

Case Study: Advanced Payment Solutions (APS)

APS Background

In September 2005, London-based start up Advanced Payment Solutions (APS) launched the first chip and pin-enabled prepaid payment card into the United Kingdom. Its first



product, the **cashplus**[™] prepaid MasterCard®, is a reloadable, full utility, highly secure MasterCard that is accepted at over 24 million merchants worldwide. **cashplus** allows cardholders to perform ATM cash withdrawals, point of sale payments and online and telephone purchase transactions.

Though common in the US, open-loop prepaid payment cards such as **cashplus** are not yet widespread in the UK, despite the fact that about half of the adult population in the UK does not have a credit card and over two million people do not have a bank account. APS' products will provide the “unbanked” (people without bank accounts) and the “underbanked” (people with only basic bank accounts) with access to a secure cash storage and payment facility previously unavailable to them.

Project Drivers

APS required a highly secure system to issue, reload and redeem cards, which could be accessed by customer service representatives, consumers, and merchants. A highly secure infrastructure was a “must-have” for APS, since its system will be used to capture identity details, process card sales, make payments, reload funds and check account balances.

APS originally considered using a one-time password token-based authentication system to verify the online identity of users with varying roles, rights and privileges, such as administrators and merchants. However, the cost of this system was prohibitive and limited the number of people to whom the tokens could be issued. In order to more cost effectively match authentication





strength to the risk level across these different groups, APS partnered with TriCipher, which offers a wide variety of authentication options and allowed APS to centrally manage different authentication strengths across its diverse user base.

Scope

The project enables APS to cover the whole of Europe. It is using the TACS system to provide strong authentication for multiple retail users issuing and redeeming cards, consumers and internal customer service reps. Retail outlets access APS software securely over the Internet to live an instant use ATM card at the point of sale. A personally embossed MasterCard is then mailed to the customer. Once activated and loaded, cardholders can use their cash**plus** MasterCard to make purchases anywhere on the global MasterCard merchant network. The APS chip and pin technology tracks customer behavior and APS software tracks how much money the consumer is spending, retailer commissions by channel and outlet, and reconciles all transactions across the system.

APS is using the TriCipher Armored Credential System™ (TACS) to provide Device 2 factor authentication for retailers and staff. This provides strong, affordable security, authenticating both the user and their location without requiring provisioning of tokens or other hardware devices because the retailers can use their existing PCs as the second factor. Consumers use TriCipher's Armored Passwords, which enable them to use simple passwords while protecting against password theft. The TACS patented architecture makes it extremely difficult to steal a user's credentials, providing critical protection against phishing attacks.

Why APS Chose the TriCipher Armored Credential System™ (TACS)

APS partnered with TriCipher because TACS was the only system to meet all of APS' business and IT security requirements:

- Authentication integrated with a customizable, secure data storage vault.
- The ability to match authentication strength to business risk for different users.
- The ability to manage multiple levels of authentication from a single infrastructure.
- The ability to use the PC as an affordable 2nd factor, avoiding the cost of managing and deploying separate hardware tokens.



- Easily manageable user roaming capabilities.
- Reliable high availability architecture.
- Certified by appropriate security authorities -- TACS is both Identrus and FIPS certified.
- Scalable enough to grow with the business and extensible enough to integrate with new security technologies.

Paul Darnell, IT and Operations Director for APS, said the TriCipher Armored Credential System stood out because it combined so many key product attributes that could not be found in any other single product offering.

“We looked for integrated user security authentication and a customisable data storage vault, as well as role-based tiered security dependent on level of business risk associated with the individual’s access rights. It was important to have customisable software installation for the tethering to specific PCs with a readily manageable user roaming facility and high resilience architecture,” Mr Darnell says.

“Our line of business demands suppliers are certified with appropriate security authorities and as a growing company we wanted to ensure the product chosen was scaleable and extensible as and when new security methods become available. Uniquely, TriCipher managed to fulfill all of these requirements.”

Deployment

Deployment of the TACS authentication infrastructure for the APS system is complete, and is currently serving multiple retail users issuing and redeeming cards, consumers and internal customer service reps. APS has launched and is actively selling its cash**plus** prepaid MasterCard, the first of its kind in the United Kingdom.

More information can be found at: www.apsgroup.com and www.mycashplus.co.uk.

TriCipher, Inc.

1900 Alameda de las Pulgas

Suite 112

San Mateo, CA, 94403

+1.650.372.1300 tel

+1.650.372.1301 fax

www.tricipher.com

sales@tricipher.com