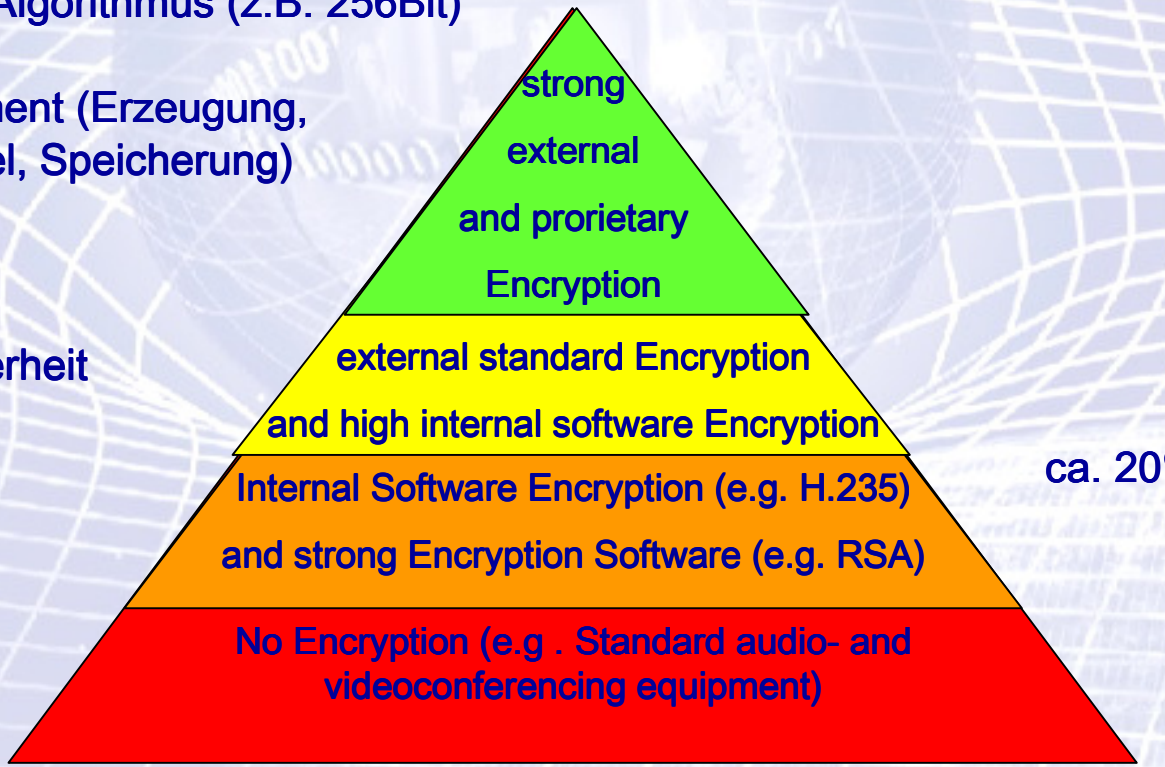
# Definition von Verschlüsselung

Welche Faktoren bestimmen die Qualität einer sicheren Kommunikationsverschlüsselung?

