System z Crypto User Experience

CRP11

Vicente Ranieri Junior
Executive IT Specialist
System z Security RDS – South Regio
Presenter: Ernie Nachtigall

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

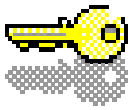
Agenda

- 5 cents about Cryptography
- Cryptographic Coprocessor Evolution
- Debit / Credit Card Authorization Process
- Banco Itaú Experience
- Summary

5 cents about Cryptography

Cryptographic System Components

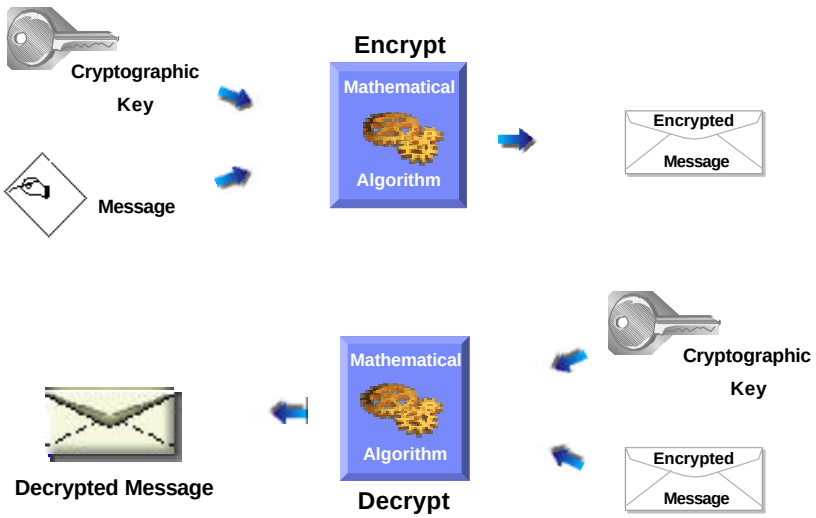
In mathematics, computing, linguistics, and related disciplines, an **algorithm** is a procedure (a finite set of well-defined instructions) for accomplishing some task which, given an initial state, will terminate in a defined end-state.



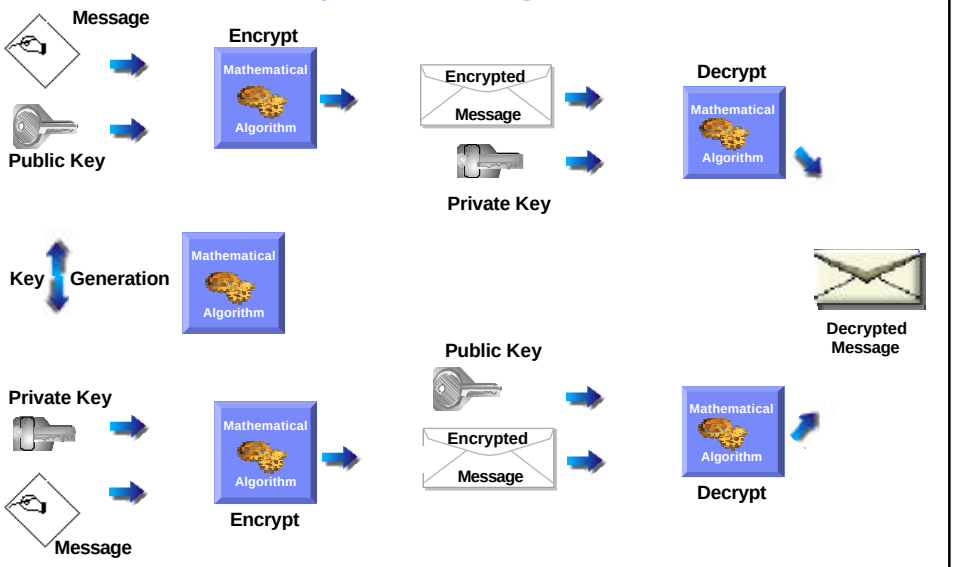
Cryptographic Key

The algorithms are publicly known. A **cryptographic key** is a piece of information that controls the operation of a cryptography algorithm. The keys are responsible for keeping the algorithm execution secret.

