

# RSA SecurID Ready Implementation Guide



## SecurID Ready Implementation Guide

### Ericsson R380

Last Modified October 26, 2000

#### 1. Partner Information

Partner Name	Ericsson
Web Site	<a href="http://www.ericsson.com/">http://www.ericsson.com/</a>
Product Name	R380
Product Description	RSA SecurID for the Ericsson R380s Smartphone is an authentication system that positively authenticates valid network users to networks and services that are protected by an RSA ACE/Agent. RSA SecurID for the Ericsson R380s Smartphone provides the same two-factor authentication solution as all other SecurID authenticators, combined with the convenience of the multi-functional Ericsson R380s mobile phone handset. In addition, RSA SecurID for the Ericsson R380s Smartphone enables secure connections to WAP-enabled services.
Product Category	Wireless Communications



## 2. Contact Information

	Pre-Sales	Post-Sales
Name	Sales	Support
Phone	1.800.ERICSSON	1.800.ERICSSON
Web	<a href="http://www.ericsson.com/">http://www.ericsson.com/</a>	<a href="http://www.ericsson.com/">http://www.ericsson.com/</a>

## 3. Product configuration

### • Administrative Setup

To enable RSA SecurID protection on a user's mobile phone, you must:

- Import the RSA SecurID Software Token records into the RSA ACE/Server database
- Create a record for the user in the ACE/Server database and assign one of the token records to the user
- Send the user the activation license that corresponds with the user's token record serial number. The user must then correctly enter the activation license into the mobile phone.

### To install and activate RSA SecurID on the Ericsson R380s Smartphone:

1. Import the RSA SecurID token records to the RSA ACE/Server database.  
The Software Token files are on the token record diskette and have the extension **.ASC**. For instructions on how to import the token records, see the RSA ACE/Server documentation.
2. In the RSA ACE/Server database, create user records for each user, and assign each user an RSA SecurID Software Token.
3. In the RSA ACE/Server Data Administration application, list the user's record to display the user's assigned token serial number.
4. On the *RSA SecurID Phone Activation Licenses* diskette, locate the activation license file whose serial number matches the serial number associated with the user's token record in the RSA ACE/Server. The activation license files have the extension **.SAL**.
5. Copy the activation license; paste it into a text file, and save the text file. The activation license is the string of characters that follows the colon. For example, in the activation license file **3314794:AJ6K452Y6N2HSCT3YE69EB2DHSRH2**, the numbers **3314794** represent the serial number, and the characters **AJ6K452Y6N2HSCT3YE69EB2DHSRH2** represent the activation license.
6. Distribute the activation license to the user.
7. Distribute the *RSA SecurID for the Ericsson R380s Smartphone End-User's Quick-Start Guide (r380user.pdf)* to the user. Distribute the documentation to users when you distribute their activation licenses.

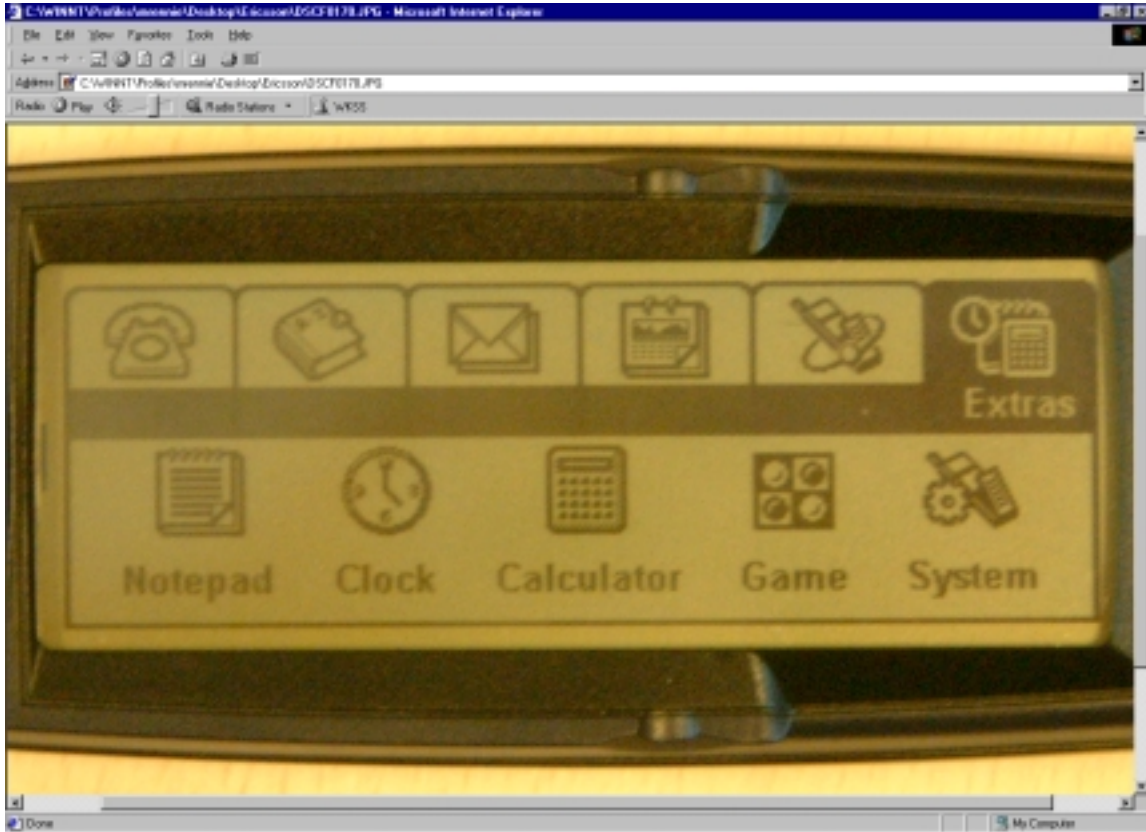
## RSA SecurID Ready Implementation Guide

