



AN ACONITE SOLUTION PAPER

**Secure Management of
Transit, Infrastructure and
Payments**

**Tim Richards
Business Consultant**



The Aconite Transit Proposition

Aconite's transit issuance solution provides a response to the many changes confronting the operators of mass transit solutions:

- how to design a system that can respond to the kinds of problems identified by the Mifare Classic hacks;
- how to design a system that supports transit operators outsourcing their card issuance to third parties;
- how to provide a system that allows a large number of different card and chip designs to be issued, managed and re-issued;
- how to provide a system that will allow transit operators to migrate their chips from physical cards to other form factors such as contactlessly enabled mobile phones;
- how to provide a system that uses secure EMV type payments mechanisms rather than proprietary solutions.

This paper discusses each of these issues and describes Aconite's solution, based on Aconite Affina® Enterprise Smart Product Management and Aconite Prepaid Value Manager products.

Developing a flexible infrastructure

The recent publicity about the weaknesses in the Mifare Classic card used in many mass transit schemes around the world highlighted a rather important underlying principle of design for systems using smart cards – that it is very unwise to assume that the smart cards themselves will always remain secure. Aconite has over 200 man years of experience in this market and we are well aware that solution design in this area must provide for a flexible infrastructure that allows for the use of different smart card types and cryptographic keys over time. Simply, if a card type is cracked it should be possible to upgrade the infrastructure to support different cards without major capital expense or human interaction.

Aconite Affina Enterprise Smart Product Manager is ideally suited to this and can be used to manage the contents of Secure Access Modules (SAM) across a transit network. By implementing the correct SAM technology Affina Enterprise can be integrated with the transit network to be able to transparently upgrade the technology being used in the various gates and readers. In the event of a security issue then the system can be used to upgrade the security of the SAM applications, to modify the SAM applications (e.g. to replace a Mifare Classic application with an alternative) or to provide an upgrade path between different applications. By designing this type of flexibility into the infrastructure it is possible to build a defensible solution that can be used to rapidly respond to the challenges posed by a world in which computing power is easily available and in which attack methods can be rapidly commoditised and made available over the Internet.



Outsourcing of card issuance

Many transit operators feel that card issuance is not a core part of their business. The essential nature of a transit application in mass transit solutions is such that many existing card issuers will be attracted to the possibility of putting the transit application onto their card to encourage consumers to use their card. Potentially transit operators can gain in two ways – through reducing their card issuance costs and through receiving royalties and fees for the use of their brand and application.

Although this is an attractive proposition, the transit operator needs to retain control of their data as the transit application along with any associated value and tickets will need to be managed. This is especially true in re-issuance scenarios where a customer who has lost their card or is having their card replaced will want their tickets and value re-instated correctly on the new card. Affina Enterprise is ideally suited to managing this kind of data preparation and storage, linking the transit operator's data to the issuance systems of the card issuer and delivering secure transit data into the card issuance facility in order to allow the creation of a proper multi-application card. The system handles the request to block existing cards and re-issue new ones and can be integrated into an existing transit account management system to provide a fully integrated solution.

Managing multiple transit operators

Many transit schemes consist of multiple transit operators using the same card and loading their different tickets to the card. This causes two problems: firstly, the replacement of cards requires data to be drawn from multiple sources to complete the full data needed to make the new card; and secondly, there may be many different physical card designs which require the purchase of lots of small batches of pre-printed plastic, which is an expensive option.

Affina Enterprise can help solve both of these problems. It can manage the integration of data from multiple sources to build the final card data as required. It can also manage and generate data for the card physical personalisation. This may include personal data such as photographs and names but can also include the full card background. Using new technology that allows white plastic cards to be fully personalised, edge to edge, to very high levels of visual quality Affina Enterprise can generate the card's physical data for as many different card types as is required, linked to the correct chip data needed for each one. In a situation where many different physical card types are required this solution can significantly improve the efficiency of the issuing systems and reduce the costs associated with ordering small batches of pre-printed cards.

Migrating to new form factors—NFC-enabled mobile phones

The ability to create new form factors for transit cards is of increasing interest to transit operators. In particular the emerging interest in contactlessly enabled mobile phones with an embedded GlobalPlatform secure element is of major interest for travellers, as this means that in future the transit application could be loaded to the phone which would then transact contactlessly with the transit readers. Not only does this offer the consumer greater convenience, it also reduces the card issuing costs of the issuer and potentially allows for a range of new business models, including using contactless posters and other media to allow timetables to be loaded to the phone, advertising to be linked back to the source of the consumer's interest and an easy way of deploying new prepaid models for use in and outside the transit network.



Affina Enterprise already supports the functionality required to securely download applications to phones and simply requires integration to the local mobile networks to add this new channel.

Using EMV type payment mechanisms

Considerable interest has been raised recently about the possibility to using EMV style payment mechanisms in a transit environment. This arises partially from the concerns around the Mifare problems where the transit ticketing mechanism and the underlying payments process are linked. Using an EMV type solution it is possible to provide a range of possible payment solutions, either using the wider financial networks or a closed loop system for the transit operator. In either case the solution offers the operator the comfort of using a technology that has been tested in an operational environment on a global scale and which will continue to receive considerable investment through the financial community in order to add functionality and maintain security.

Our Prepaid Value Manager product provides our customers with a ready made EMV based solution which allows for the provision of a prepaid product onto transit cards for use in an off-line environment. The integration of these products with transit ticketing and transit accounting applications can offer a complete transit payments solution.

Conclusion

Aconite's products can provide a modern and secure solution to supporting transit application issuance onto multiple platforms and can also allow the use of the latest in smart card payments technology. These products, deployed as part of a wider solution, offer transit operators a flexible and robust infrastructure which can be used to reduce issuance costs, introduce new flexibility and generate new revenue streams while maintaining the highest level of security.



About the Author

Tim Richards is a business systems and security consultant with seventeen years experience in the smart card industry. He was one of the design team for the Mondex electronic purse developed by National Westminster Bank, led the development of the Multos multi-application smart card operating system and was Development Director of the *platform seven* smart card security group. He is the inventor of the Affina Smart Product Management System and has spent the last few years acting as a solutions architect and presales consultant for Datacard Group in both Financial and Government Sectors, covering EMV Migration and the introduction of ICAO e-Passports. Tim now provides Aconite's customers with business and technical analysis consultancy specialising in the development and maintenance of new business solutions using secure smart card systems.

About Aconite Technology Ltd.

Aconite delivers software solutions and provides consulting expertise for managing business applications on chips in smart cards, tokens or mobiles to issuers around the world. We provide a rapid and cost-effective route to implementing new customer propositions, entering new markets and complying with international standards.

Incorporating a unique blend of proven software and professional services, Aconite solutions can be tailored to meet individual business requirements without the need to replace legacy systems and with minimal impact on staff and processes.

Based in the UK, Aconite operates across the globe, with a local presence in many markets.



Aconite Technology Ltd
8 –14 Vine Hill
London EC1R 5DX

Tel: +44 (0)20 7713 4800
Fax: +44 (0)20 7713 4801
Email: enquiries@aconite.net