</td>
<td>Ethernet, Dial-up</td>
</tr>
<tr>
<td><strong>Attended</strong></td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td><strong>EMV</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>PKI</strong></td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>Banrisul/clients</td>
<td>Banrisul/clients</td>
<td>Clients</td>
<td>Banrisul</td>
</tr>
</tbody>
</table>
Deciding for EMV or PKI

(EMV or PKI) x (EMV and PKI)?

EMV and PKI are well-known and proven technologies, but EMV and PKI alone would not be sufficient to implement all required products and features.

Using EMV to solve PKI’s problems or PKI to solve EMV’s problems does not appear to be technologically viable. Two chips (or chip + token) is not a cost-effective alternative either.

EMV and PKI as different applications in the same chip delivers the best the two worlds can offer.
Deciding for EMV or PKI

Why choose ONE when you can have BOTH?

Benefits of one card capable of running both PKI and EMV

$ Smaller TCO (Total Cost of Ownership) of issuing, delivering and managing 1 instead of 2 separate cards (EMV+PKI) or issuing “card + token”

Historically, the card is the main link between financial institutions and customers – more products per card promote exposure beyond standard banking frontiers

PKI requires a RSA-enabled crypto-processor. Combining EMV and PKI allows issuing EMV on a more powerful chip, which enables high-security EMV features
“Banricompras”, Banrisul’s retail network, has the largest independent debit card user base in Brazil.

The cards are loaded with a customized EMV application for MULTOS, developed with the aid of Smartcon. The application is similar to M/Chip and VSDC, but independent.

Banrisul’s EMV cards can perform off-line enciphered PIN validation and Combined Dynamic Data Authentication (CDA) → the most secure debit cards in Brazil and the first debit product in Brazil to support full-grade EMV.

Banrisul can use off-the-shelf EMV PIN Pads to accept its EMV cards (cards and terminals “speak” EMV).
Implementing EMV

EMV at ATMs and Authorizer

ATMS:

- Banrisul ATMs upgraded with “EMV Level II Application Kernel” software in order to process EMV transactions
- In contingency, transactions can be validated off-line with CDA technology

Authorizer:

- Previous magnetic-stripe authorization system upgraded with EMV Authorization libraries that can validate cryptograms and generate Issuer responses
Implementing PKI

PKI Application

“ICP-Brasil” compliant PKI application for MULTOS, developed with the aid of Smartcon

All Internet Banking products (Home and Office Banking) are secured by PKI. All transactions are signed by the PKI application.

PKI application supports enciphered PIN verification from the virtual keyboard.

Lightweight infra-structure: browser plug-in talks directly to smart card reader without requiring additional software. CSP and PKCS#11 modules are only required for advanced PKI usage
Implementing PKI

PKI policies

Card-less Internet transactions are limited. Card-based transactions can be individually configured for much higher limits.

Cards are issued with proprietary free-of-charge certificates issued by Banrisul’s internal CA. Clients can buy (via AC-RS or other CA’s) “ICP-Brasil” compliant certificates to access extended services.

PC/SC Smart card readers can be bought on-line via Banrisul’s website (at very convenient prices).
Conclusions
Conclusions

1. Reduction of losses related to fraud:
   - Number of fraud cases that generated losses at channels protected by chip: **ZERO**
   - Number of cloned/counterfeit chip cards successfully used in transactions: **ZERO**
Conclusions

2. Reduction of operational costs:

- Attended transactions (performed at branches) are the most expensive ones

- Increased usage of Banrisul’s electronic channels, despite the numerous incidents reported by the media (at other banks! 😊) directly cuts operational costs
Conclusions

3. Using a security-oriented smart card OS allows Banrisul to:

- Focus on businesses and applications and not on security evaluation and processes
- Guarantee total application isolation - different teams and different paradigms co-exist on the same card
Conclusions

4. Intangible benefits:

- Customer feels secure when performing high-value transactions on the Internet, protected by chip

- Customer associates Banrisul with technology and security

- Increase brand visibility - Banrisul card used in more and more scenarios
Thank you.

Any questions?

Jorge F. Krug (jorge_krug@banrisul.com.br)
Banrisul S.A.
www.banrisul.com.br

Daniel F. Nunes de Oliveira (daniel.oliveira@smartcon.com.br)
Smartcon Consultancy Ltd.
www.smartcon.com.br