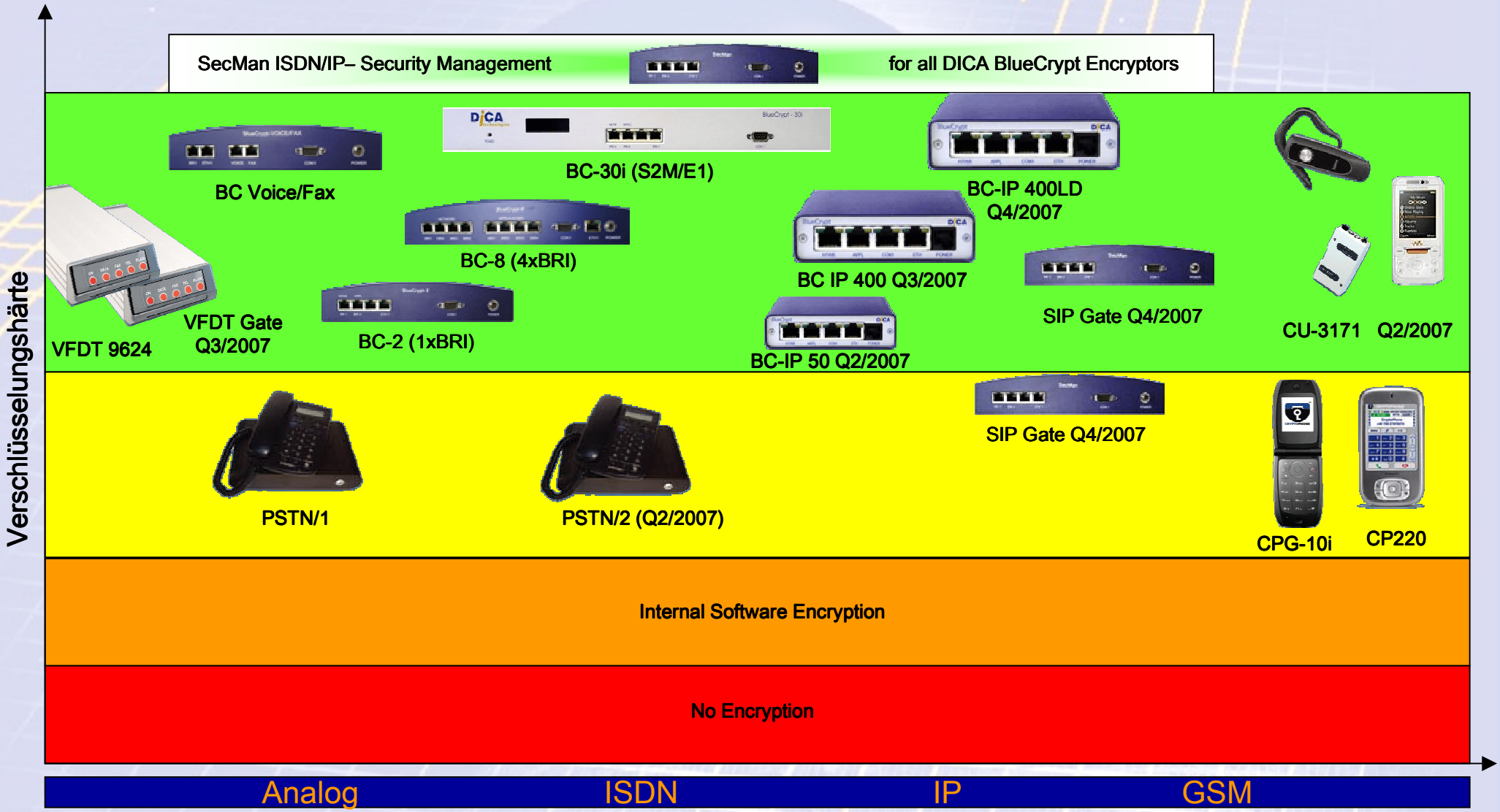
- Verschlüsselungsalgorithmus (AES, 3DES, Twofish etc) — ca. 15%
- Schlüsseltiefe des Algorithmus (z.B. 256Bit) — ca. 10%
- Schlüsselmanagement (Erzeugung, Austausch, Wechsel, Speicherung) — ca. 30%
- Authentifizierung — ca. 20%
- physikalische Sicherheit — ca. 5%
- Sicherheitskonzept — ca. 20%




Ist ihre Kommunikationsverschlüsselung wirklich sicher ?

DiCA technologies - *security made simple*

# DICA Produkt Portfolio




DICA technologies - *security made simple*

# BlueCrypt Produktmerkmale

Starke Verschlüsselung für:

- Analog: Sprache und Fax
- ISDN: Sprache, Daten, Video und Netzwerk
- IP: Sprache, Daten, Video und Netzwerk

Höchste Sicherheit durch:

- 3DES Algorithmus mit 192 Bit, IDEA Algorithmus mit 128 Bit und AES mit 256 Bit Schlüssellänge (IP)
- Mehrstufiges Schlüsselmanagement
- Hardware-basierte externe Verschlüsselung mit Cryptochip
- Transparenz zu Anwendung und Netzwerk
- Restriktive Authentifikation für hochsichere Verbindungen
- Erzeugen , Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor
- SecMan Sicherheitsmanagement für die zentrale Verwaltung

