

Voice over Internet Protocol (VoIP)

Security Features Checklist

Core Security Functionality

Encryption
 Wireless Encryption
 Opportunistic Encryption
 Caller ID
 Emergency Services (911)
 Caller Location
 Availability
 CODEC
 Redundant Internet / PSTN
 Connection
 VoIP protocols
 NAT Gateways
 Firewalls and packet filters
 Proper Protocol Format
 Filtering
 IDS
 Quality of Service
 Indicators
 Routers and Switches
 Remote Management of
 Network Elements
 Segregation of Traffic
 Hardware Handsets

Conformance to Protocol Standards

Internet Protocol Security
 Transport Layer Security
 Secure Real-time Transport
 Protocol
 MIKEY Protocol
 Internet Key Exchange

Authentication

Password Management
 Password Lockout
 PKI Based Authentication
 Multi-factor Authentication

PKI Standards

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

Cryptographic Standards

Encryption Algorithms

RSA
 KEA
 Elliptic Curve algorithms

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

Assurance Standards

FIPS 140-1
 FIPS 140-2
 Common Criteria – EAL 3
 or higher
 Protection Profile or
 Security Target

Configurability

Changeable Default Values
 Allow or Disallow
 Encryption
 Allow or Disallow
 Authentication
 Logging

Usability

Configuration by Users
 Authentication by Users
 Maintenance by
 Administrators
 Failed logins
 Reconfiguration by
 Administrators
 Password Recovery
 (Administrator-assisted)

Manageability

Central Management
 Authentication of
 Management Traffic
 Encryption of Management
 Traffic

Scalability

Degree of Scalability