

S/WAN Toolkit

A Technical Overview

Roy Pereira

Senior Software Designer

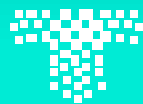


The S/WAN Initiative

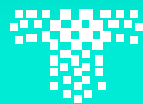
IPSec Interoperability

What is S/WAN ?

- Initiative from RSA
- Based on IETF IPsec
- Promote multi-vendor virtual private networks (VPNs) among firewall and TCP/IP vendors
- To make recommendations and additions to IPSec



more stuff about S/WAN



TIMESTEP

Copyright 1996 TimeStep Corporation. All rights reserved.

Who's Involved ?

10 Vendors Interoperate!



TIMESTEP

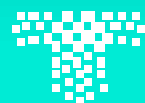
Check Point

Software Technologies Ltd.

tis



Morning Star Technologies



TIMESTEP

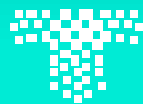
Copyright 1996 TimeStep Corporation. All rights reserved.

IETF IPSec

Security Standards for IP Network-Layer

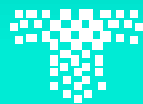
Why Network (IP) Layer?

- **Transparent to applications**
- **Independent of Networking topologies**
- **Limited or No User Impact**
- **Station-to-Station Security**

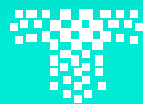
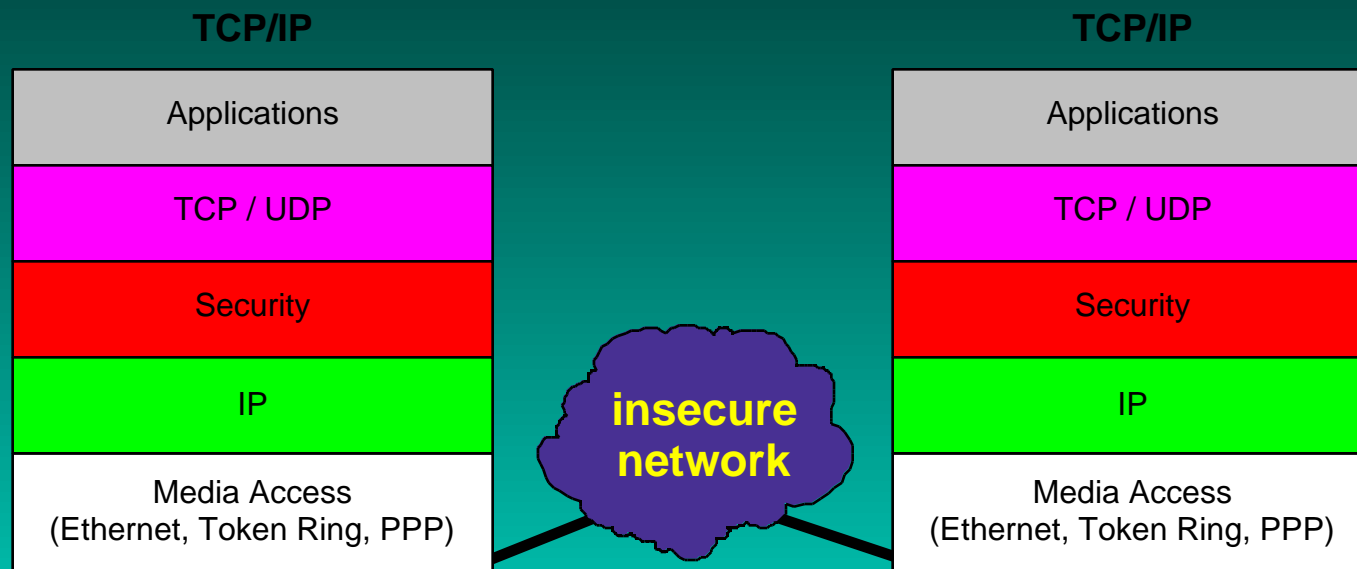


