



P3 Data preparation

Gilliaume Oosthuizen





P3 Overview

- P3 is a turnkey solution of dedicated FIPS 140-2 Level 3 approved tamper resistant cryptographic hardware and Windows server software.
- Developed in conjunction with the card associations since 1996 to help with migration from Magstripe to EMV
- Often referred to as the industry de-facto standard for EMV data prep
- 250 installation worldwide (and growing) all capable of issuing Multos cards
- Track record of keeping P3 ahead of the curve with Multos support





P3 Product family – keep data preparation in-house

Thales P3™ Advance

- Traditional batch issuance
- Medium volume system
- Mid sized issuers and small bureaus
- Latest release V1.7

Thales P3™ Server

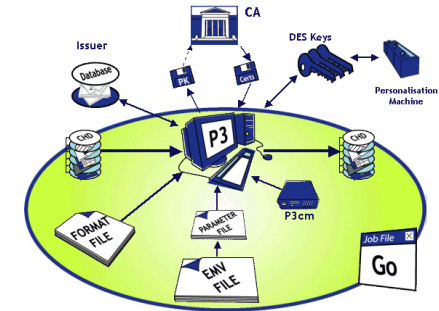
- High performance online or batch system
- Large volume in-house issuers and bureaus
- Scalable system can grow as required
- Supports instant and post issuance
- Latest release V1.7

Thales P3™ P3CM

- A HSM optimized for data preparation
- FIPS 140-2 L3 certified
- Comprehensive secure ALU creation
- Latest model P3CM-250

Thales P3™ Professional Services

- P3 configuration and optimisation
- EMV project management
- EMV card parameter configuration
- Multos and Card Application consultancy
- Application integration



Support a range of smart card platforms including:

- MULTOS
- GlobalPlatform
- TIBC
- Proprietary single and multi-application cards

as well as commonly used card applications including:

- MasterCard
 - M/Chip Lite, M/Chip 2 Select, M/Chip 4 (MULTOS), M/Chip Flex, PayPass, MICA and CAP
- Visa
 - VSDC (SDA or DDA), PayWave, Visa CEPS, VisaCash (DES/RSA) and DPA
- JCB
 - JCB Lite, J/Smart, J/Speedy



- Supports full Multos and Multos Step/one cards
 - Support for confidential and protected ALU
 - Support for major card schemes and associated applications e.g. VSDC, M/Chip & J/Smart
 - Existing installations of P3 all capable of issuing Multos cards

- Extensions to Global Platform Scripting language
 - Supports Multos ALU generation - enable ID card generation

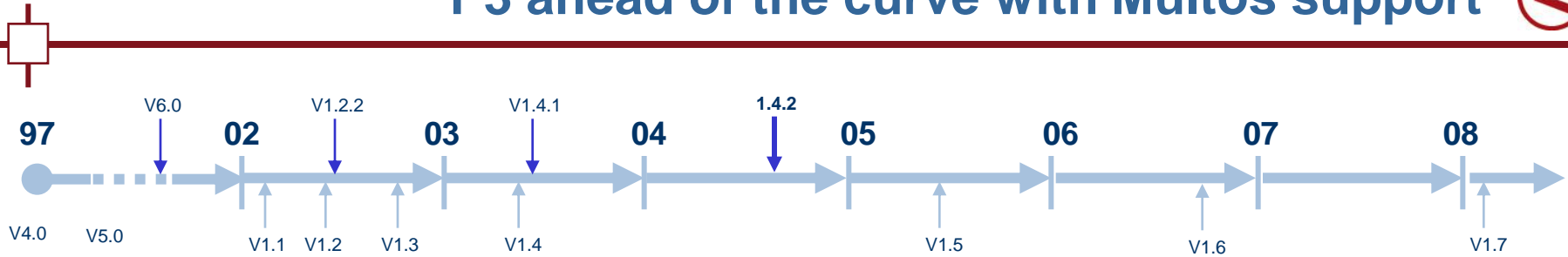
- Multos ALU output
 - Flexible packaging – for ease of use by personalisation system

- Post issuance and instant issuance
 - Support generation of KTU under shared KEK or under card public key (Instant issuance)

- Comprehensive ALU creation inside FIPS approved security module
 - Help with audit requirement
 - Maximum reuse of HSM 8000 (Issuance Firmware)