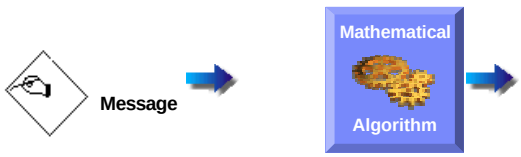
Symmetric Algorithms



Asymmetric Algorithms



Hash Algorithms
(One-Way Algorithms)



Bit String

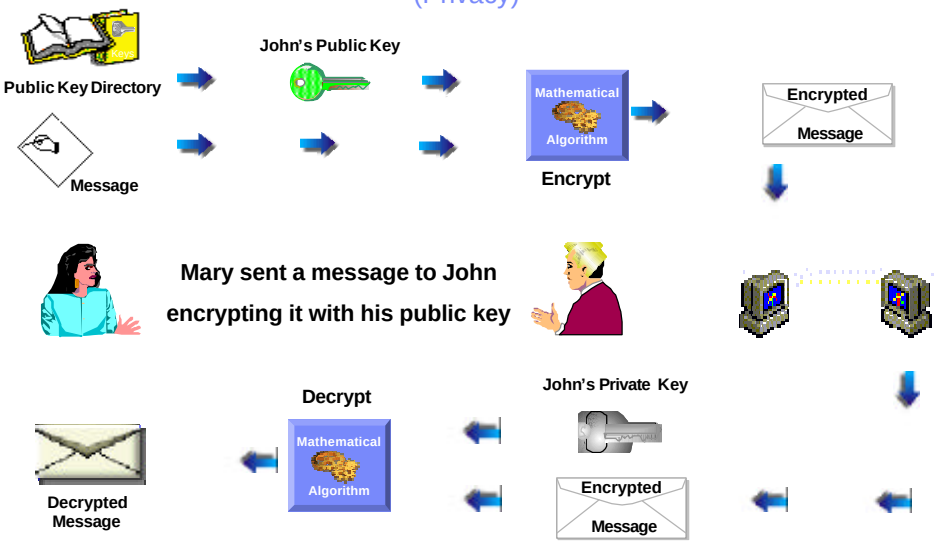
MD5 = 128 bits (16 bytes)
SHA-1 = 160 bits (20 bytes)
SHA-256 = 256 bits (32 bytes)

Pay US$ 100 to Vicente Ranieri = 5064c498576ec57e9e75fbb04ee8ccaa58c29c1a

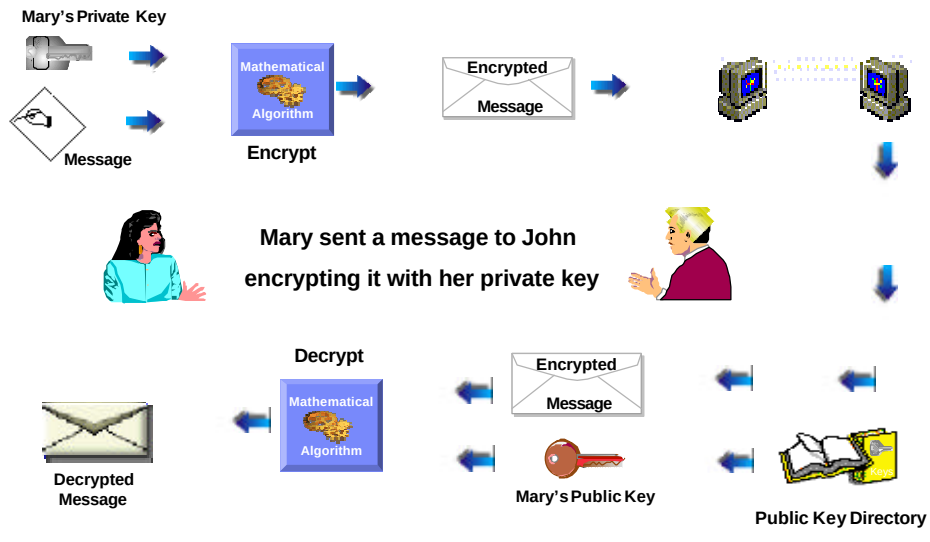
Pay US$ 100 to Vicente Ramieri = 83a8e63994fba9d9c927dd6fcf7c92ddc3185063

m = D4 (Hexadecimal) = 1101 0100 (Binary)
n = D5 (Hexadecimal) = 1101 0101 (Binary)