IPSec Security Architecture

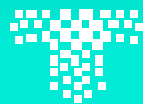
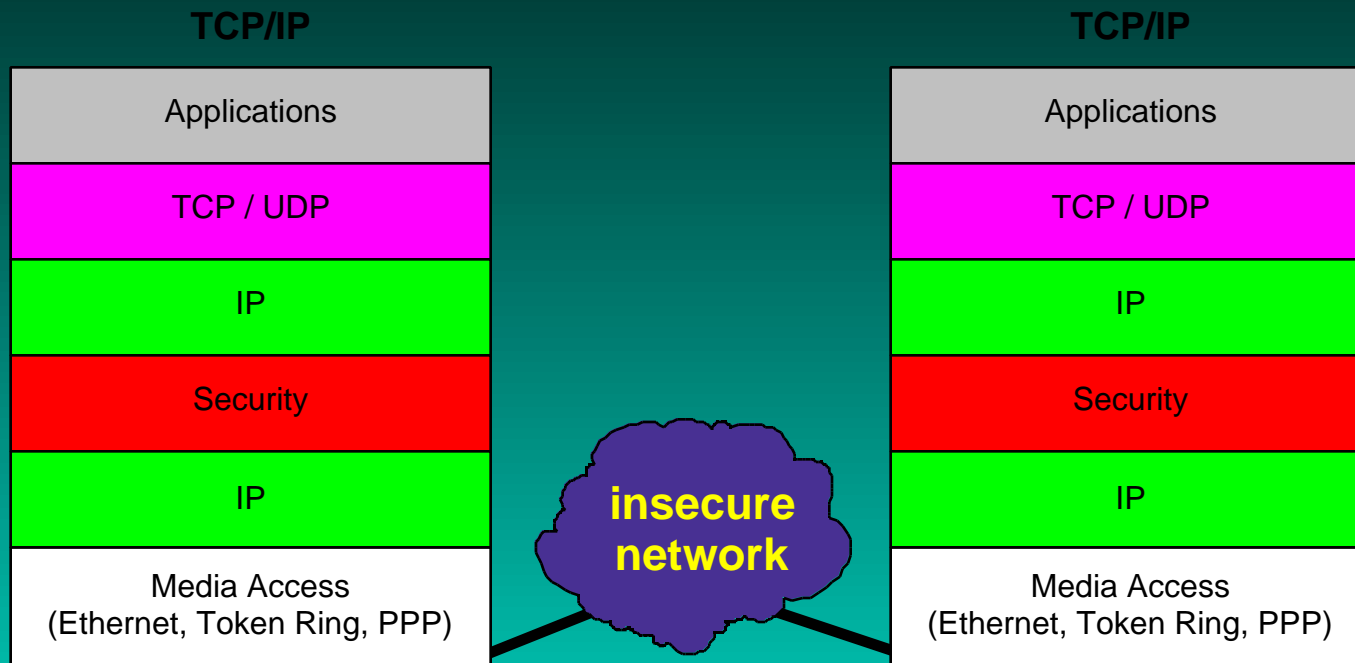
- **Overall Architecture (RFC 1825)**
 - Sets out high-level goals and guidelines
 - Key negotiation and authentication
 - Data confidentiality / Data Integrity
- **Authentication Header (RFC 1826)**
 - General framework for integrity mechanisms
- **Encapsulating Security Payload (RFC 1827)**
 - General framework for confidentiality mechanisms
- **Key Exchange Protocol (ISAKMP draft)**



