Ingenu System Security

Farooq Anjum
Cyber Security, Systems Design & Test
Nov 2015

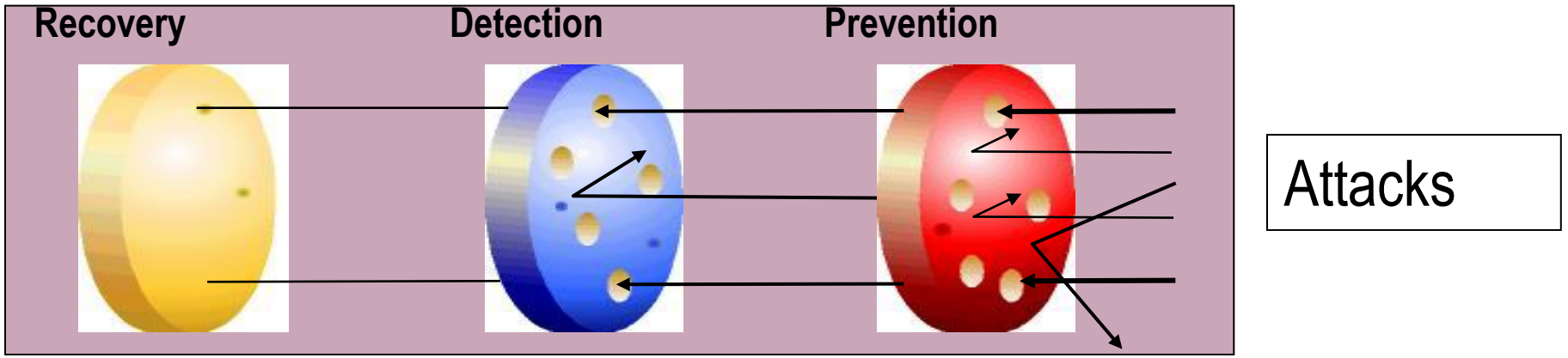
TRN Security – the 12,000 ft view

Security Approach

- Security mechanisms designed for long life (20+ years), power constrained, low bandwidth networks
- Implementing secure software
- Security mechanisms not bolted on but part of the design
  - Supports NERC CIP 002-009 and NIST SP 800-53 guidelines for critical cyber assets
  - Meets FIPS 140-2 Level 2
  - Follows guidelines prescribed in NISTIR-7628

ORW Security Approach

- Defense in depth strategy



Independent Security Evaluation

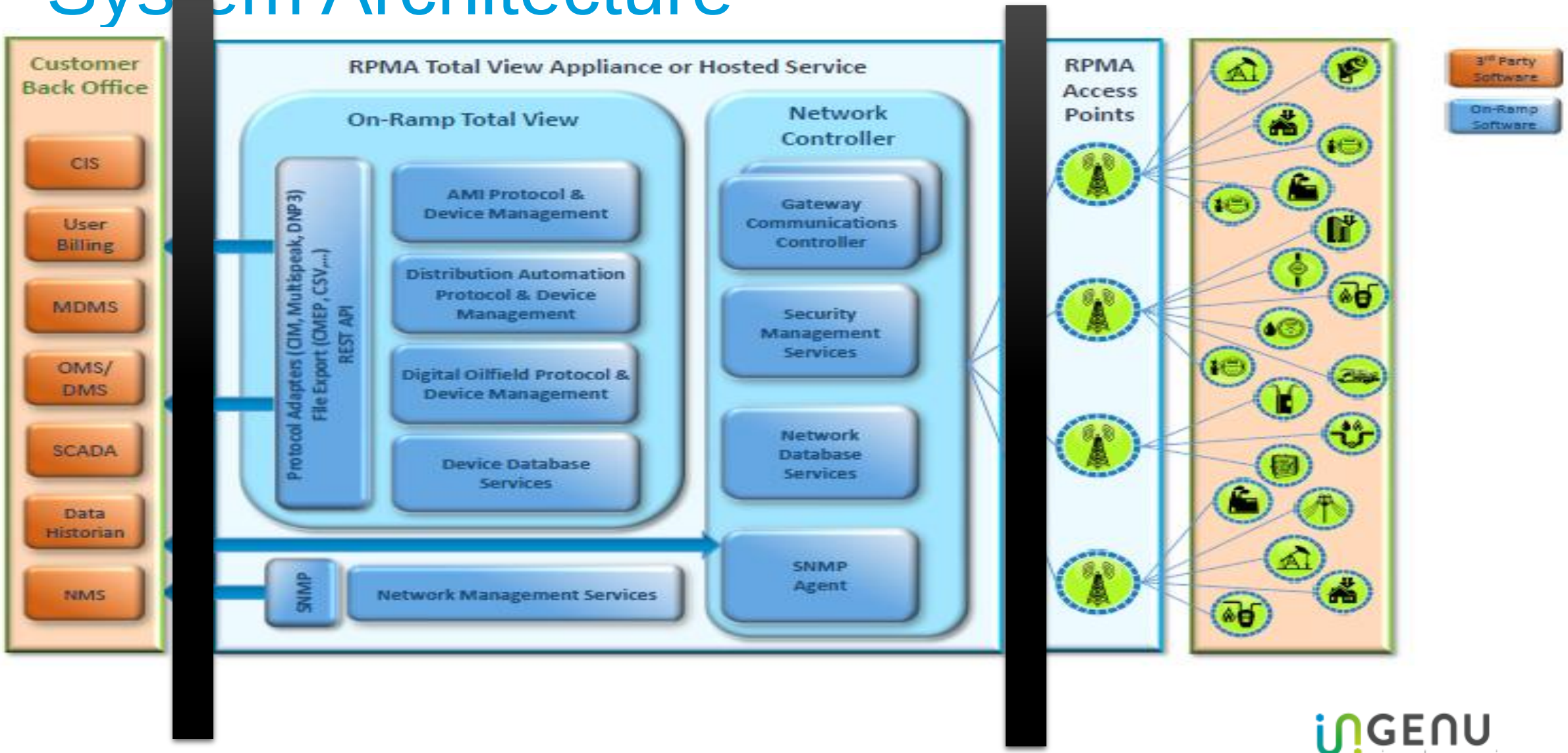
- On-Ramp completed 3rd party security design audit with InGuardian

