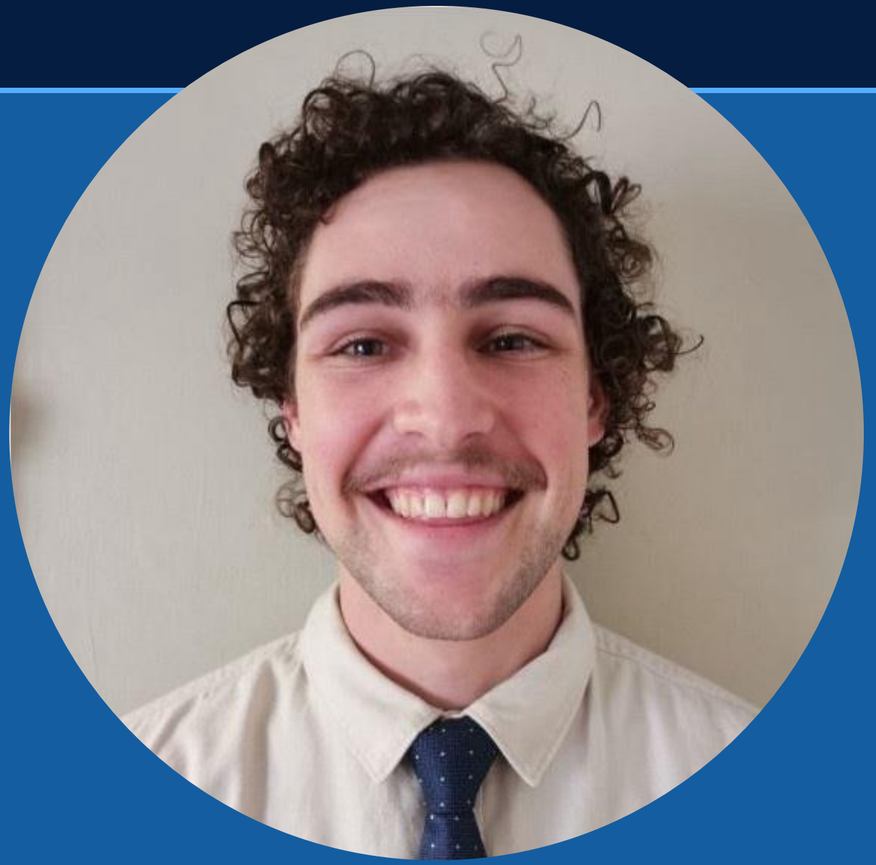
EMV Cards, Data Preparation and the Future of Secure Payments



Willem F. De La Bat

BARNES
SMART SOLUTIONS

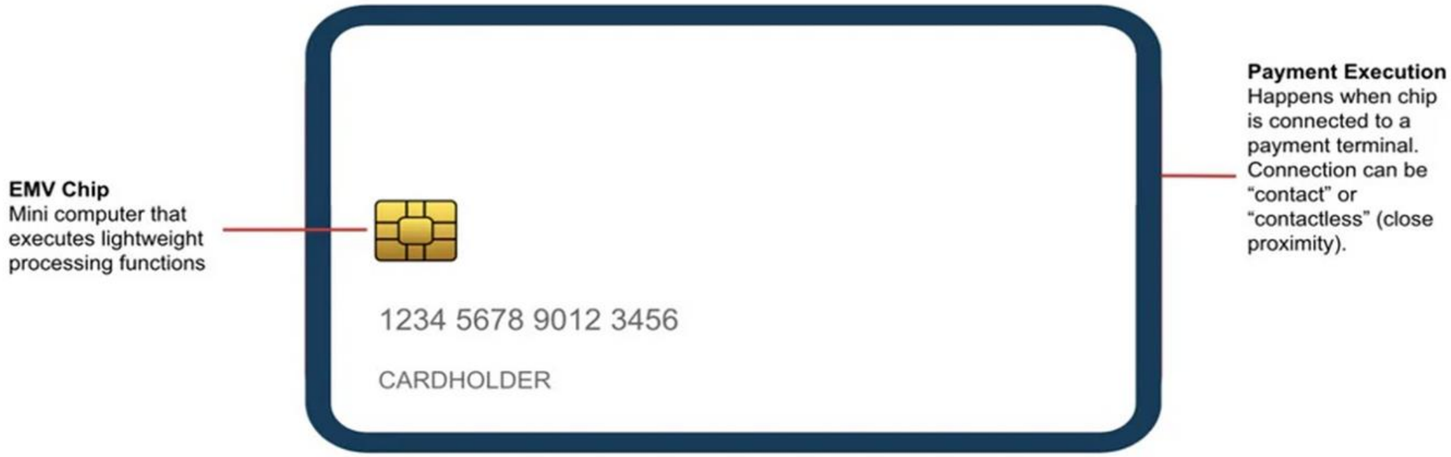
ON THE AGENDA..