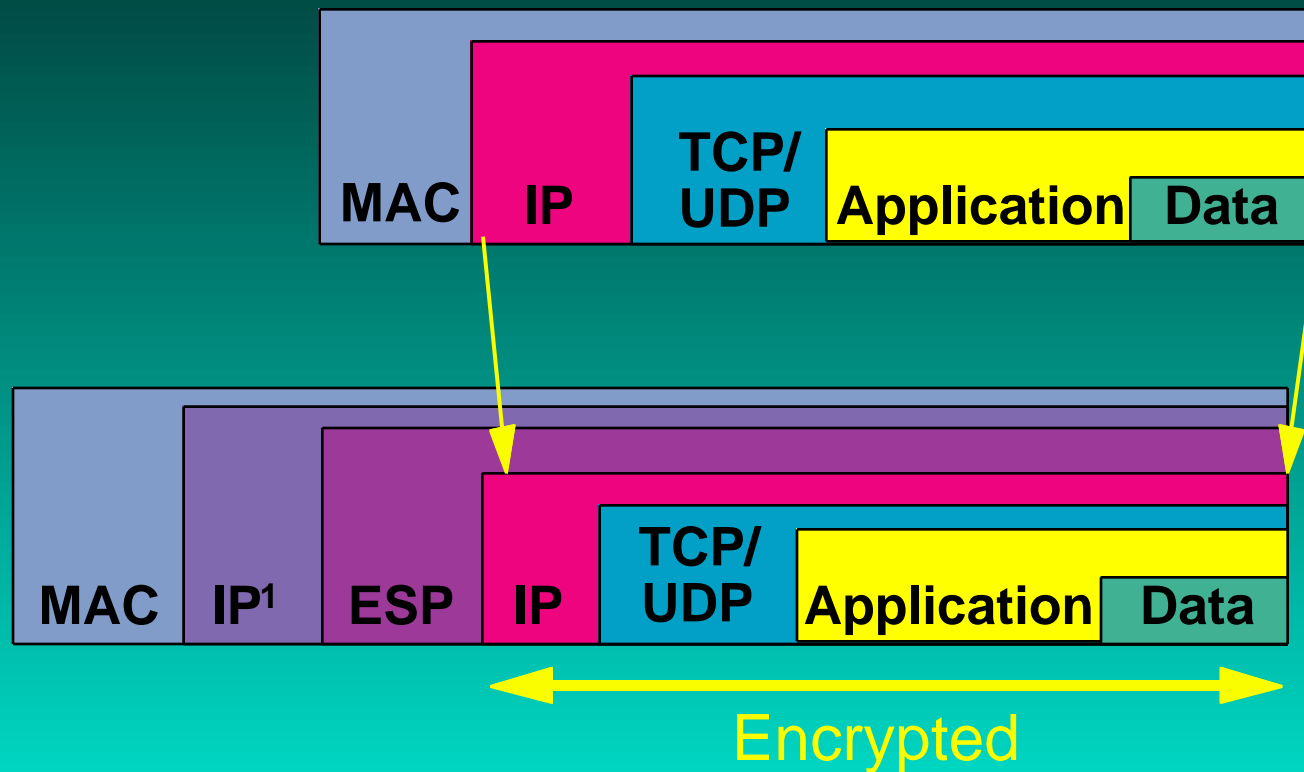
IPSec Transport Mode



IPSec Tunnel Mode

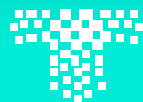


Encapsulating Security Payload (ESP Tunneling Mode)



ISAKMP & Oakley

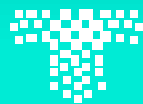
- **ISAKMP: Internet Security Association and Key Management Protocol**
 - defines protocol structures
- **Oakley Key Exchange Protocol**
 - defines how to combine ISAKMP structures in a handshaking mechanism