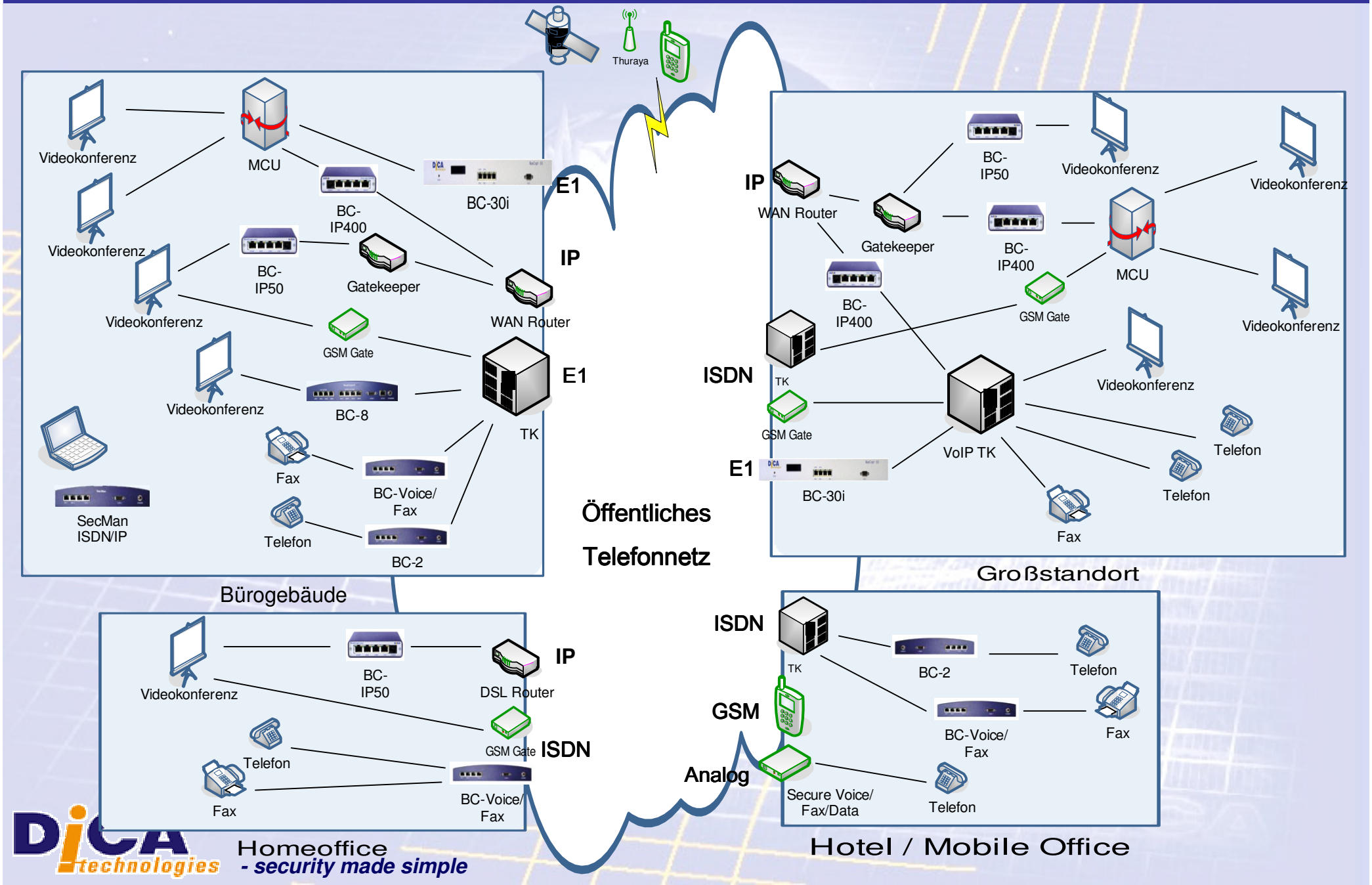
Benutzerfreundlichkeit durch:

- Plug & Play – einfache Integration in der IT- und TK-Architektur
- Automatische Erkennung einer Anforderung zur Verschlüsselung
- Weltweite Verwendbarkeit und niedrige Folgekosten
- SecMan Sicherheitsmanagement für die zentrale Verwaltung
- Verschlüsselung in Echtzeit