- **User Setup**

To activate RSA SecurID on your mobile phone, you must obtain an activation license from your administrator (see previous steps). The license consists of approximately thirty alphanumeric characters that you must key in to your mobile phone.

**To activate RSA SecurID on your Ericsson R380s Smartphone:**

1. Make sure that the phone is on and in standby mode.
2. Open the flip, and tap the **Extras** tab:



3. Tap **System**.
4. Tap **Preferences**, then **Messaging**, and then **One-Time Passcodes**.
5. Tap **Initialise RSA SecurID**. If an activation license is already installed on the phone, the activation program prompts you to confirm the removal of the previous license. If you are not sure whether you want to remove the previous license, select **No**, and consult your administrator.
6. Tap the **Activation License** input field. The activation license input view appears, showing a software keyboard at the bottom of the screen.
7. Use the keyboard to enter your activation license. The license is not case-sensitive. However, do not enter a space or carriage return at the end of the activation license string. If you do, the activation license will be rejected.
8. Tap to return to the **Initialise RSA SecurID** view, then tap **OK** to continue. If you enter a correct license, the message, "RSA SecurID has been successfully initialized" appears briefly. RSA SecurID Software Token is activated on your mobile phone. If you see this message, do not continue on to the next step. If you enter an incorrect license, the message, "Activation license incorrect" appears. If you see this message, continue on to Step 9.
9. At the message, "Activation license incorrect," tap **OK** to return to the **Initialise RSA SecurID** view.
10. Tap the activation license text to access the software keyboard. The incorrect license remains in the input field so you can compare what you entered with the correct activation license.
11. Repeat Steps 7 and 8 to re-enter the activation license.

## RSA SecurID Ready Implementation Guide

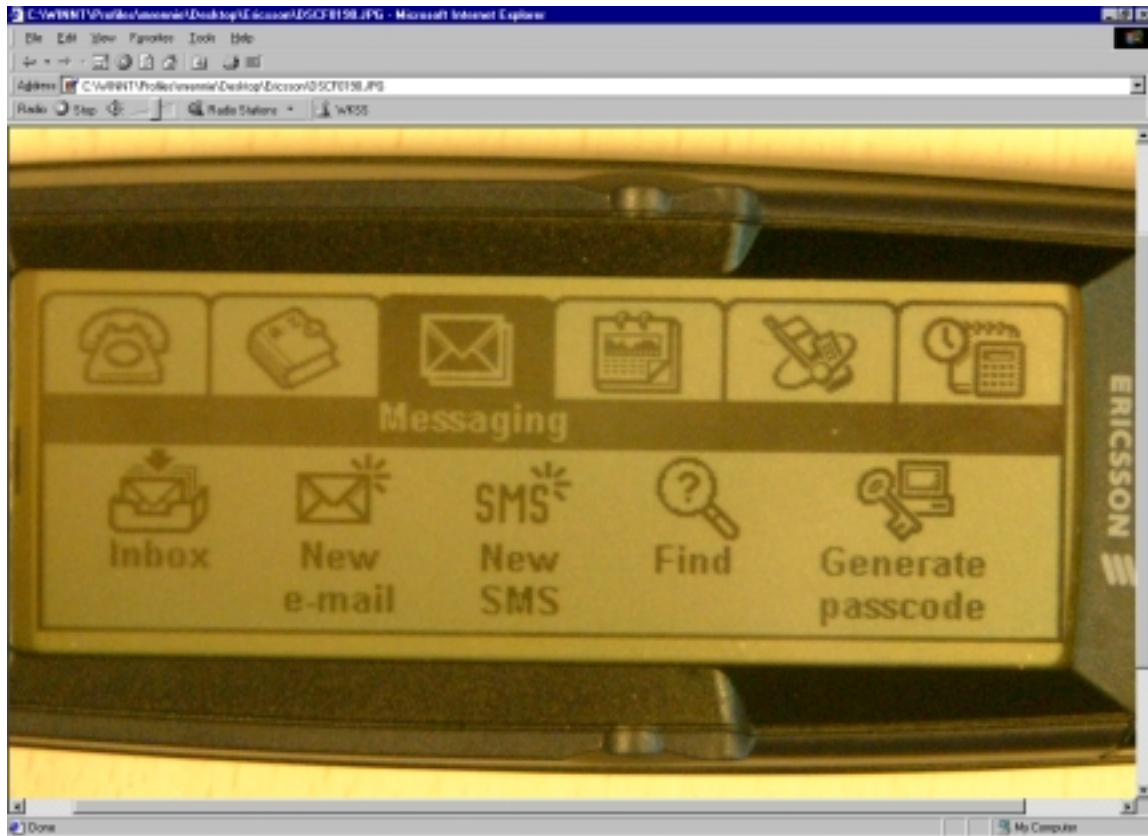
### Using RSA SecurID on the Ericsson R380s Smartphone

