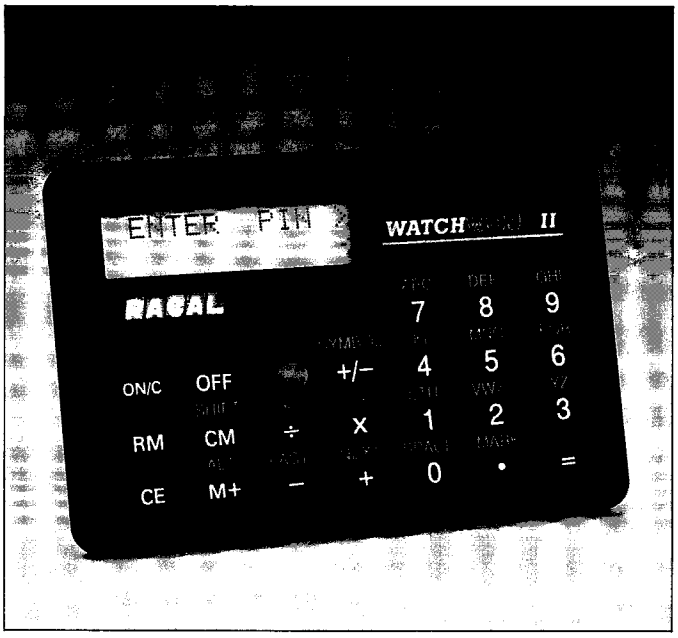
Personal Authentication Range RG551/RG552
WATCHWORD II User Tokens

Guardata Range of Products and Services



WATCHWORD II is the state-of-the-art in hand-held personal authentication tokens and addresses two distinct application areas:

- **Secure User Identification**
- **Message or Payment Authentication**

The token uses the DES algorithm and is compliant with relevant ISO and ANSI security standards.

Users enter data in response to a series of issuer-definable alphanumeric prompts, allowing the token to be used in customised and multilingual applications. Each token is fully configurable and can support up to 8 users, accessing up to 16 separate applications and can store up to 78 issuer-definable prompts.

Man Machine Interface

The WATCHWORD II token contains a two-line display with twelve characters per line. The top line is a dot matrix display giving a full alphanumeric capability. The lower line is a conventional 7 segment numeric-only display. Every prompt and message can be defined by the issuer and may be customised for each token. This is particularly useful in customer specific and multi-lingual applications.

The keypad uses keys with moving raised buttons spaced sufficiently far apart to give a friendly and convenient operation. These features, plus a positive tactile feel to the keypad, help to ensure that input errors are kept to a minimum.

Secure User Identification

The growth of data networks and their rapidly widening applications has exposed serious risks of theft and tampering. These are especially high when computer data can be accessed via telephone and packet switched networks.

Passwords are often used to restrict network access through terminals, in an attempt to reinforce security, but many such systems are easily compromised. All too often, easily guessed names or telephone numbers are used as passwords and these are not changed sufficiently often, if at all. Passwords are always entered in the clear and, as such, are inherently vulnerable. The use of passwords therefore can make unauthorised access relatively easy.

WATCHWORD II provides a convenient-to-use alternative to passwords, that offers a greatly increased level of security. Unlike passwords, when using WATCHWORD II, critical information is never transmitted in the clear.

The principle of operation of WATCHWORD II is based on the well known Challenge/Response mechanism described in the Secure Sign-on Standard (ANSI X9.26). The user enables the token by entering a Personal Identification Number (PIN). A seven digit challenge, supplied from the host computer system is entered into the token, which then generates a seven digit response. The response is calculated from the challenge using a cryptographic process.

At the heart of the process is the widely acknowledged DES algorithm (ANSI X3.92) which uses a cryptographic key that is unique to each user. The key is stored inside the token. The PIN personalises the token to its user, and the same key, stored at the host, enables the system to establish the validity of the user. The fact that a different challenge is issued at each access attempt means that even if someone is monitoring the communication channels, he will gain no information which will enable him to impersonate a valid user.

A verify facility is also provided by the WATCHWORD II token. This allows a WATCHWORD II user to issue a challenge to another user and to verify the response without being able to compute the response himself. There is no practical limit to the number of users that can be verified by this technique. In a network application, tokens can be configured so that any user can authenticate, but not impersonate, any other user.

Message Authentication

The WATCHWORD II token may also be used to calculate a Message Authentication Code (MAC). A typical application where this function might be used is the authorisation of payment instructions. This facility enables a user to add a unique signature to the instruction, which can later be verified as originating only from that user. Any attempt to modify an instruction after it has been signed can therefore be detected.

The Message Authentication function allows a user to enter a series of data items via the keypad. These are then processed to form a MAC. Each data item may be up to 12 characters in length, and may, if required, be alphabetic as well as numeric. Longer fields (up to 63 characters) may be entered, but these will scroll off the display. The length, type (numeric, alphabetic, alphanumeric or hexadecimal), format (fixed or free) and textual prompt for each data item is fully configurable by the issuer. This feature improves user-friendliness by reducing operator errors and also allows the token to be used in multi-lingual applications. When the last field has been entered, the MAC is generated and displayed in the required format. The MAC is produced using one of up to sixteen keys which are stored in non-volatile memory. The key itself, and the number of keys available for use, are established at initialisation time. The MAC is generated in accordance to the internationally recognised standards (ANSI X9.9 / ISO 8731-1) to produce an eight hexadecimal character value. If required, a decimal digit MAC of up to twelve characters may be produced as an alternative.