Exploiting Asymmetric Cryptography
(Privacy)

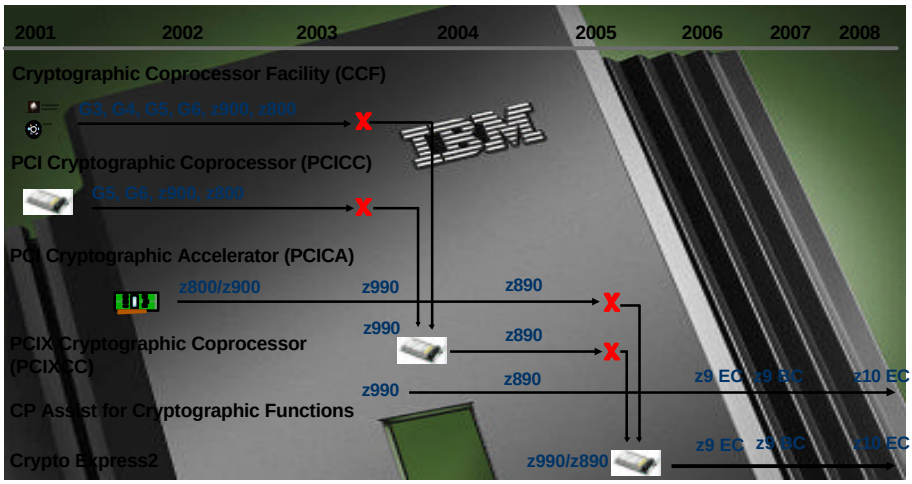


Exploiting Asymmetric Cryptography
(Digital Signature)

