

Hand-held Communications Security Features Checklist

Core Security Functionality

Encryption
Storage Security
Storage on Device
Storage on Network Server
User Authentication

Network Security

Transmission Security
User Authentication to Network
Device Authentication to Network
Server Authentication

Availability

Emergency Bypass
Incoming Call Answer
Malware

Privacy

E-mails / Text Retention
Disposal of Device

Change Security Parameters

Change Password
Change Key
Key Expiry
Data Recovery after Key Expiry

Conformance to Protocol Standards

Cellular phone standards
Internet standards
TCP/IP
Corporate E-Mail
Secure Hypertext Transport Protocol

Authentication

Password Management
Password Lockout
PKI Based Authentication
Multi-factor Authentication
Online Revocation of Access
Automatic Off-line Revocation of Access
Automatic Log-off
Password Recovery
Administrator Recovery
Third Party Recovery

PKI Standards

X.509 Public Key Certificates
LDAP Repository
Certificate Revocation
Cryptographic Algorithms

Cryptographic Standards

Encryption Algorithms
Advanced Encryption Standard (AES)
Triple- Data Encryption Standard (3DES)

Key Establishment Algorithms

Rivest, Shamir, Adleman (RSA)
Other algorithms based on exponentiation of finite fields
Key Exchange Algorithm (KEA)
Elliptic Curve algorithms

Digital Signature Algorithms

RSA
Digital Signature Algorithm (DSA)
Other algorithms based on exponentiation of finite fields
Elliptic Curve Digital Signature Algorithm (ECDSA)

Hashing Algorithms

SHA-1
SHA-224
SHA-256
SHA-384
SHA-512

Cryptoperiod

Should be appropriate for the algorithm in use

Configurability

Changeable Default Values
Logging

Usability

Configuration by Users
Authentication by Users
Maintenance by Administrators
Reconfiguration by Administrators

Manageability

Remote Management
Authentication of Management Traffic
Encryption of Management Traffic
Central Management

Scalability

Degree of Scalability