



HOME BIOGRAPHY TOPICS RESOURCES NEWS CONTACT

REMOTE CHIP AUTHENTICATION (RCA)

OVERVIEW

Remote Chip Authentication (RCA), in the form of MasterCard's Chip Authentication Program (CAP) or Visa's equivalent Dynamic Passcode Authentication (DPA), is taking off rapidly throughout Europe as a strong two-factor solution for secure remote banking. At the same time, the 3D Secure protocol is taking off as a single-factor solution for secure remote card payments, in the form of MasterCard's SecureCode or Verified by Visa. The time is now right to combine these two approaches into a universal, strong, two-factor RCA solution for all remote banking and payments leveraging the security of EMV chip.

Remote Chip Authentication

- Enables highly secure chip-based authentication of cardholders
- Leverages and extends the EMV infrastructure into the virtual world
- Uses chip card and PIN to generate one-time password
- Already a proven method of securing online banking
- For online shopping, one-time password treated as 3D Secure token (SecureCode or VbV)
- Result: strong, cost-effective, two-factor authentication using standard PIN, applicable across all remote channels (internet or telephone)



HOW RCA WORKS

Cardholders insert their EMV chip card in a simple, low-cost, handheld reader, enter their PIN, and a one-time-password (OTP) is displayed after the card has verified the PIN. The OTP can then be used to authenticate remote banking transactions via the internet or telephone. For secure remote payments, the OTP is treated as a dynamic MasterCard SecureCode or Verified by Visa passcode and processed over the 3D Secure infrastructure.

WHY RCA IS A GOOD SECURITY SOLUTION

RCA delivers strong two-factor authentication based on "something you own" (the EMV chip card) and "something you know" (the PIN). Since the OTP is dynamic, it cannot be re-used for fraudulent transactions. This means RCA is a good defence against phishing attacks. Since all processing takes place in the EMV card while inserted in a handheld reader, which is physically separate from the PC, RCA is also not vulnerable to "spyware" and viruses. CAP can also easily be made even more secure for highly sensitive transactions by using Challenge-Response (CR), or Transaction Data Signing (TDS).

HISTORY AND TERMINOLOGY

CAP was developed about 5 years ago by MasterCard as an added value application which leverages the EMV chip infrastructure. MasterCard licensed the specification to other players in the card payments industry including Visa. APACS has also adopted and extended the CAP specification and refers to it as Remote Cardholder Authentication (RCA). In the UK, it is being promoted as "Chip & PIN at home".

DEPLOYMENT

RCA is now widely deployed in Europe for secure e-banking, by banks such as Barclays, RBS, ABN AMRO, Rabobank, KBC, Dexia, Fortis, Nordea, with many more in the process of rollout. The latest announcement was by Nationwide in the UK. MasterCard polled estimates from the industry showing that last year between 10 and 15 million CAP readers were deployed in the field.

WHY BANKS CHOOSE RCA

Compared with other options, RCA is:

- Highly secure, not just in today's world, but also in terms of future threats. For example, by using TDS, where the cardholder enters the payment amount and account number of a beneficiary in addition to the PIN to generate the OTP, RCA can be used to protect against possible future "man-in-the-middle" attacks where fraudsters alter the data in a funds transfer transaction.
- Cost-effective, because it leverages the investment already made in EMV chip migration. The handheld readers are inexpensive and can be shared across applications.
- Comprehensive and convenient, since a single chip & PIN approach, already familiar to cardholders from ATM and physical POS experience, is applied to all remote banking and payment channels.

EXTENDING RCA TO SECURE REMOTE PAYMENTS

Although several banks are planning to use RCA for secure e-commerce, it has not yet been widely deployed for this purpose - all banks to date have started deployment of RCA with e-banking. The reason is that, unlike RCA for e-banking, RCA for e-commerce requires banks to work together on a coordinated basis with other banks and with merchants to agree and put in place a standard data transport infrastructure. The card payments industry has already developed such a standard, known as 3D Secure, and implemented by MasterCard as SecureCode and by Visa as Verified by Visa (VbV). When shopping online with a payment card, the cardholder is prompted by the card issuer to enter a static password - the SecureCode or VbV passcode - which authenticates their identity. With RCA, the dynamic OTP is used instead of the static password, and is processed as a standard 3D Secure token using exactly the same infrastructure as before. This is more secure since it involves two-factor rather than single factor authentication, and since the 3D Secure token is dynamic and cannot be re-used fraudulently. The dynamic nature of the token also means that it can be safely used, not just for e-commerce, but also over the telephone for telephone order payments.

RCA DEPLOYMENT

2009 may be the year when RCA for secure remote card payments takes off as a widespread commercial solution. 3D Secure penetration is increasing steadily throughout most of Europe and is approaching critical mass in some markets such as the UK. RCA deployment can be expected to accelerate this trend - with RCA, cardholders do not need to register with their bank and do not need to remember a new password. Several large banks which have already distributed RCA readers for e-banking plan to extend their use to e-commerce soon - for example Nordea RCA readers already feature a "buy" button in anticipation of this development. Perhaps most significantly, MasterCard is working with all major issuers and acquirers in selected countries for a coordinated mass market deployment of a CAP + SecureCode solution in the near future.

Interested? Please contact Nick Collin on nick@ncollin.demon.co.uk or **+44 (0)207 833 8765** with comments or questions.

Designed by - Blue Nostromo © 200505