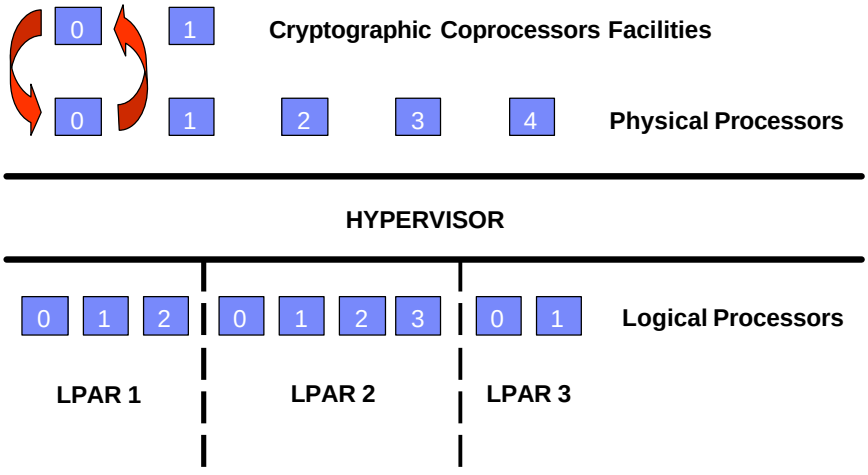


Cryptographic Coprocessor Evolution

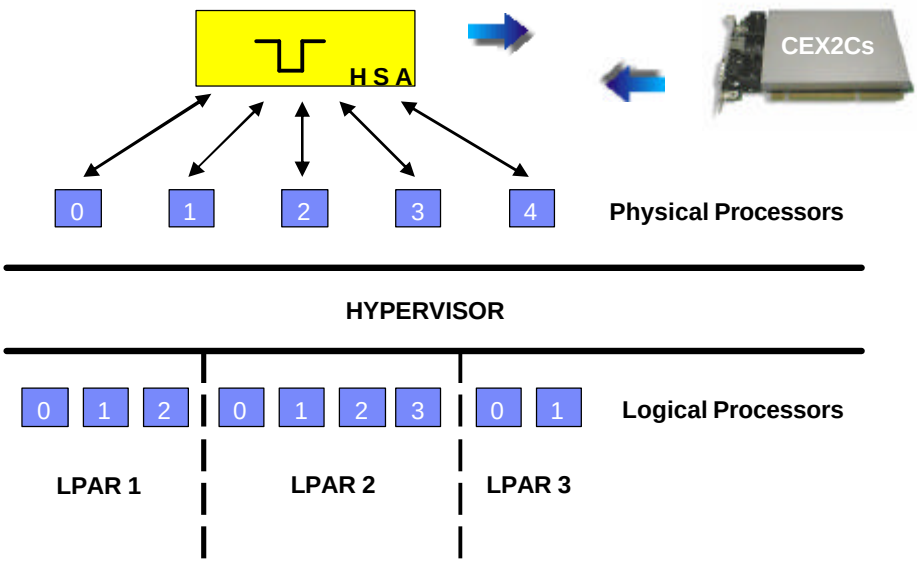
System z Crypto over time



z900 Secure Key Symmetric Processing



z990 Secure Key Symmetric Processing



Crypto Express2 Cards

- It is tamper-responding hardware validated at the highest level under the stringent FIPS PUB (Federal Information Processing Standards Publication) 140-2 Level 4.
- Specialized hardware that performs AES, DES, TDES, RSA, and SHA-1 cryptographic processes relieving the main processor from these tasks.
- Configurable as a coprocessor or as an accelerator.
- It is a very scalable solution, as System z supports up to 16 cryptographic coprocessors (8 Crypto Express2 features).

Debit / Credit Card Authorization Process

Payment Card Processing Roles

- **ISSUER**: Financial institution or its agent that issues the payment card to the cardholder. Responsible for responding to authorization requests.
- **CARDHOLDER**: Customer of the issuer using the payment card. Identified by a PAN (Personal Account Number).
- **ACQUIRER**: Financial institution or its agent that acquires the payment message related to a transaction and feed the data at interchange system.
- **CARD ASSOCIATION**: Owner of the payment card product. Responsible for the interchange system that exchanges transaction between acquirer and issuers.
- **MERCHANT**: Store or personal who is selling a good and will receive the payment.

Magnetic Stripe Card Withdraw Processing

Magnetic Stripe Card

stores financial information of cardholder

ATM

Read financial data of the cardholder

Add transaction detail (amount, currency)

Add business environment (Terminal ID, date, time)

Add digital envelop containing cardholder's PIN

Compute payment message

Issuer

Check whether the cardholder has enough funds in the account.