The RSA SecurID software token provides you with a PASSCODE that enables you to access protected services and networks.

### Using RSA SecurID on the R380s Smartphone with a Personal Computer

To access a protected service or network from a personal computer, you use the Ericsson R380s Smartphone to generate a PASSCODE. Then, on your computer, you type the PASSCODE when you are prompted for it.

1. Open the flip, and tap the **Messaging** tab:



2. Tap **Generate passcode**. The Generate Passcode view appears.
3. Tap the **PIN** input field. The software keyboard view appears. Use the keyboard to enter your PIN. If you have not been assigned a PIN, or if your PIN has been cleared by your administrator, leave the input field blank and continue with the next step.

## RSA SecurID Ready Implementation Guide

4. Tap to return to the Generate Passcode view, and tap **OK** to continue. The PASSCODE appears for 60 seconds:



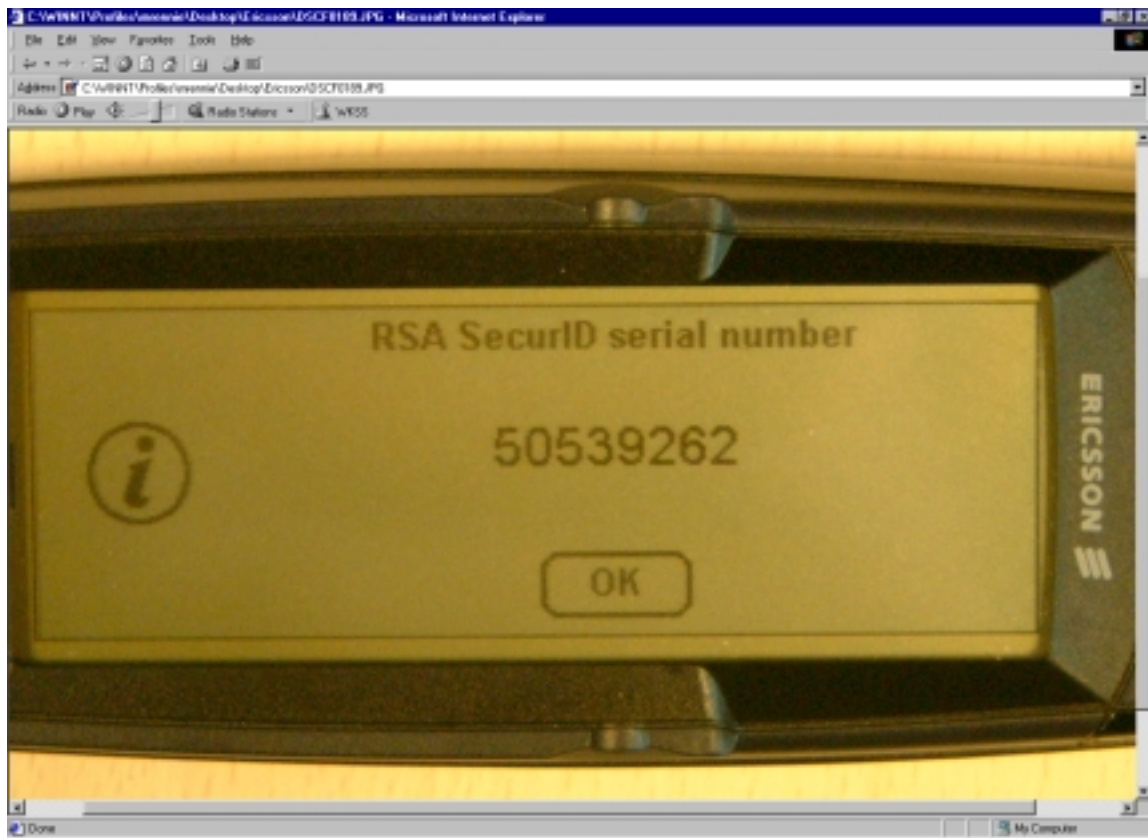
5. When you are prompted for it, type the PASSCODE. Be sure to type in the PASSCODE within the 60-second interval, or the PASSCODE will not be valid. If you are prompted for a second PASSCODE, wait 60 seconds until the software token on your phone generates a new PASSCODE, then repeat steps 1 through 4.



