



# MasterCard and Cryptographic Research

Paper submitted by Michael Ward for the  
STORK Cryptography Workshop 26/27 November 2002

## 1 Introduction

This paper provides an overview of MasterCard International, its payment products and its technology, and proposes directions for cryptographic research important to MasterCard.

## 2 Overview of MasterCard

MasterCard International is a global payments company, managing a range of payment programs and services, including MasterCard<sup>®</sup> credit and debit cards, Maestro<sup>®</sup> online debit cards, Cirrus<sup>®</sup> ATM cash access, and related programs.

MasterCard operates one of the world's largest global telecommunications networks, processing as many as 32 million authorisations of financial transactions a day.

### 2.1 Security and New Technology

MasterCard has been an industry leader in the innovation and development of fraud-preventing security techniques such as the first tamper-evident signature panel, the use of three-dimensional holograms and card validation codes.

The new *OneSMART* MasterCard smart card delivery program offers a broad menu of smart card applications, including: chip-based credit and debit, personal data storage, digital ID and security, loyalty, e-ticketing, e-coupons and stored value. There are currently more than 116 million MasterCard, Maestro, Mondex, and Clip<sup>™</sup>-branded smart cards around the world. Currently, 70% of these cards have multi-function or multi-application capability. MasterCard also actively supports all major smart card environments (MULTOS, JavaCard, and proprietary platforms).

MasterCard is a leader in the field of proximity payments, m-commerce and e-commerce. In September 2002, MasterCard unveiled a global e-commerce security solution for protecting confidential cardholder data over the Internet. The new service is known as MasterCard<sup>®</sup> SecureCode<sup>™</sup>.

## 3 MasterCard and Cryptography

MasterCard depends on symmetric and asymmetric cryptography in many of its products and systems. Examples include the use of hardware security modules for authorisation (PIN transport, chip authorisation and on-behalf services), and key management systems for the key

management of security modules, for software downloading, and for PKI to support chip and e-and m-commerce.

### **3.1 Cryptographic Research**

MasterCard deploys security solutions based on international standards. Although there are many standards making bodies (e.g. ISO, IEEE, RSA PKCS, IETF), and thankfully much commonality between the standardisation of cryptographic algorithms, there is still a need to encourage cryptographic research that improves the maturity and stability of techniques in readiness for standardisation.

As can be seen by the evolution of RSA encryption schemes that are provably secure in the Random Oracle Model, achieving some accepted notion of security proof prior to standardisation is important. For this reason MasterCard encourages the continuing research into pragmatic security proofs along the lines of the work of Bellare and Rogaway. Research should include the Random Oracle Model but also explore new, alternative paradigms. The set of cryptographic mechanisms that should be addressed especially includes non-primitive mechanisms and techniques such as:

- authenticated encryption,
- symmetric key exchange using asymmetric encryption,
- incremental cryptography,
- random number generation and key derivation.

MasterCard also encourages the development of standards and guidance for the secure implementation of cryptographic algorithms and mechanisms. This includes security and performance issues relating to different platforms or 'form factors'.

MasterCard recognises that new technology such as proximity cards and biometrics may soon be pervasive, and if so then any associated cryptography will need to be fit-for-purpose and trusted. Thus research into new algorithms with special characteristics (e.g. low bandwidth, low power consumption, biometric-specific) will continue to be important.

MasterCard also sees a need for new ways of using existing algorithms. For instance, given a device with (enhanced) capability to execute a certain algorithm (e.g. a smart card with a DPA-resistant co-processor for DES or modular exponentiation), one may want to implement other cryptographic functions (e.g. a fast and strong DPA-resistant hash) using that algorithm. A specific example might be a function for computing a 20-byte hash using DES but with  $2^{112}$  collision resistance (see ISO 10118-2 for similar but weaker functions). Also needed are comprehensive key management techniques for managing secret keys of 'unusual' length (e.g. 20 byte HMAC keys managed using a 64-bit block cipher).

In conclusion, MasterCard and its product suppliers depend on the results of cryptographic research in order to enable secure payments using new technology in new environments. MasterCard welcomes the opportunity to influence research in this field.