- SDG&E contracted 3rd party organization for exhaustive security evaluation of On-Ramp system

Technical Overview

1200 ft view!

System Architecture



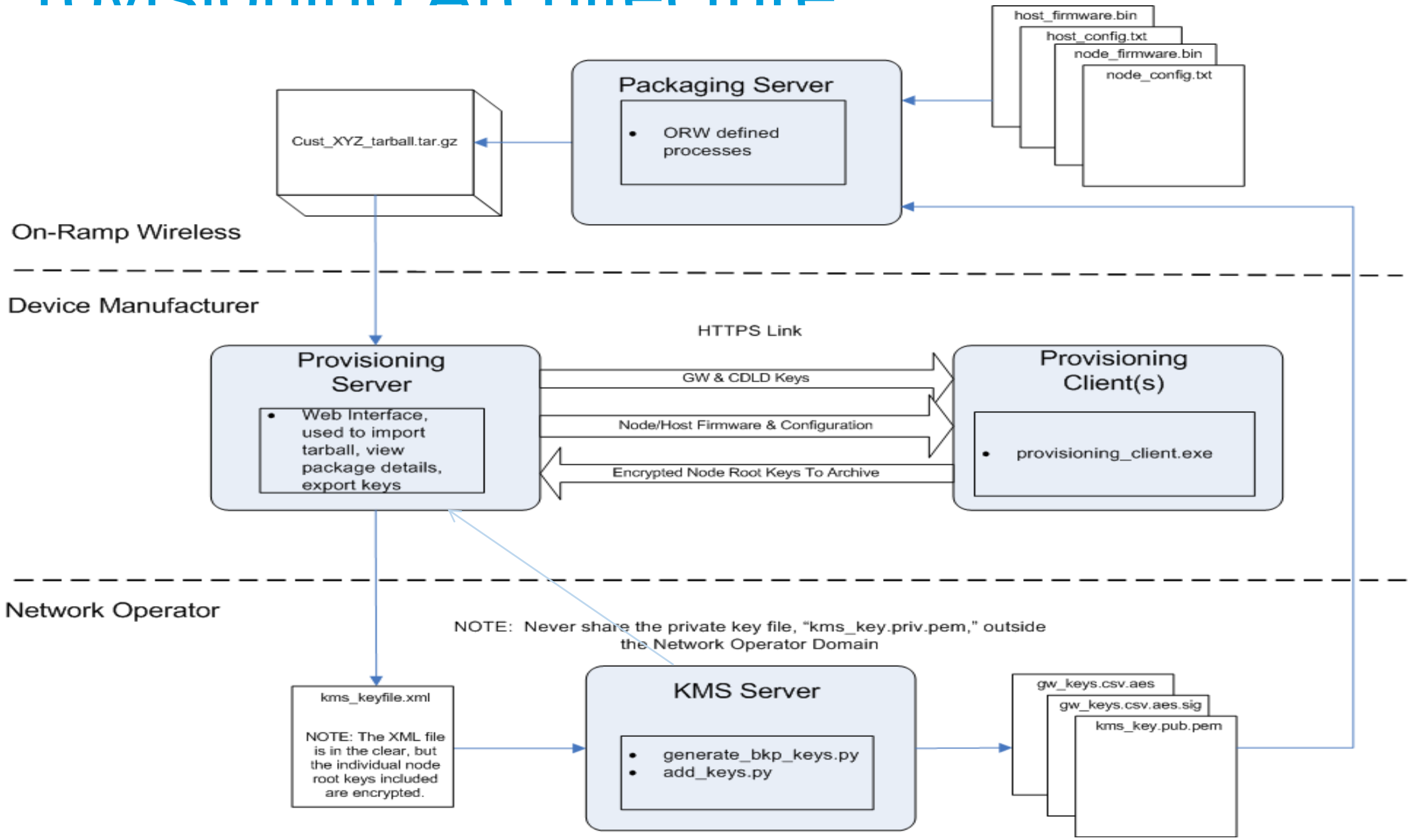
ULP Security attributes

- Attributes
  1. Mutual authentication
     - For a modem to join the network
  2. Message integrity and replay protection
     - At the message level
  3. Message confidentiality
     - At the message fragment level
  4. Limited Anonymity
     - At the modem level
  5. Authentic firmware upgrade
     - At the modem/host level
  6. Secure Multicast
     - At the modem/host level

Security algorithms

- Depend on symmetric key mechanisms
  - TDES and AES, NIST approved for until 2030 or beyond
  - Better option given star topology, low bandwidth, low power characteristics of ULP network
  - No OTA key exchange
  - Key material changed as dictated by the network
- What about security for other networks such as mesh?
  - Is more complicated

Provisioning Architecture



Security Requirements

- The security solution shall ensure privacy of user payloads over the entire network.
- The security solution shall ensure that unauthorized data is dropped in the network without being delivered to the application.
- The security solution shall ensure that replayed data is dropped in the network without being delivered to the applications.
- The security solution shall authenticate all nodes before allowing the nodes to join the network.
- The security solution shall ensure that only authenticated nodes can send/receive data successfully from the network.
- The security solution shall ensure the keys are updated based on system policies without any OTA key exchange.
- The security solution shall be designed for networks containing low bandwidth links with power constrained end devices.
- The security solution shall use NIST recommended security mechanisms.

Compliance with security requirements

The security solution shall …

1. … ensure privacy of user payloads over the entire network.
   - ORW compliance: MAC PDU payloads encrypted using TDES at AP/Node, AP- GW packets transmitted over secure tunnels, AP and GW in trusted zone.
2. … ensure that unauthorized data is dropped in the network without being delivered to the application.
   - ORW compliance: SDU CMAC (AES based) keyed hash mechanism, GW in trusted zone
3. … ensure that replayed data is dropped in the network without being delivered to the applications.
   - ORW compliance: SDU CMAC (AES based) keyed hash and SDU counter, GW in trusted zone