Verify cardholders PIN

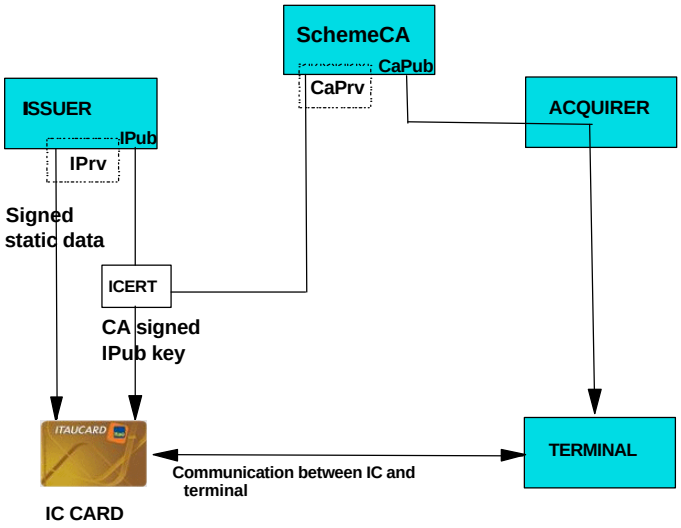
Approve or decline withdraw

Acquirer

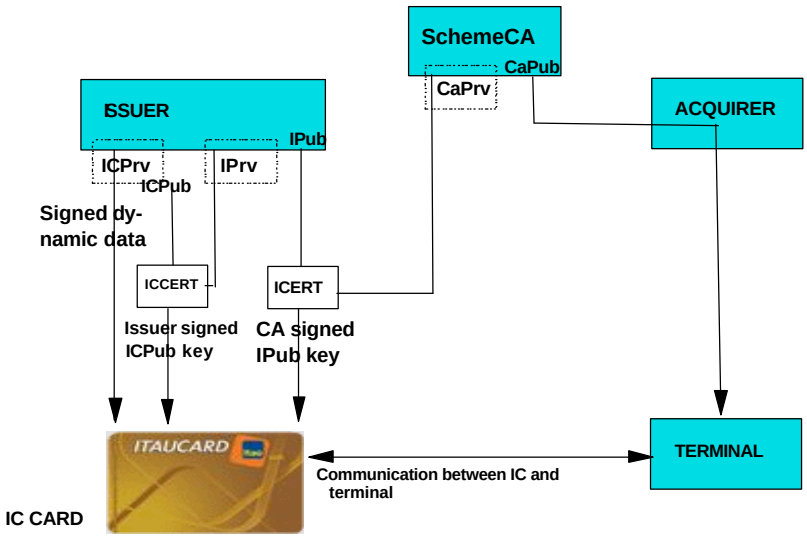
Create an authorization request from the payment message

Direct the authorization request to the issuer

Chip Card - Static Data Authentication



Chip Card - Dynamic Data Authentication



Banco Itaú Experience

Who is Banco Itaú ?

- Established in 1945 in São Paulo, Brazil.
- Privately owned bank with operations across North and South America, Europe and Asia.
- Currently the second largest private bank in Brazil.
- 15 million checking accounts and 9 million savings accounts.
- 3,000 branches
- 42,000 employees

Banco Itaú Problem

- Banco Itaú is migrating its debit and credit cards from magnetic strip technology to ICC (Integrated Circuit Card) also know as chip cards.
- Adoption of the new smart-card technology is successfully helping to protect customer accounts against frauds.
- Banco Itaú used to exploit external HSMs (Host Security Modules) to keep their cryptographic keys.
- As more and more customers switched over to the new cards, the bank realized that it would need a more scalable solution.
- The increasing load on its existing solution was beginning to cause problems with performance and reliability on its authentication systems.
- As the bank looked to replace all 15 million customer debit cards with the latest chip cards, it considered whether its existing authorization solution was up to the challenge.

Europay, MasterCard, Visa (EMV) Standard

- EMVCo LLC was formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV™ Integrated Circuit Card Specifications for Payment Systems.
- With the acquisition of Europay by MasterCard in 2002 and JCB joining the organisation in 2004, EMVCo is currently operated by JCB International, MasterCard Worldwide and Visa, Inc.
- EMVCo's primary role is to manage, maintain and enhance the EMV Integrated Circuit Card Specifications to ensure interoperability and acceptance of payment system integrated circuit cards on a worldwide basis.
- EMV 2000 is the current standard

Banco Itaú Proof of Concept

- Banco Itaú was already an ICSF user for some very specific symmetric encrypt/decrypt requirements (CCF exploiter).
- Moving from an HSM solution to IBM crypto coprocessor requires application changes.
- HSMs are called through some specific commands and IBM crypto coprocessors are called through ICSF callable services.
- IBM loaned a PCICC card to Banco Itaú z900 machine for functionality and performance tests. Required for CSNBDKG (Diversified Key Generate) callable service.
- Close support during the P-O-C was instrumental in the successful implementation of the new solution.

Additional Tests Required

- Banco Itaú was a z900 customer when the Proof-of-Concept took place.
- Just after testing the solution, Banco Itau migrated from z900 to z990s.
- Cryptographic Coprocessor architecture changed dramatically at z990. All the secure key functions performed at CCF were moved to PCIXCC and then to Crypto Express2 cards.
- IBM experienced some performance impacts during this movement in other customers.
- Proof-Of-Concept had to be rerun for checking as some functions exploits MAC with Triple-DES.