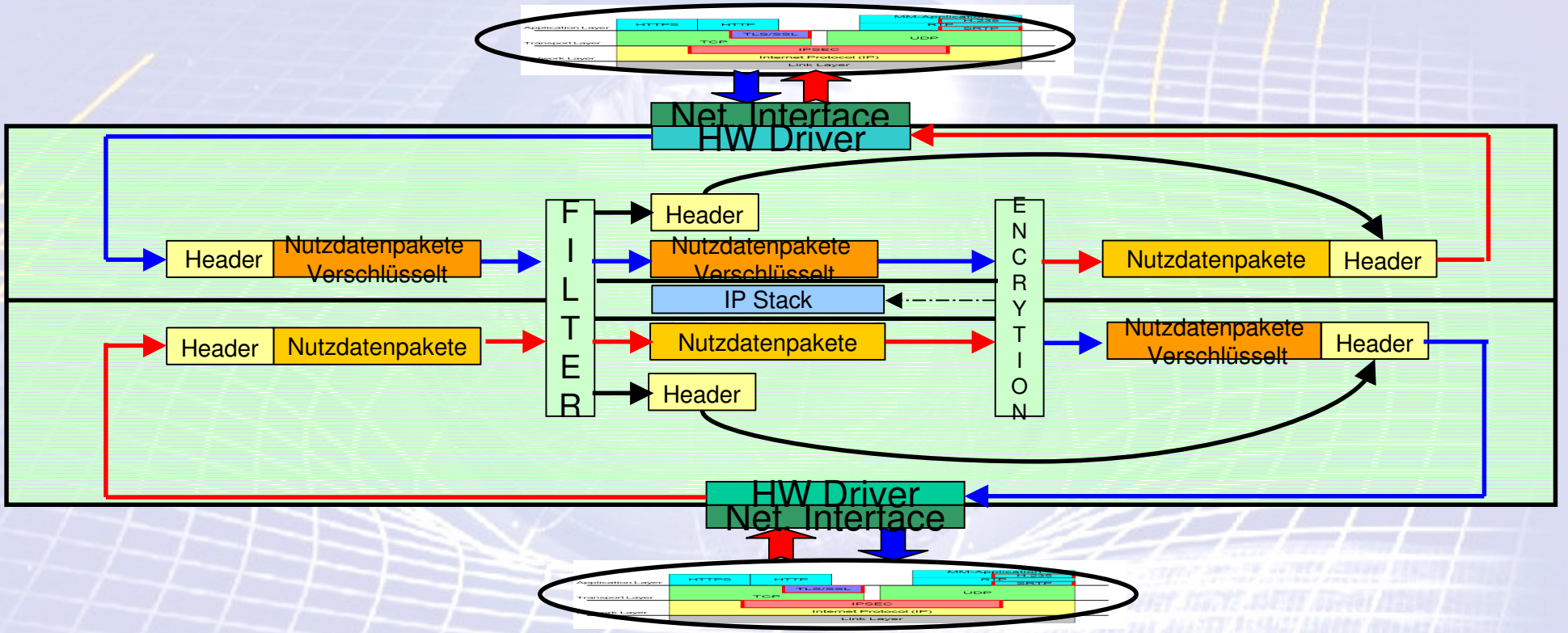
Zuverlässigkeit durch:

- DICA‘s Herstellungsverfahren nach ISO 9001

# Kommunikationsstruktur - Verschlüsselung DICA + Partner



# BlueCrypt IP-Verschlüsselungskonzept



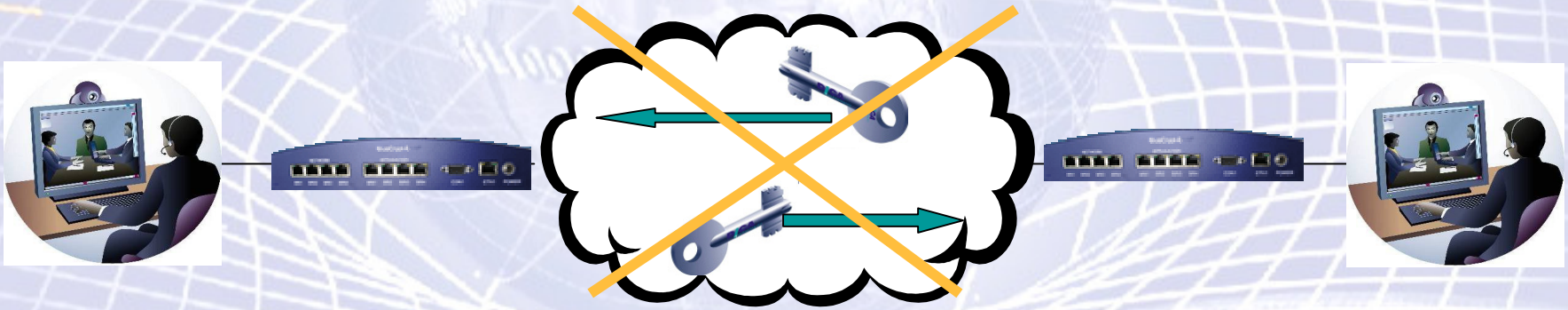

- keine feste IP Adresse
- keine feste Mac Adresse

→ Unsichtbarkeit der BlueCrypt Geräte im Netzwerk (Netztransparenz)