4. … authenticate all nodes before allowing the nodes to join the network.
   - ORW compliance: Node authentication based on AES and shared secrets between Node and the GW

Compliance with security requirements

The security solution shall …

1. … ensure that only authenticated nodes can send/receive data successfully from the network.
   - ORW compliance: GW sends and processes data only from authenticated nodes.
2. … ensure the keys are updated based on system policies without any OTA key exchange.
   - ORW compliance: GW can instruct the nodes to update the keys based on system policies
3. … be designed for networks containing low bandwidth links with power constrained end devices.
   - ORW compliance: Proposed solution requires minimal bandwidth overhead (2 PDUs per SDU) and leverages hardware implementations of TDES and AES on the node
4. … use NIST recommended security mechanisms.
   - ORW compliance: Solution based on AES-128, TDES, Key derivation functions, Pseudo random functions all based on NIST recommendations.

BACKUP SLIDES

Algorithm Lifetimes – NIST Recommendation

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[5] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: k=3072	Min.: f=256

NIST – Comparing Various Algorithms

A.1 Comparable Algorithm Key Size Strengths

This table is Table 2 in Part 1 of SP 800-57.

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA[1]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

NIST Integrity Protection Recommendation

Table 10: Message Authentication Code Transitions

MAC Algorithm	New Validations	Already Validated Implementations
HMAC	Any approved hash function Key lengths ≥ 80 bits and < 112 bits approved through 2010 only Key lengths ≥ 112 bits approved	Any approved hash function Key lengths ≥ 80 bits and < 112 bits approved through 2010 only Key lengths ≥ 112 bits approved *beyond 2010*
CMAC	Two-key Triple DES approved through 2010 only AES and Three-key Triple DES approved	Two-key Triple DES approved through 2010 only AES and Three-key Triple DES approved *beyond 2010*

NIST Encryption Algorithm Recommendation

DRAFT SP 800-131 **January 2010**

Table 1: Encryption Transitions

Encryption Algorithm	New Validations	Already Validated Implementations
Two-key Triple DES	Approved through 2010 only	Approved through 2010 only
Three-key Triple DES	Approved	Approved *beyond 2010*
SKIPJACK	Approved through 2010 only	Approved through 2010 only
AES-128	Approved	Approved *beyond 2010*
AES-192	Approved	Approved *beyond 2010*
AES-256	Approved	Approved *beyond 2010*