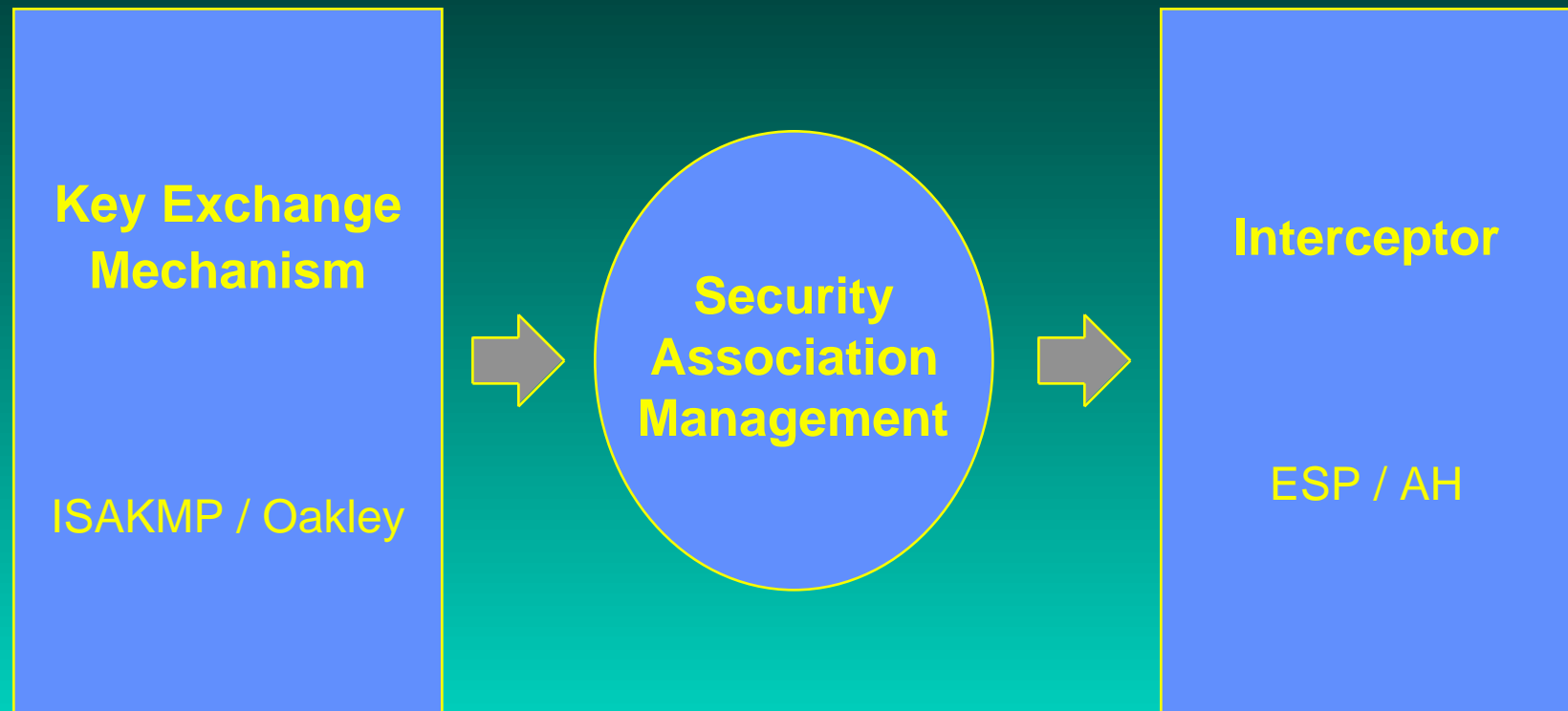
S/WAN Tool-kit

Overview

- **Portable across platforms and Operating Systems**
- **Completely in C++**
- **Extensive use of inheritance and polymorphism**
- **High level abstraction of IPSec protocols**



S/WAN Tool-kit Sections



S/WAN Tool-kit Sections

ISAKMP / Oakley

ADD ()
MODIFY ()
DELETE ()

Security
Association
Management

BUILD ()
PARSE ()