## RSA SecurID Ready Implementation Guide

### Troubleshooting

- If login attempts consistently fail, verify that the time settings on your mobile phone are correct in relation to Coordinated Universal Time (UTC) time, also known as Greenwich Mean Time (GMT). Because RSA SecurID relies on UTC, the time, date, and time zone settings on your mobile phone must always be correct in relation to UTC. If the time settings drift, authentication to SecurID-protected networks and services cannot take place. To get UTC, call a reliable time service. For instructions on how to change the time settings on your mobile phone, see the *Ericsson R380s User's Manual*.
- Inspect the RSA ACE/Server logs to determine whether the user's token has been disabled because of failed login attempts.
- Verify that the user has installed the correct activation license on the mobile phone by listing the activation license serial number on the phone, then verifying that it matches the serial number assigned to the user in the RSA ACE/Server.
  1. Open the flip, and tap the **Extras** tab.
  2. Tap **System**.
  3. Tap **Preferences**, then **Messaging**, then **One-Time Passcodes**, and then **Get serial number**. The RSA SecurID activation license serial number appears:



## 4. Known Problems

None

## RSA SecurID Ready Implementation Guide

### 5. Certification Checklist

The following are the original tests performed against the Ericsson R380 during the QA testing process:

Test Description	Results
<b>Successful Authentication</b>	<b>PASS</b>
1. Select Messaging   Password Access   SecurID	
2. Enter <i>correct</i> PIN and press 'Enter'	
3. Use the resulting Passcode to perform a test authentication on the ACE/Agent	
4. Test must result in successful authentication message	
<b>Unsuccessful Authentication</b>	<b>PASS</b>
1. Select Messaging   Password Access   SecurID	
2. Enter <i>incorrect</i> PIN and press 'Enter'	
3. Use the resulting Passcode to perform a test authentication on the ACE/Agent	
4. Test must result in unsuccessful authentication message	
<b>Next Tokencode</b>	<b>PASS</b>
1. Place the token in Next Tokencode Mode by trying 3 unsuccessful authentications	
2. Select Messaging   Password Access   SecurID	
3. Enter correct PIN and press 'Enter'	
4. Use the resulting Passcode to successfully authenticate on the ACE/Agent	
5. ACE/Agent will prompt for Next Tokencode	
6. Select Next Tokencode Button	
7. Use the new PRN as the Next Tokencode on the ACE/Agent	
8. Test must result in successful authentication message	
<b>New Pin Mode</b>	<b>PASS</b>
1. System generated PIN	
2. Set ACE/Server to system generated PIN	
3. Place token in New PIN mode	
4. Authenticate with just the PRN displayed on the Ericsson R380 SecurID (this may require a Null PIN – '0000')	
5. The system will generate the PIN to be used in the rest of this test	
6. Use the PIN on the Ericsson R380 SecurID to generate a Passcode	
7. Use the generated Passcode to successfully test authenticate	
<b>User generated PIN</b>	<b>PASS</b>
1. Set ACE/Server to user generated PIN	
2. Place token in New PIN mode	
3. Authenticate with just the PRN displayed on the Ericsson R380 SecurID (this may require a Null PIN – '0000')	
4. The user will create the PIN to be used in the rest of this test	
5. Use the PIN on the Ericsson R380 SecurID to generate a Passcode	
6. Use the generated Passcode to successfully test authenticate	
<b>User selectable PIN</b>	<b>PASS</b>
1. Set ACE/Server to user selectable PIN	
2. Place token in New PIN mode	
3. Authenticate with just the PRN displayed on the Ericsson R380 SecurID (this may require a Null PIN – '0000')	
4. The user may select whether to create their own or let the system generate the PIN to be used in the rest of this test	
5. Use the PIN on the Ericsson R380 SecurID to generate a Passcode	
6. Use the generated Passcode to successfully test authenticate	