



Secode Mobile Encryption

Because the Internet and IT never sleep, certain security services must be in place and managed 24/7 - a demanding challenge for most companies. When going mobile the basic premise of deploying enterprise mobility is to enhance workforce productivity and effectively cut operational costs. While it is understandable that enterprises are concerned about the security of their valuable data and information while transmitting it over wireless networks, their IT department should work closely with the solution providers in defining the policies and security requirements for the solution.

Secode Mobile Encryption is a solution that gives a solid foundation for preventing unwanted access to corporate data stored on mobile devices of corporations.

Research shows that the majority of lost or stolen mobile devices contain confidential company communications and information. Applications such as push email make it even more difficult to keep track of the information stored on these highly mobile smartphones and PDAs. The new generation of mobile devices is in many respects like portable PC's where a lot of information is stored thus - the need for encryption is obvious.

Secode Mobile Encryption service provides our customers with a comprehensive solution for securing corporate information stored on mobile devices.

Features

- Strong encryption (AES-128)
 - Centrally enforced authentication policies
- Centrally enforced encryption policies
 - E-mail
 - Calendar
 - Contacts
 - Files and Folders
 - Memory Cards
- Secure remote password reset by phone (helpdesk)
- Management integrated with Secode Mobile Manager

The solution

Secode Mobile Encryption Service adapts to the different needs of the corporation, allowing for customization of the encryption policies implemented across different user groups and devices. The mobile encryption does not encrypt system information but focuses on securing the content created and stored on the device by either various services or the user.

The encryption is easy to use from an end user perspective. Access to encrypted information is granted once the user successfully has entered the password. The encryption is closed either by the user or by time triggers that are set and enforced centrally. The end user has no rights to remove the encryption or bypass the policies set. If the user forgets the password it can be safely reset remotely by phone with the assistance of the help desk operator.

Service Startup

Starting to use Secode Mobile Encryption service is very easy because nothing has to be installed on in the customer's network. The customer only has to subscribe on the necessary amount of user rights and inform Secode whether he/she wants to manage the service him-/her-self or have Secode do the managing. After this Secode enable the service and inform the customer about how to manage the service and how the support is arranged for.

Supported Devices

- Nokia (Series 60 3rd ed. phones)
 - E- and N-series phones
- Sony-Ericsson (UIQ 3 phones)
 - P1i, W950i, M600i, P990i, W960i
- Windows Mobile Phone 5 and 6 devices

References

For information on previous project- and service- deliveries please contact Secode.

Additional Information

Additional information about Secode and our services is found at www.secode.com. You can also contact us on the phone +46 564 875 00 or by e-mail info@secode.com