DiCA technologies *- security made simple*

# BlueCrypt-Schlüsselmanagement

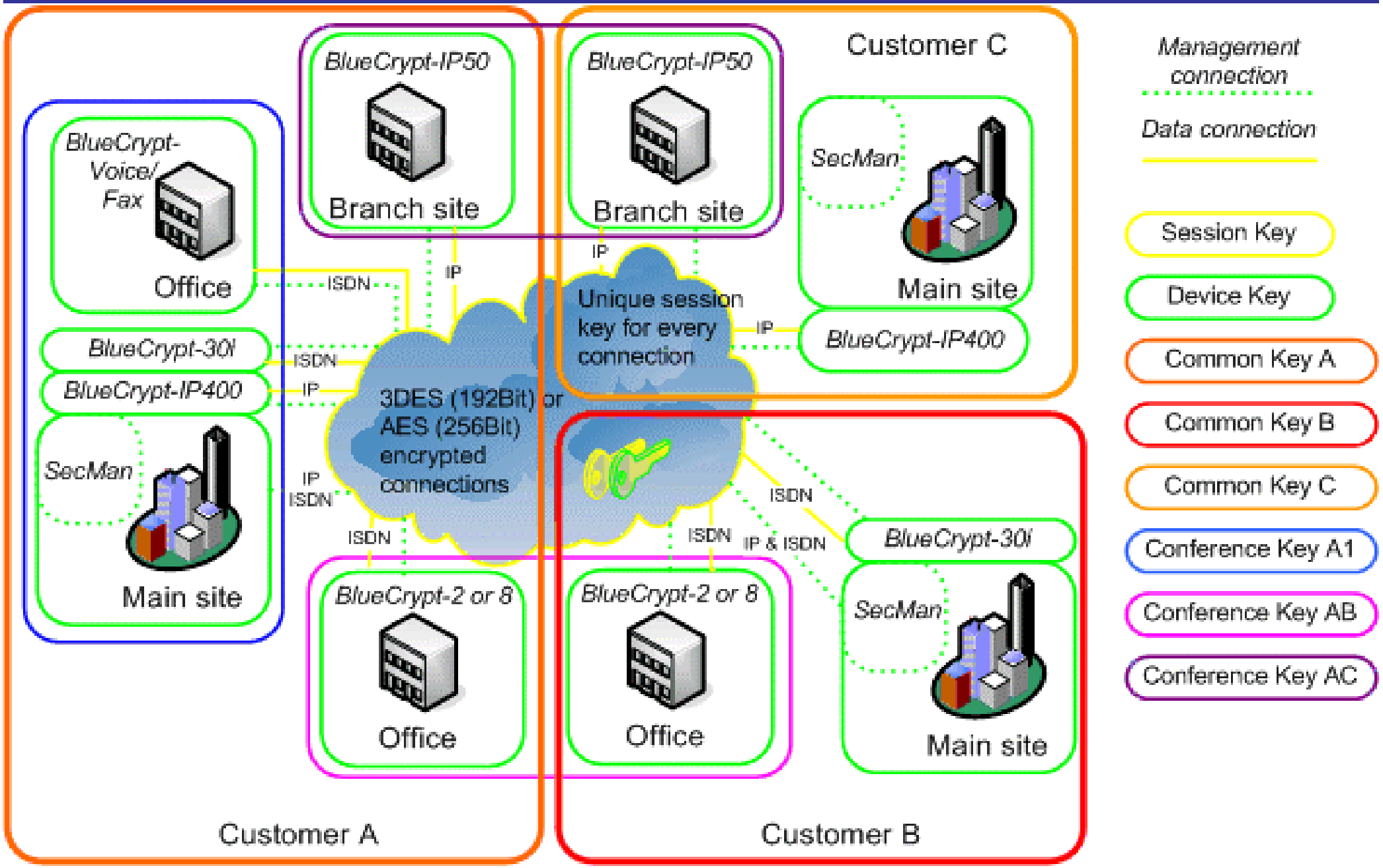
Nicht nur verschlüsselt, sondern auch sicher!