- Current state of EMV payment cards and their production process.
- Deeper dive into data preparation for the payment industry.
- The future of secure payments.
- The rising influence of quantum computing.
- The evolution of cryptography standards.

BARNES
SMART SOLUTIONS

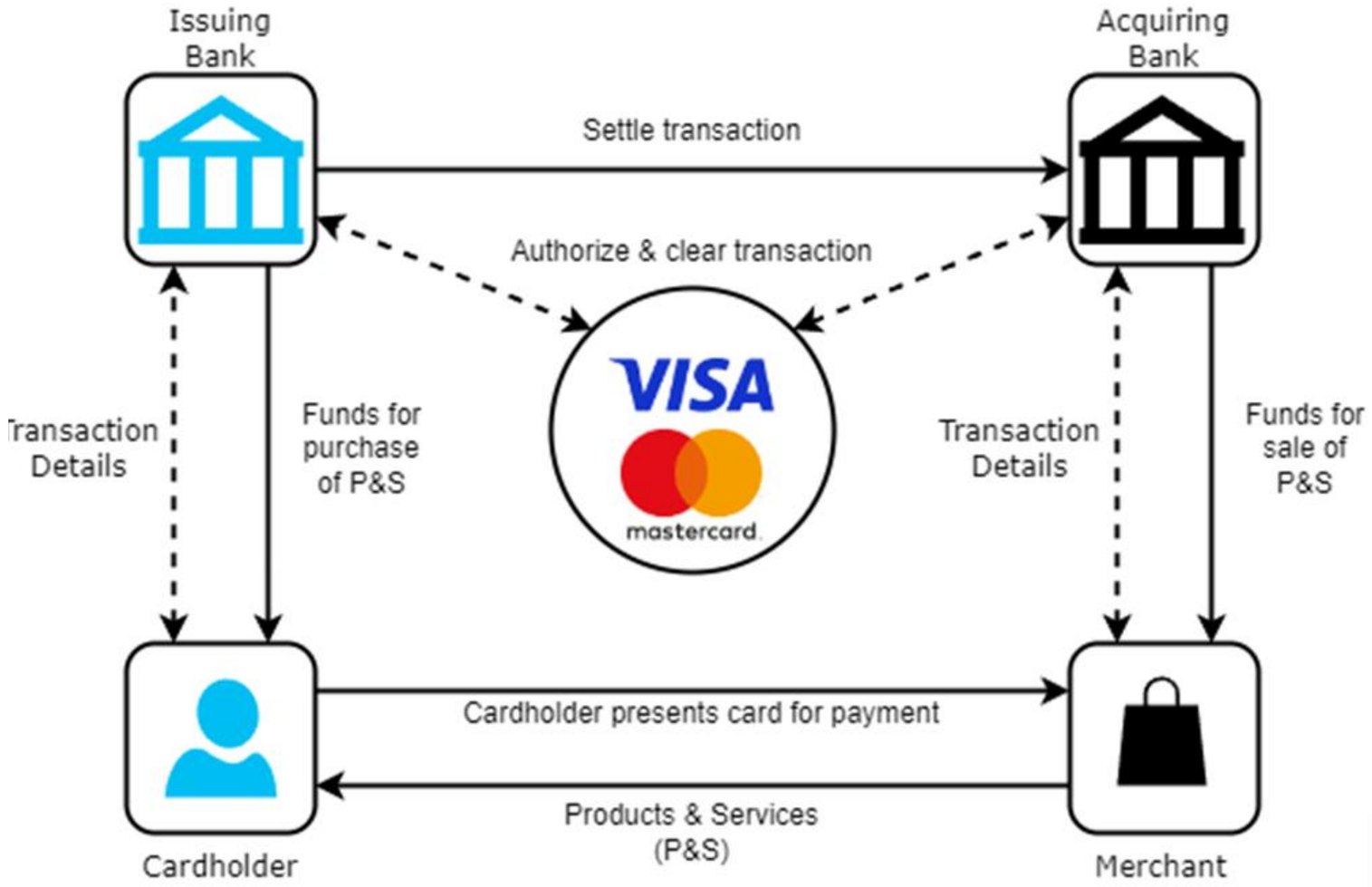
WHAT IS EMV?