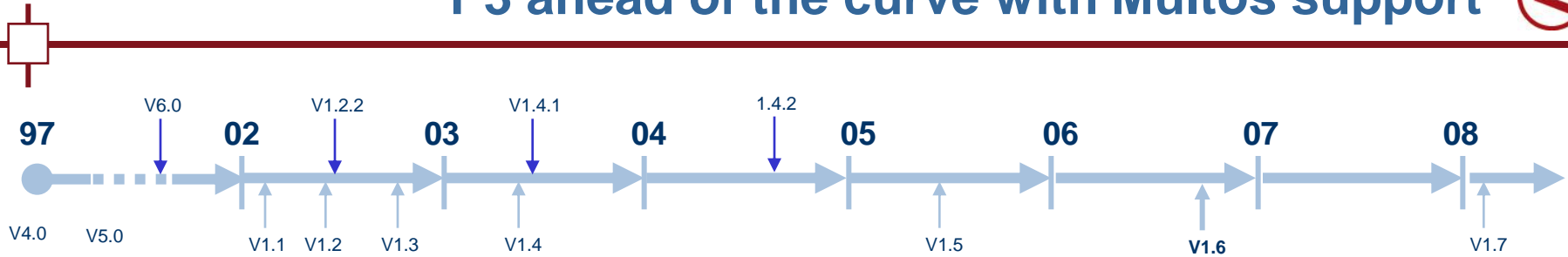
P3 ahead of the curve with Multos support



1997 -2002	P3 V4.0 - V5.0	Support for J/Smart 1 and VSDC on proprietary cards. MChip/2 (Lite & Select) on Multos.
April 2002	P3 V1.1	First release of P3 Server utilising multiple P3CMs for scalable performance. SCMS integration with P3 via Microsoft Message Queue Server (MSMQ).
July 2002	P3 V1.2	Updates in line with new Multos File Information Formats (FIF).
July 2002	P3 V1.2.2	Custom P3 build to support Hong Kong ID programme using P3 CCSB scripting support.
Nov 2002	P3 V1.3.0-1	Updates to P3's GP scripting implementation to support EMV 4.0.
July 2003	P3 V1.4	Support for MChip/4 on Multos, J/Smart 2 and updates to the GP script Multos extensions.
July 2003	P3 V1.4.1	Support for VSDC on Multos & Carte Bancaire's Multos delegator application.
Nov 2004	P3 V1.4.2	Ticketing project in conjunction with MasterCard PayPass on Multos. MasterCard Asia Pacific OneSMART Platinum Award.

Proactive developed with Card associations and Multos Vendor Community

P3 ahead of the curve with Multos support



June 2005	P3 V1.5	TCP/IP support for job submission. Support for the generation of Multos Application Load Units for Multos Step One smart cards. Support for VSDC on MULTOS Personalisation Data Map (3.1).
Oct 2006	P3 V1.6	Data preparation for VSDC on MULTOS using the iSmart Customisation Utility. Data preparation for the M/Chip Integrated Card Application (MICA) using the MasterCard Applications Customisation Utility (MACU). Data preparation for domestic and co-branded SPAN profiles. PayPass on GP cards.
Feb 2008	P3 V1.7	Contactless data preparation support for the VSDC(2.6) applet including support for MSD and qVSDC in P3 TLV format and EMV Card Personalisation Specification format (CPS). Contactless data preparation support for the J/Smart 3 application in P3 TLV format and CPS format. Data preparation support for the contactless MasterCard PayPass M/Chip Flex application. Support for EMV 4.1.

Proactive developed with Card associations and Multos Vendor Community



- Thales fully committed to onward development of Multos technology
 - Continue software development

 - Expand the crypto hardware
 - Performance
 - Functionality
 - Security

- Where we can go from here
 - Promote the simplicity and low cost of instant issuance using Multos technology

 - Explain benefits of multi-application Multos card
 - Value added third party applications e.g. loyalty
 - Post issuance add/remove/update applications
 - Easy start with Multos Step/one then migrate to Full Multos

 - Drive a high level security protocol to simplify audit compliance for issuers
 - Data transfer between disparate systems – e.g. host, data prep and perso



Thank You

Gilliaume Oosthuizen

Product Manager

e-mail: gill.oosthuizen@thales-esecurity.com

mobile: +44 (0)7854903573