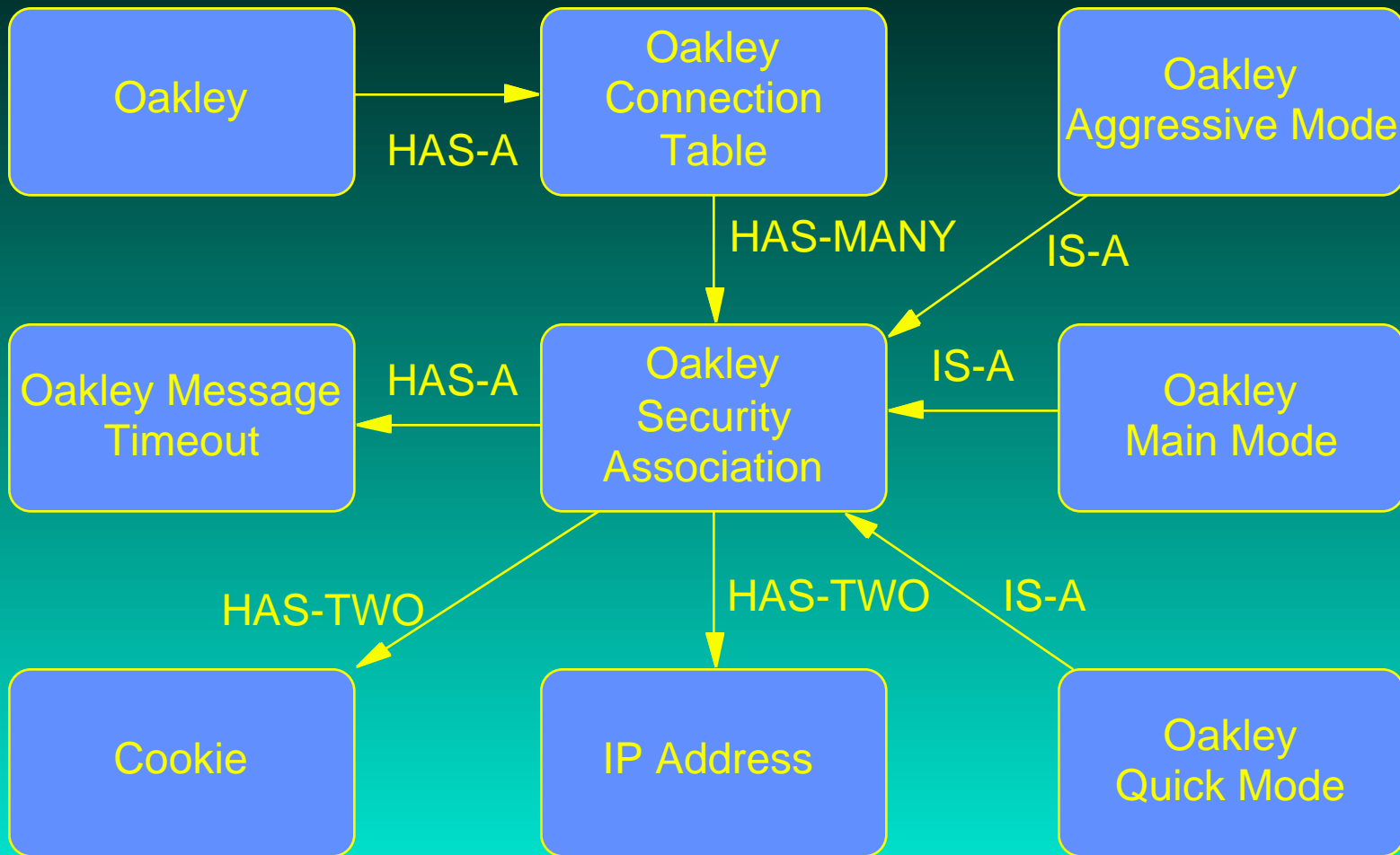
ESP / AH



TIMESTEP

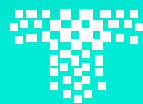
Copyright 1996 TimeStep Corporation. All rights reserved.

Oakley Class Overview



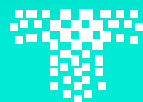
Oakley Main Mode

- **Negotiate policy under which to protect subsequent communication**
- **Exchange Diffie-Hellman public values and any ancillary information necessary to complete the exchange**
- **Authenticate the Diffie-Hellman exchange**



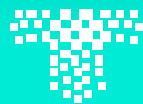
Oakley Main Mode Exchange

Initiator		Responder
HDR, SA	→→	
	←←	HDR, SA
HDR, KE, NONCE	→→	
	←←	HDR, KE, NONCE
HDR*, ID, SIG [,CERT]	→→	
	←←	HDR*, ID, SIG [,CERT]



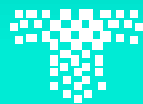
Oakley Quick Mode

- Only used when an existing ISAKMP Security Association has been established
- Mainly used to establish ESP and AH Security Associations



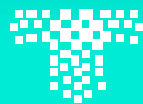
Oakley Quick Mode Exchange

Initiator	Responder
HDR*, HASH ¹ , SA, NONCE [,KE] [,ID]	→→
←←	HDR*, HASH ² , SA, NONCE [,KE] [,ID]
HDR*, HASH ³	→→



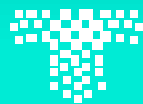
Oakley Aggressive Mode

- Can be used instead of Main Mode
- Does not provide identity protection
- Faster than Main Mode