- EMV stands for Europay, Mastercard, and Visa.
- EMV is the global standard for secure payment card transactions.
- Chip-based technology is used to secure transactions, replacing magnetic stripes.
- EMV cards generate dynamic cryptograms for each transaction, making it much harder for fraudsters to replicate card data.
- As of the end of 2023, 13.7 billion EMV cards in circulation. (EMVCo,2023)



BARNES
SMART SOLUTIONS

HOW DOES AN EMV TRANSACTION WORK?



BARNES SMART SOLUTIONS

EMV CARD PRODUCTION PROCESS

1. Physical Card Manufacturing

2. Data Preparation

3. Personalization and Issuance

4. Post-Issuance Management

BARNES
SMART SOLUTIONS

Symmetric vs. Asymmetric Encryption in EMV Cards

Symmetric Encryption:

- Single key for encryption and decryption
- Fast and efficient
- Used in EMV for:
  - Data preparation before card personalization (e.g., encrypting keys and application data)
  - Protecting transaction data integrity

Asymmetric Encryption:

- Uses a public and private key pair
- Ensures card and issuer identity verification
- Certificates are used to verify authenticity of the card and issuer
- Prevents the use of fraudulent cards

BARNES
SMART SOLUTIONS

DATA PREPARATION AND P3: THE PERSONALISATION PREPARATION

Data preparation for wide variety of card types and secure elements:

- Single-purpose and multi-application cards.
- Secure Elements (SE's) for smartphones.
- Remote SE's for cloud-based virtual card systems.

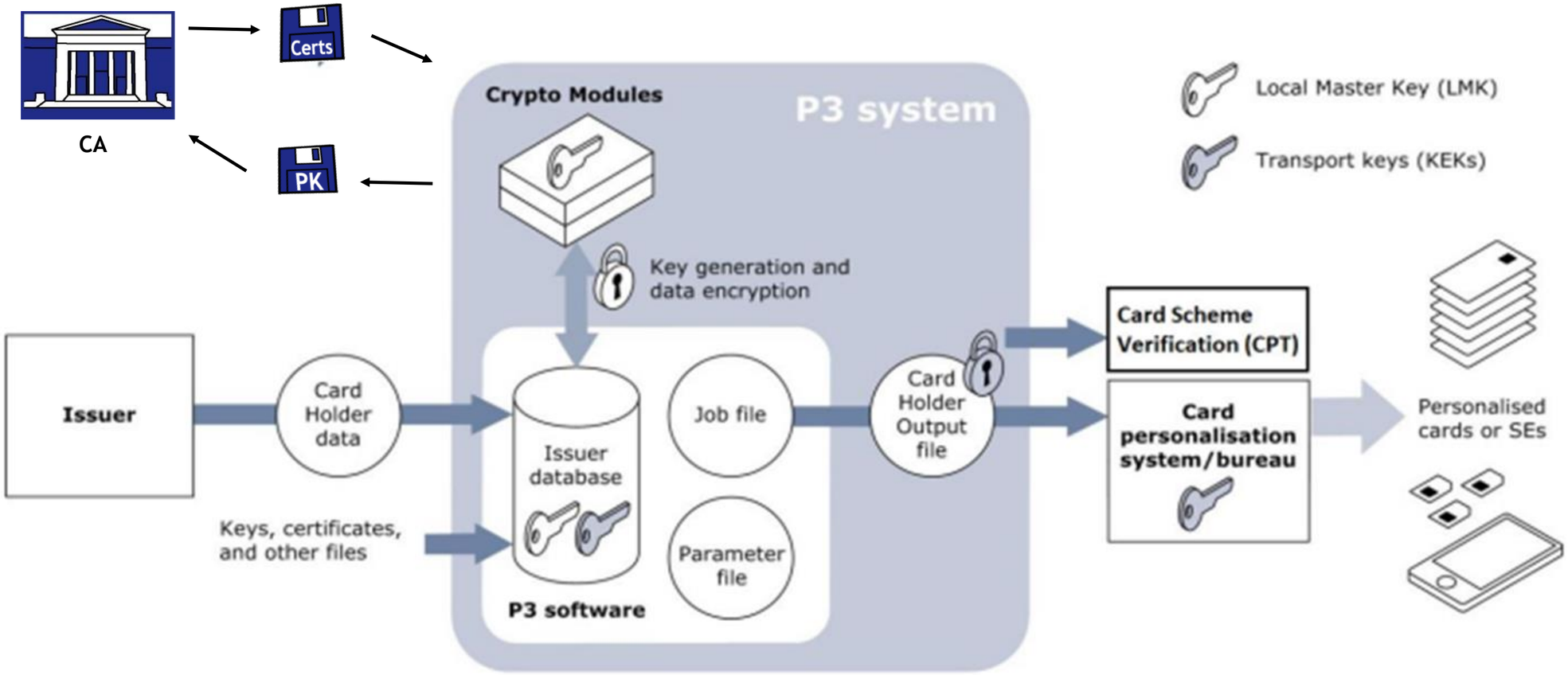
The P3 System: P3 software and Hardware Security Modules (HSMs):

