



e-Smart Combo

Application Note for the Banking & Financial Services Industry

I. Strong Authentication

The solution could be of particular interest to vendors of core banking software.

With the implementation of Core banking solution & access to customers for various transactions on the Internet, a strong authentication becomes very important, particularly when funds transfer is involved.

Datanet's e-Smart Combo supplied as a set of special pocket smart card reader called e-Smart Pocket, a fully personalised smart card, a web service call which can be integrated by the banking software developer and a 24x7 server for verification service constitutes a complete, ready to use and secure solution.

At the time of logging into the bank's website or for specific transactions which demand strong authentication, this capability can be used. It essentially works as a challenge-response system. The customer enters a 16-digit card serial number; the authentication server displays a 8-digit challenge to which the customer generates a response (TAC) using the e-Smart Combo. This is verified before access is given or command is accepted.

The USP of e-Smart Combo is that it can generate the response for multiple upto 8-digit data strings (no limit).

NOTE: As e-Com Pocket works in an unconnected mode, it can be used with desktop PCs, PDAs or mobile devices that can connect to Internet.

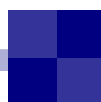
Consider some examples:

Consider the case where the e-Banking facility allows linked accounts of a single customer.

For own account funds transfer, the data needed could be:

- (i) From acct No.
- (ii) To Acct. No.
- (iii) Amount
- (iv) Currency code
- (v) Any other special input

Using e-Smart Combo a TAC can be generated involving all the above inputs, thus giving a very high level of assurance & non-repudiation to the transaction.





For third party funds transfer, the data items could be:

- (i) From Acct. No.
- (ii) 3rd party branch code (numeric)
- (iii) 3rd party acct. type
- (iv) 3rd party acct. No.
- (v) Amount
- (vi) Currency code
- (vii) Any other special input

Using e-Smart Combo a TAC can be generated involving all the above inputs, thus giving a very high level of assurance & non-repudiation to the transaction.

Consider the case of Stop Cheque service in which typically,

- (i) Account number
- (ii) Cheque number
- (iii) Amount
- (iv) And perhaps cheque date are involved.

Using e-Smart Combo a TAC can be generated involving all the above inputs, thus giving a very high level of assurance & non-repudiation to the transaction.

Use for Demat account transactions

The power of generating TAC from data items could also be used for demat account holders for relevant transaction on the Internet where non-repudiation may be of considerable value.

In this case TAC can be generated for a suitable combination (depending on the option chosen by the user) of the following data items:

- (i) DP Acct. No.
- (ii) DP ID
- (iii) Client ID
- (iv) CMBP ID
- (v) Settlement No.
- (vi) Execution date
etc.,



**INNOVATION**

2. Loading e-Purse

Datanet has created a unique method by which e-Purse of the smart card with e-Smart Combo can be credited with value in an unconnected mode. The scenario assumes that the balance in the customer's account is available on a central server that is accessible over Internet. The customer first logs into the server with suitable authentication, including e-Smart Combo based strong authentication. Then he/she go thro a simple sequence of steps using the e-Smart Combo, at the end of which the desired amount is debited from the central server's account & credited to the smart card's e-Purse.

This can be used in any situation where e-Purse value can be used meaningfully such as e-Cash, or Credit Limit or any representative value. What is more, up to ten purses can be loaded with values. The system incorporates rigid 3DES security.

This could be of particular interest to closed user groups with centralized accounts server.

3. Anti-phishing

Phishing is the act of sending e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. Strong authentication is one of the best remedies for Phishing attacks.

Datanet's e-Smart Combo, consisting of a pocket smart card reader called eCom Pocket and a smart card along with associated software at the server end is a complete & affordable Anti-Phishing solution, particularly for the financial institutions.

The solution does not require any software to be loaded or installed at the client PC. The pocket smart card reader is used in 'unconnected mode'. The e-Smart Combo is very attractively priced making it possible for customers to possess the same. The 'Authenticode' generated by the server software and verified by eCom Pocket is unique to each customer and can be used in two variations (either or both): (i) to validate the e-mail by including it in the message (ii) for strong authentication to the web site.

Complete system including security management is available.

This could be of particular interest to financial institutions.

For details contact**Datanet Systems limited**

II Floor, GRS Complex, No.90,
2nd Cross, 8th Main, JP Nagar III Phase
Bangalore - 560 078

Phone: 91(80) 66648 200 **Fax:** 91(80) 66648 203

Email: vish@datanetsystems ltd.com