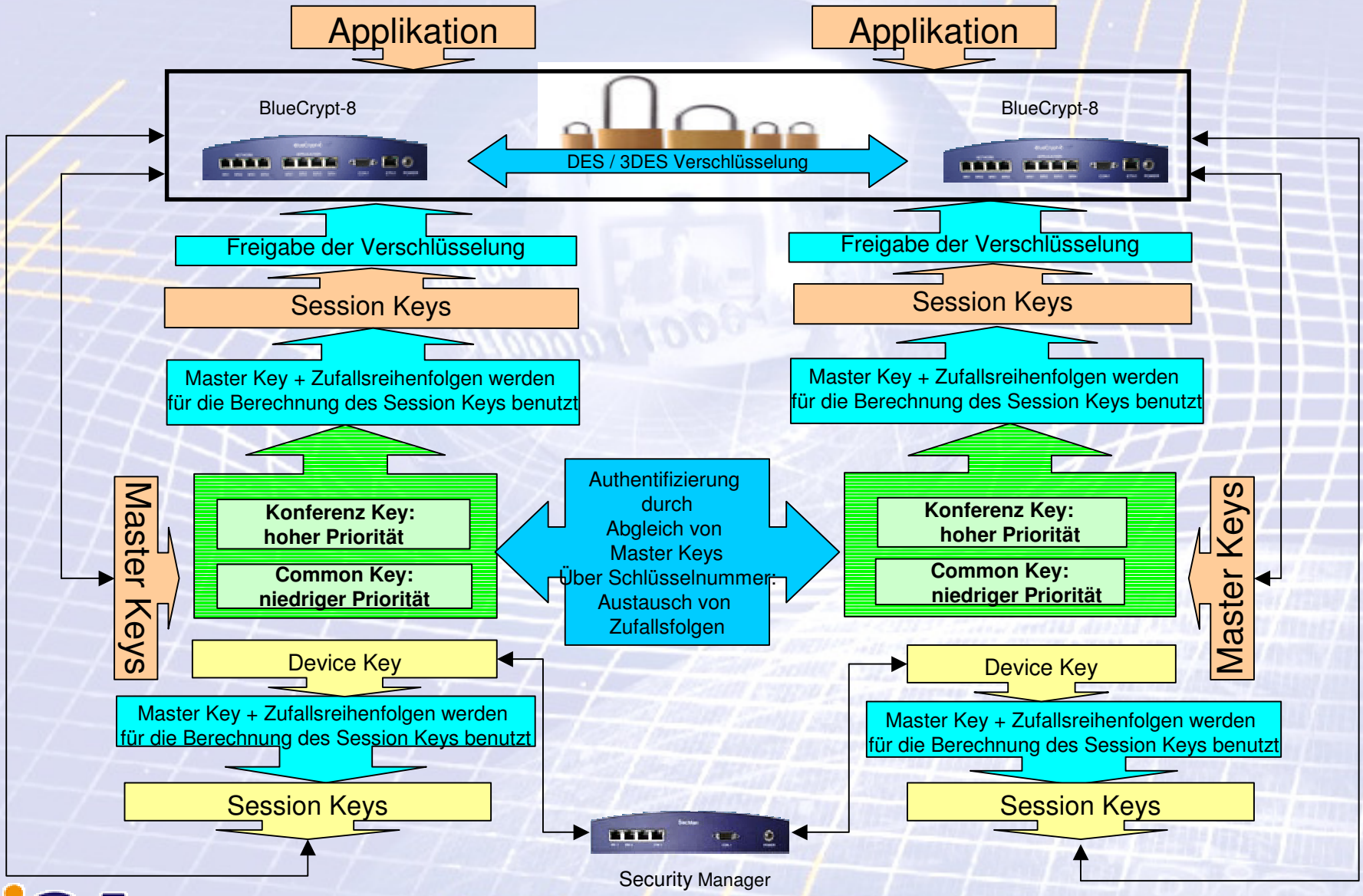
Die DICA-Technologie benötigt keinen Schlüsselaustausch!

DiCA technologies - *security made simple*

# Schema des Schlüsselmanagements



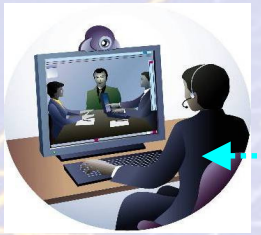
# Funktionsprinzip des Schlüsselmanagements