P3® Advance

P3® Server

BARNES SMART SOLUTIONS

DATA PREPARATION AND P3: THE PERSONALISATION PREPARATION PROCESS



BARNES SMART SOLUTIONS

THE FUTURE OF PAYMENTS: DIGITAL, SECURE, AND DATA-DRIVEN

Significant Shift Toward Electronic Payments:

- Increasing consumer adoption of digital wallets, mobile payments, and virtual cards.
- Convenience and security of contactless payments and tokenization technologies are driving this shift.
- These technologies are built on the same EMV principles used in physical card transactions.

Projected Growth:

- By 2027, electronic transactions are expected to make up over 70% of all global transactions, reducing reliance on physical cards. [Global Payments Report by FIS(Worldpay), 2022].
- Contactless payments are expected to account for over 80% of all card payments by 2030.
- Mobile payments and virtual cards are projected to reach $12 trillion by 2028.

BARNES
SMART SOLUTIONS

WHY DATA PREPARATION REMAINS ESSENTIAL IN A DIGITAL PAYMENTS WORLD

1. **Virtual and Tokenized Payments**
   - Tokenization replaces sensitive card data with unique tokens per transaction.
   - Relies on cryptographic keys and secure data preparation—exactly what P3 provides.
   - Keys are generated and encrypted similarly to traditional EMV cards, regardless of device used (smartphone, wearable).

2. **Mobile Payments and Secure Elements (SEs)**
   - Secure Elements (embedded or cloud-based) act as virtual cards with personalized, encrypted data.
   - P3 securely prepares and transmits data to SEs.
   - Ensures mobile payments are as secure as traditional card transactions.

Pay | G Pay | SAMSUNG pay

BARNES SMART SOLUTIONS

WHY DATA PREPARATION REMAINS ESSENTIAL IN A DIGITAL PAYMENTS WORLD

3. Cloud-Based Virtual Cards

- Virtual cards depend on secure cloud infrastructures.
- Cryptographic keys and data must be securely prepared before cloud storage.
- P3 ensures virtual cards are as secure as physical cards through seamless data preparation.

4. Continued Security and Compliance

- Compliance with standards like EMVCo, PCI DSS, and ISO/IEC remains essential.
- P3 encrypts all sensitive data and maintains compliance in both physical and virtual transactions.
- Protects both issuers and consumers in the evolving payment landscape.

EMVCo®

PCI DSS COMPLIANT

BARNES SMART SOLUTIONS

WHY DATA PREPARATION REMAINS ESSENTIAL IN A DIGITAL PAYMENTS WORLD

- Innovation in the payment market is happening in the acquirer side of things.
- The fundamental structure of the card scheme (Cardholder, Merchant, Issuing Bank, Acquiring Bank) remains unchanged.
- Payment methods like magnetic strip, chip, etc. are managed in the same way as new innovations on the market.