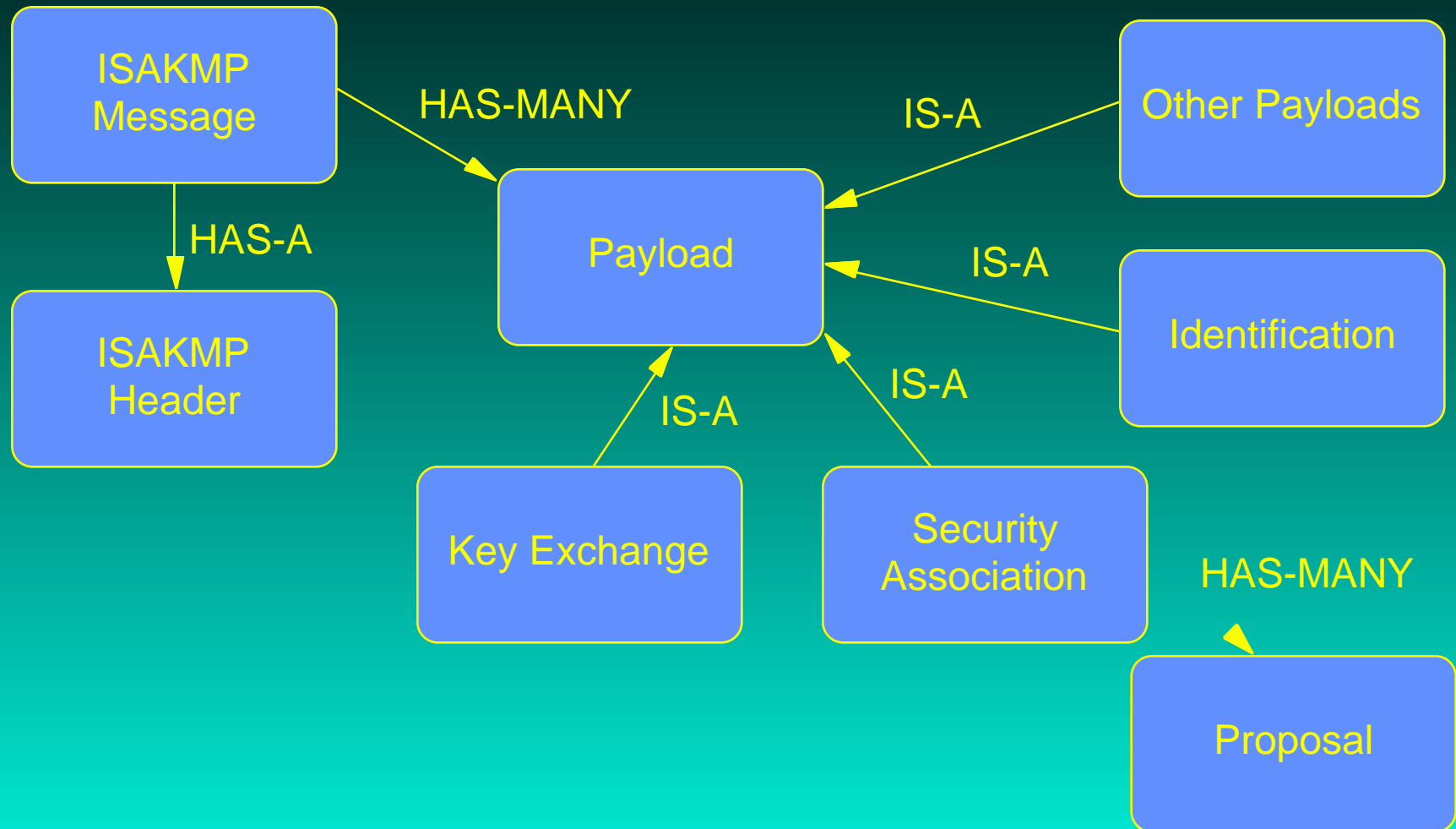


Oakley Aggressive Mode Exchange

Initiator	Responder
HDR, SA, KE, NONCE, ID	→→
←←	HDR, SA, KE, NONCE, ID, SIG [,CERT]
HDR, SIG [,CERT]	→→

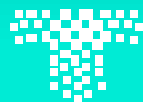


ISAKMP Class Overview



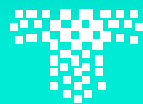
ISAKMP Header

- Initiator's Cookie
- Responder's Cookie
- Next Payload Type
- Version [1]
- Exchange Mode [Main, Quick, Aggressive]
- Flags [Encryption, Collate]
- Length



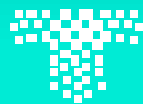
ISAKMP Payloads

- **Payloads Types include:**
 - Security Association (SA)
 - Key Exchange (KE)
 - Identification (ID)
 - Signature (SIG)
 - Nonce/Random (NONCE)
 - Certificates (CERT)
 - Hash (HASH)



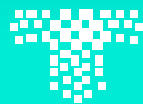
ISAKMP Payloads (cont)

- **ISAKMP Messages:**
 - Notify
 - Modify
 - Delete
- **All Payload types contain:**
 - Next Payload
 - Payload Length



ISAKMP Security Association

- **Situation**
 - Identity
 - Secrecy
 - Integrity
- **Proposal**
 - Protocol
 - Transform
 - Transform Attributes



Roy Pereira

rpereira@timestep.com

(613) 599-3610 x4808

TimeStep Corporation

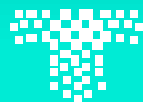
<http://www.timestep.com>

362 Terry Fox Drive

Kanata, Ontario, K2K 2P5

Phone: (613) 599-3610

FAX: (613) 599-3617



TIMESTEP

Copyright 1996 TimeStep Corporation. All rights reserved.