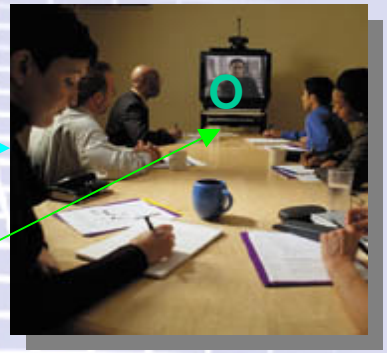

DiCA technologies - *security made simple*

# BlueCrypt IP vs. H.235

VC mit H.235




VC mit H.235



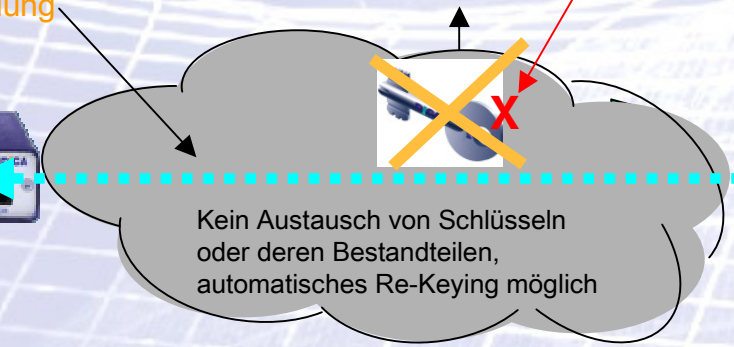
Verschlüsselte H.235 VC-Verbindung

Ungesicherter bzw. wenig gesicherter Management-Port

Internet

VC mit BlueCrypt

Verschlüsselte DICA VC-Verbindung




VC mit BlueCrypt

Management-Port ist verschlüsselt

DICA technologies - *security made simple*

# BlueCrypt IP vs. H.235 (1)

- Schlüssellänge 192Bit / 256Bit vs. 128Bit
  - Angriff ist in Potenzen aufwendiger (abhängig vom Schlüsselmanagement)
- Externe Hardwareverschlüsselung vs. Softwareverschlüsselung
  - Zukunftssichere Infrastruktur für HD Videokonferenz größer 768 Kbit/s Bandbreite
  - Höhere Performance und Sicherheit gegenüber in Anwendung integrierter softwarebasierter Verschlüsselung
- Transparent zur Anwendung und zum Netzwerk vs. voller Adressierbarkeit
  - Firewall Traversal als Anwendungsprotokoll (z.B. SIP)
  - Problemlose Integration in Netzwerkstruktur ohne Änderung von IP Adresskonzepten
  - BlueCrypt funktioniert ohne eigene IP- und MAC Adresse, praktisch nicht adressierbar
- Patentiertes DICA Schlüsselmanagement vs. online Schlüsselaustausch (IKE)
  - jeweils ein einmalig gültiger Session Key pro Übertragungsrichtung
  - unterschiedliche Master Keys und automatisches Rekeying verhindern Kompromittierung des Schlüsselmaterials
  - Erzeugen , Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor
  - absolut zufällig erzeugte Schlüssel durch patentierten Zufallsgenerator

# BlueCrypt IP vs. H.235 (2)

- Zentral gesteuerte Verschlüsselung von IP, ISDN, GSM und Analogverbindungen vs. nur IP
  - Durchgängige Verschlüsselung der Kommunikation über alle Medien
  - Verschlüsselungslösung für weitere weltweite IP basierte Kommunikation
  - rapid return on investment (ROI) und **low** total cost of ownership (**TCO**)
- Verschlüsselung der Nutzdaten (Payload encryption)
  - Volle Bandbreite steht für die Anwendungen zur Verfügung
  - Unverschlüsselte Adress Header – vereinfachtes Firewall Traversal
- Restriktive Authentisierung via Key Management vs. fehlender Authentisierung
  - jedes H.235 konforme VC Gerät kann potenziell an verschlüsselter Konferenz teilnehmen
  - BlueCrypt Verschlüsselungsmodus für restriktive Authentifikation via Master Key
  - keine individuelle Authentisierung, auch nicht durch PSK oder Zertifikate

# BlueCrypt IP vs. IPSec VPN (1)

- Verschlüsselung der Nutzdaten (Payload encryption)
  - Volle Bandbreite für Anwendungen, unverschlüsselte Adress Header für Firewall
  - Hardware-basierte Verschlüsselung mit Cryptochip, Erzeugen, Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor
- Transparent zur Anwendung und zum Netzwerk vs. voller Adressierbarkeit
  - Firewall Traversal als Anwendungsprotokoll (z.B. SIP)
  - Problemlose Integration in Netzwerkstruktur ohne Änderung von IP Adresskonzepten
  - BlueCrypt funktioniert ohne eigene IP- und MAC Adresse, praktisch nicht adressierbar
- Patentiertes DICA Schlüsselmanagement vs. online Schlüsselaustausch (IKE)
  - unterschiedliche Master Keys und automatisches Rekeying verhindern Kompromittierung des Schlüsselmaterials
  - Erzeugen , Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor
  - jeweils ein einmalig gültiger Session Key pro Übertragungsrichtung
  - absolut zufällig erzeugte Schlüssel durch patentierten Zufallsgenerator

# BlueCrypt IP vs. IPSec VPN (2)

- Authentisierung Key Management vs. Zertifikate / pre shared Keys
  - deutlich geringerer Aufwand und Kosten, keine Folgekosten für Zertifikatsverlängerung
  - keine trusted Zertifikatsinfrastruktur notwendig
  - unabhängig von stationärer Sicherheitsreferenz (Zertifikatsserver)
- Einfache Implementierung
  - Vermeidung von Sicherheitsschwachstellen durch fehlerhafte Implementierung
  - nach kurzem Training kann sicheres weltumfassendes Netz administriert werden
  - Keine Probleme mit Network Adress Translation (NAT), da nur Nutzdaten verschlüsselt
  - Firewall Traversal als Anwendungsprotokoll (z.B. SIP)
- Keine beständige Beseitigung von softwarebasierten Schwachstellen
  - BlueCrypt-IP verschlüsselt ab Layer 2, IPSec Implementierungen dagegen im Layer 3 und ist daher leichter angreifbar
- Teilweise softwarebasierte IPSec Verschlüsselungslösungen in Endgeräten
  - BlueCrypt-IP ist eine externe hardwaregestützte End to End Verschlüsselung
  - kein durchgängiges Sicherheitslevel bei Verbindung starker hardware-basierender IPSec Implemtierungen mit einfach software-basierten Lösungen