BARNES
SMART SOLUTIONS

CHALLENGES IN THE FUTURE OF SECURE PAYMENTS: CRYPTOGRAPHY & QUANTUM COMPUTING

Quantum Computing & Cryptographic Threats

- Quantum computing, while still developing, poses a serious risk to current cryptographic methods.
- Algorithms like RSA and ECC can be broken by quantum computers, potentially in hours, using Shor's Algorithm.
- By 2030, quantum computers are expected to be capable of challenging today's encryption.

Immediate Action Required

- Though quantum computing is not mainstream yet, preparing for its impact on cryptography is crucial now.

Google Quantum AI

IBM Quantum

D-Wave The Quantum Computing Company™

BARNES SMART SOLUTIONS

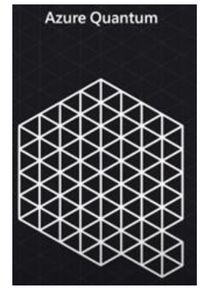
CHALLENGES IN THE FUTURE OF SECURE PAYMENTS: CRYPTOGRAPHY & QUANTUM COMPUTING

Asymmetric Encryption (RSA, ECC):

- Vulnerable to quantum algorithms like Shor's Algorithm.
- RSA and ECC used for key exchanges and digital signatures in payments can be broken by quantum computers.
- Quantum computers can intercept communication and break cryptographic systems, exposing sensitive payment data.

Example Threats:

- Compromise of public-key encryption used in card issuance and mobile payments.
- Risk to digital wallets and tokenization if asymmetric encryption is broken.



BARNES
SMART SOLUTIONS

WHERE WE ARE SAFE FROM QUANTUM COMPUTING (FOR NOW…)

Symmetric Encryption (AES):

- AES-256 remains strong even with quantum attacks (due to Grover's Algorithm, which halves security).
- Widely used in EMV cards and HSMs, providing strong protection for card data and cryptographic keys.

EMV Cards:

- EMV cards use dynamic data authentication (DDA), ensuring each transaction generates unique cryptograms.
- Symmetric encryption in EMV cards and HSM-based key management remains safe from quantum threats. (for now…)

Google Quantum AI

IBM Quantum

D:Wave The Quantum Computing Company™

BARNES SMART SOLUTIONS

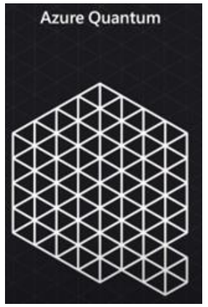
POST-QUANTUM CRYPTOGRAPHY

Quantum-Resistant Algorithms:

- Cryptography experts are developing quantum-resistant methods such as:
- Lattice-based cryptography
- Hash-based cryptography
- Multivariate-quadratic-equations
- These algorithms are designed to withstand quantum computing attacks.

Transitioning to Quantum-Resistant Standards:

- Fintech companies must begin experimenting with and adopting these algorithms.
- Transitioning infrastructure gradually is essential to secure future payments.



BARNES
SMART SOLUTIONS

ADVANCEMENTS IN CURRENT CRYPTOGRAPHY

What is Key Block Encryption

- Encrypted packaging of cryptographic keys with usage metadata.

Why is it used?

- Enhances security by preventing key misuse.
- Controls key usage through embedded metadata.
- Aligns with industry standards (e.g., ANSI TR-31).

P3’s Advantage

- One of the first data preparation solutions to support Key Block Encryption.
- Provides secure key management within data preparation.
- Ensures compliance and future-ready security practices.

BARNES
SMART SOLUTIONS

PREPARING FINTECH'S FOR THE FUTURE OF PAYMENTS

Stay Ahead of Cryptographic Standards:

- Adopt quantum-resistant encryption early.
- Implement Key Block formats and track emerging cryptographic trends.
- Engage with standard bodies like EMVCo, PCI DSS, and NIST to stay compliant.
- Use solutions like P3 that is always implementing the latest cryptographic standards.

Invest in Cryptography Expertise:

- Cryptography talent is scarce in the fintech industry.
- Companies must hire and train experts in cryptography and encryption.
- Encourage ongoing education, certifications, and participations in industry conferences.

Engage with the Cryptographic Community:

- Fintechs should actively participate in industry working groups, academic collaborations, and open-source projects.
- This ensures a proactive approach to future cryptographic challenge and helps shape the future of secure payments.

BARNES
SMART SOLUTIONS

THANK YOU!

BARNES
SMART SOLUTIONS