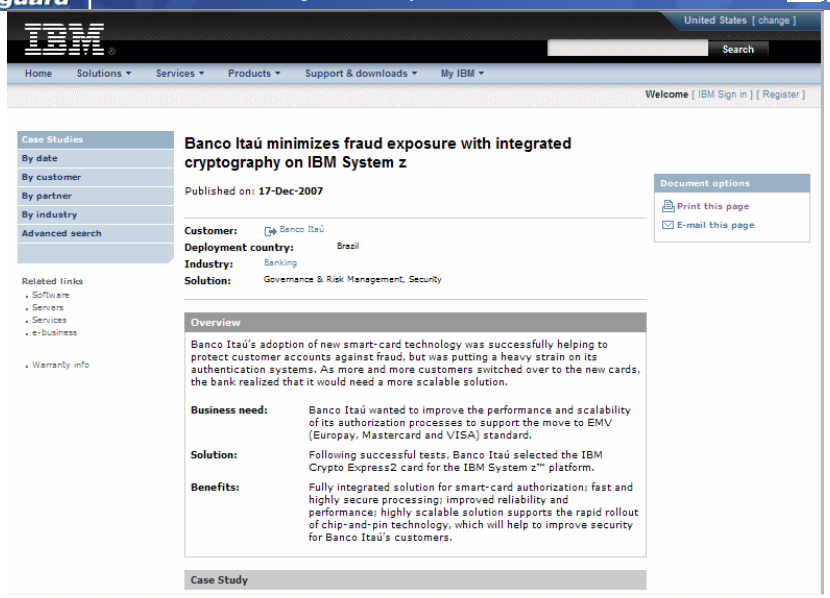
Simple, Safe and Scalable Solution

- The IBM Crypto Express2 solution for System z has met all of Banco Itaú's expectations in terms of performance, system simplification, reliability and availability.
- It also offers considerable scope for expansion and is expected to comfortably support all 15 million smart cards when the rollout is complete.
- By replacing a stand-alone proprietary solution, the Crypto Express2 card has reduced maintenance and operational costs for Banco Itaú
- The solution simplified its network architecture. Moving the authorization processes into the System z environment, Banco Itaú has eliminated a whole level of external network connections and increasing significantly reliability and security. The IBM solution has also eliminated a potential external point of failure, moving authentication onto the highly reliable mainframe platform.

Summary

Summary

- Banco Itaú concludes that it sees the IBM solution as a reliable, integrated security system that helps the bank reduce its risk and offer better protection against fraud to its customers.
- The new smart cards have helped to give its customers more confidence in the security of the bank's transactions, and the System z platform plays an important part in enabling Banco Itaú to offer this benefit to its customers.



IBM | United States [change] | Search

Home | Solutions | Services | Products | Support & downloads | My IBM

Welcome [IBM Sign in] [Register]

Case Studies
By date
By customer
By partner
By industry
Advanced search

Related links
- Software
- Servers
- Services
- e-business
- Warranty info

Banco Itaú minimizes fraud exposure with integrated cryptography on IBM System z

Published on: 17-Dec-2007

Customer: Banco Itaú
Deployment country: Brazil
Industry: Banking
Solution: Governance & Risk Management, Security

Document options
Print this page
E-mail this page

Overview

Banco Itaú's adoption of new smart-card technology was successfully helping to protect customer accounts against fraud, but was putting a heavy strain on its authentication systems. As more and more customers switched over to the new cards, the bank realized that it would need a more scalable solution.

Business need:	Banco Itaú wanted to improve the performance and scalability of its authorization processes to support the move to EMV (Europay, Mastercard and VISA) standard.
Solution:	Following successful tests, Banco Itaú selected the IBM Crypto Express2 card for the IBM System z™ platform.
Benefits:	Fully integrated solution for smart-card authorization; fast and highly secure processing; improved reliability and performance; highly scalable solution supports the rapid rollout of chip-and-pin technology, which will help to improve security for Banco Itaú's customers.

Case Study

http://www-01.ibm.com/software/success/cssdb.nsf/CS/STRD-79YEWB?OpenDocument&Site=

QUESTIONS