# BlueCrypt IP vs. SSL VPN (1)

- SSL im eigentlichen Sinne kein Tunnelprotokoll, anwendungsspezifische Umsetzung
  - wenn Applikation nicht per Browser bedienbar, dann müssen Daten immer auf den Layer 7 des OSI-Modelles durchgereicht und ggf. emuliert werden, verbunden mit Performanceeinbußen und hohem Fehlerrisiko der Umsetzung
- Diverse Probleme die mit der softwarebasierten Implementierung bzw. Nutzung von Java und ActiveX Applets und der Verwendung von Browsern einhergehen
  - XSS Angriffe, Heraufladen von Malware, Ausspähen des Cache, unberechtigte Nutzung nicht geschlossener Sitzungen, Angriffe auf bereitgestellte Applikationen etc.
- Verschlüsselung der Nutzdaten (Payload encryption)
  - Volle Bandbreite für Anwendungen, unverschlüsselte Adress Header für Firewall
  - Hardware-basierte Verschlüsselung mit Cryptochip, Erzeugen, Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor

# BlueCrypt IP vs. SSL VPN (2)

- Patentiertes DICA Schlüsselmanagement vs. online Schlüsselaustausch (IKE)
  - jeweils ein einmalig gültiger Session Key pro Übertragungsrichtung
  - unterschiedliche Master Keys und automatisches Rekeying verhindern Kompromittierung des Schlüsselmaterials
  - Erzeugen , Halten und Löschen des gesamten Schlüsselmaterials in versiegeltem Sicherheitsprozessor
  - absolut zufällig erzeugte Schlüssel durch patentierten Zufallsgenerator
- softwarebasierte VPN Verschlüsselungslösungen für Site to Site oder End to Site Anwendungen
  - BlueCrypt-IP ist sowohl als externe hardwaregestützte End to End als auch Site to Site Verschlüsselung bzw. End to Site verfügbar
- Authentisierung Key Management vs. Zertifikate / pre shared Keys
  - deutlich geringerer Aufwand und Kosten, keine Folgekosten für Zertifikatsverlängerung
  - keine trusted Zertifikatsinfrastruktur notwendig
  - unabhängig von stationärer Sicherheitsreferenz (Zertifikatsserver)

# BlueCrypt IP vs. MPLS

- MPLS Zugänge meist direkt an einen speziellen Provider weltweit gebunden, da MPLS Übergänge zwischen den Providern nicht existieren
  - BlueCrypt ist standortunabhängig, fest und mobil einsetzbar, weltweit
- MPLS Netzwerke selten für kleine Standorte und Homeoffice verfügbar
  - BlueCyrpt-Verschlüsselungsprodukte für alle Einsatzbereiche verfügbar
- MPLS Netzwerke aufgrund der Bandbreite und Architektur meist ohne Verschlüsselung
  - induviduelle und skalierbare Sicherheit nur mit BlueCrypt Produkten
- Vergleichsweise hohe monatliche Kosten für Nutzung bzw. Betrieb
  - geringe laufenden Kosten oder Folgekosten mit BlueCrypt Produkten
- MPLS benötigt Übergänge in Netzwerkstrukturen (IPSEC VPN), damit keine durchgehende Sicherheit
  - höchste Sicherheit durch End to End Verschlüsselung mit BlueCrypt Produkten (evtl. als Ergänzung von MPLS Netzwerkanbindungen)

# Summary

- Bedrohungen und Angriffe nehmen immer mehr zu
- DICA BlueCrypt ist bereits Verschlüsselungsstandard für viele namhafte Kunden
- Viel sicherer bei gleichzeitig einfachster Handhabung im Vergleich zu derzeit am Markt eingesetzten Technologien bei niedrigsten Folgekosten
- Nur dedizierte Hardware kann die Kundenanforderungen nach Sicherheit, Einfachheit und Skalierbarkeit bieten
- Klare Strategie der Integration der verschiedenen Medien, umfassende Abdeckung der Kundenanforderungen
- Mehr als 16 Jahre Erfahrung auf dem Gebiet der Verschlüsselung
- Deutscher Hersteller mit weltweitem Vertrieb von externen Verschlüsselungssystemen