Another configurable option available on WATCHWORD II is for a sequence number to be maintained by the token. This is incremented every time a MAC is generated, and is used to detect message duplication at the recipient site.

A MAC verify facility is also provided by the WATCHWORD II token which allows a MAC computed by another user to be verified. Only the originator can compute the MAC. This facility provides a type of digital signature for non-repudiation purposes. In a network application, the token can be configured such that any user can verify (but not fraudulently originate) any message received from any other user.

PIN Management

Access to a WATCHWORD II token is normally controlled by a user PIN. The token supports a number of PIN management philosophies and variations which are determined at configuration time. The PIN mechanism may also be disabled, if required.

Each user may also be issued with a second PIN for use under duress. Use of the second PIN can be detected at the host end and appropriate action taken.

User PINs may be up to 8 digits long. A minimum length of PIN may be specified at initialisation time. A user may change his PIN at any time and may be forced to change his PIN on first use. The token can prevent the previous PIN or a trivial PIN being used. The issuer can determine whether PINs are echoed back when entered. The WATCHWORD II token can be configured either to give a wrong result if a wrong PIN is entered or to display a warning message. If the latter approach is taken, then the token will become locked after a pre-determined number of consecutive PIN entry attempts has been exceeded. At this point, even submission of the correct PIN will not allow access to the token.

A user may be unlocked either by local entry of an 'Unlock' PIN or by a remote interchange with a central site. This second option is particularly useful where users are remote, but where an Unlock facility, controlled centrally, is required. Lock and Unlock facilities may be disabled at configuration time.

Multiple Functionality

Each WATCHWORD II token can support up to eight separate users, each with up to two PINs. This allows the total system costs to be significantly reduced by having multiple users for each token.

Each WATCHWORD II token can also support up to 16 separate keys, which can be used independently for any of the following services: WatchWord Generate, WatchWord Verify, MAC Generate, MAC Verify, Help or Unlock. (The Help service simply displays a sequence of issuer-definable messages.) Each key can be assigned to any user, or group of users, thus allowing complete flexibility for the issuer. Each token can therefore allow access to 16 separate systems, reducing total system costs still further.

Calculator

The WATCHWORD II token may also be used as a five function calculator with memory (Add, Multiply, Subtract, Divide and Reciprocal). The calculator function can be disabled by the issuer, if required.

Battery Change

The WATCHWORD II token is powered by a single lithium battery. A second battery compartment is provided to allow the battery to be changed easily in the field, without losing the configuration data.

Token Initialisation

The WATCHWORD II token is provided with an electrical interface for electronic initialisation and operation.

The RG570 WATCHWORD II Initialisation Facility PC software package and the RG560 Programming Interface together provide a secure, convenient and efficient mechanism for initialising and issuing WATCHWORD II tokens and associated PIN mailers. A number of hooks and exit points are available to facilitate integration with other host processing systems.

Access to the electrical interface is strictly controlled. A token, which is to be used to access two separate systems, may be partially initialised by one issuer and completed by the other issuer.

Compatibility

The WATCHWORD II token is backwards compatible with earlier generations of the product, including Racal-Datacom's RG500 WatchWord Generator.

Personal Authentication Range
RG551/RG552
WATCHWORD II User Tokens

Guardata Range of Products and Services

Technical Specification

Options	RG551 - Full function token, excluding MAC functionality	
	RG552 - Full function token, including MAC functionality	
	RG560 - Programming Interface	
	RG570 - WatchWord Initialisation Facility PC software package	
Functionality	1 - 8 users per token	
	1 or 2 PINs per user	
	78 Issuer-Definable Prompts	
	16 Services (WatchWord Generate, WatchWord Verify, MAC Generate*, MAC Verify*, Help or Unlock) * RG552 only	
Dimensions	8mm x 100mm x 65mm	
Display	2 Line LCD Upper line: 12 character alphanumeric dot matrix	
	Lower line: 12 character 7 segment	
Algorithms	Data Encryption Algorithm (ANSI X3.92)	
	15 proprietary algorithms	
Cryptographic Standards	ANSI X3.92 Data Encryption Algorithm	
	ISO 8731-1 Message Authentication	
	ANSI X9.9 Message Authentication	
	ANSI X9.26 Secure Sign-on	
Battery	Panasonic CR2025 135mAhour 2.7V lithium coin cell	
	Battery Life: 2 years when used no more than 20 minutes a day	
Environmental	Operating Temperature Range:	5°C to 40°C
	Storage Temperature Range:	-10°C to +50°C
	Humidity:	Up to 95% relative humidity at +40°C

Racal-Datacom

Racal-Datacom Ltd.
Landata House,
Station Road, Hook
Hampshire UK
RG27 9PE
Telephone 0256 763911
Fax 0256 764717

RACAL