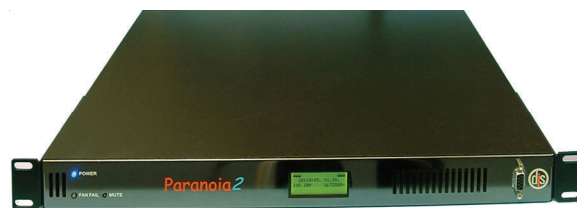




iSecure & iCard



OUTLINE

iCard - Smartcard Configuration GUI

Security management package which allows for the personalisation of the smart cards and includes the software and hardware necessary to add to a standard Windows based system

iSecure - Paranoia2 GUI

Operations management package, this includes a GUI and hardware to allow Paranoia or SafeTape units to be controlled via the smart card system.

FEATURES

- **key generation**
- **key management**
- **key entry**
- **selection of encryption modes**
- **selection of secure or non secure modes**
- **engineering functions**
- **audit logging and reporting**

THE SOLUTION

iSecure allows the utilisation of smart card technology to control and manage the Paranoia2, ParanoiaFF and SafeTape products, functions include:

- Key entry
- selection of encryption modes
- Selection of secure or non secure modes
- Engineering functions
- Audit and reporting

The product consists of two elements:

iCard - Smartcard Setup GUI

Management package which allows for the personalisation of the smart cards and includes the software and hardware necessary to add to a standard Windows based system.

iSecure - Paranoia2 Setup GUI

Package, which includes a new GUI and the hardware, to allow the control of Paranoia or SafeTape units via the smart card system.

As part of this update the front panel status is now available on the GUI to allow for the remote monitoring of the units if required. For security this function is also password protected.

Avax will supply the pre-programmed smart cards for the customer to personalise.

iSecure & iCard

Part No	Description
SMST0-01	Smartcard starter kit: Contains iCard and iSecure software, 2 USB card readers and 10 smartcards

AVAX INTERNATIONAL

8 Thompson Crescent
 Erin, ON N0B 1T0 Canada
 Tel: +1-519-833-2900 or 1-800-443-4542
 Fax: +1-519-833-7469
www.avax.com



iCARD

This would normally be controlled by the Audit/ Security department within an organisation. Smartcards can be configured to allow staff to carry out all functions with differing levels of authority and can be site specific or cover all sites within the business. Cards are personalised by the customer to contain:

- Key(s) if their access level requires it
- User ID and full Name,
- User Access levels
- User pin (random number generator)
- P2 Password
- Issue Number
- Site ref

To activate the cards the user is required to enter a PIN number, this maybe personalised by the user, any change will be recorded in the audit log. All data on the card is encrypted except for the user name.

iSECURE

This is the operations management element of the solution and contains a secure database which will be automatically updated as users use their cards. Any card that is either lost or has been superseded (i.e. user rights changed) will automatically be voided when the new card is used.

Keys, encryption methodology and passwords are loaded into the Paranoia2 via a set of smart cards generated by the iCard system, at no time is this information visible to the operations staff.

When a smartcard is inserted the user will only be able to access the authorised functions e.g. if they are an operator the only information available to them is the status of the Paranoia2 appliances.

Available from: