Military Grade Security for Video over IP

Jed Deame, CEO, Nextera Video

Nextera Video

VSF VIDEO SERVICES FORUM

Agenda

- Why Secure Video over IP?
- Security Primer
- NMOS Security
- Customer Case Study

Nextera Video

VSF VIDEO SERVICES FORUM

Why Secure Video over IP?

- High value content may require protection
- Keep unauthorized/unintended streams off air
- Hackers everywhere
- Threats INSIDE the facility

Nextera Video

VSF VIDEO SERVICES FORUM

3 Classes of Protection

1. Essence Encryption (Military, Mission Critical, etc.)
2. Control Encryption (NMOS)
3. Physical/Environmental Protection

Nextera Video

VSF VIDEO SERVICES FORUM

Security Primer

1. Cryptographic Security Standards
   - FIPS 140-2
   - NSA Suite B
2. Cryptographic Algorithms
   - Encryption Algorithms
   - Key Establishment
   - Digital Signatures
   - Secure Hash Algorithms (SHA)

Nextera Video

VSF VIDEO SERVICES FORUM

1. Cryptographic Security

FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

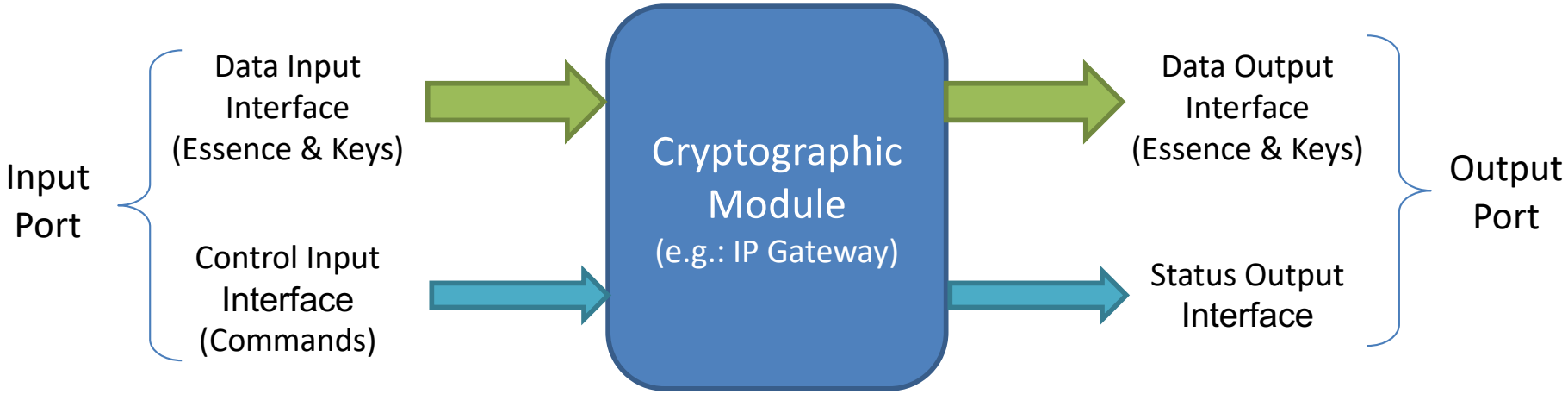
CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Nextera Video

VSF VIDEO SERVICES FORUM

FIPS 140-2 Ports & Interfaces



Nextera Video

VSF VIDEO SERVICES FORUM

Security Level 1 – Lowest

(Physically protected environments)

- Approved Cryptographic Algorithm & Key Management
- Standard Compute Platform, unvalidated OS
- No Physical Security

Nextera Video

VSF VIDEO SERVICES FORUM

Security Level 2

- Approved Cryptographic Algorithm & Key Management
- Standard Compute Platform
- Trusted OS (Tested)
  - meets Common Criteria (CC) Evaluation Assurance Level 2 (EAL2)
  - Referenced Protection Profiles (PP's)
- Tamper Evidence
- Identity or Role-based Authentication

Nextera Video

VSF VIDEO SERVICES FORUM

Security Level 3

- Approved Cryptographic Algorithm & Encrypted Keys
- Standard Compute Platform
- Trusted OS (Tested) – meets CC EAL3, Referenced PP's
- Tamper Response (zeroizes data)
- Identity-only based Authentication
- Plaintext Keys/passwords must be entered on separate ports
  - Physical or Logical Separation with a trusted path

Nextera Video

VSF VIDEO SERVICES FORUM

Security Level 4 – Highest

(Suitable for Physically Unprotected Environments)

- Approved Cryptographic Algorithm & Encrypted Keys
- Standard Compute Platform
- Trusted OS (Tested) – meets CC EAL4, Referenced PP's
- Tamper Response (zeroizes data and plaintext keys)
- Identity-only based Authentication
- Plaintext Keys/passwords must be entered on separate ports
- Protected for voltage and temperature extremes

Nextera Video

VSF VIDEO SERVICES FORUM

Crypto/Physical Security (FIPS 140-2)

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.

Nextera Video

VSF VIDEO SERVICES FORUM

FIPS 140-2 *cont.*

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Nextera Video

VSF VIDEO SERVICES FORUM

NSA Suite B Cryptography

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.

Nextera Video

VSF VIDEO SERVICES FORUM

Commercial National Security Algorithm Suite

(CNSA)

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity
AES-256	Confidentiality

Nextera Video

VSF VIDEO SERVICES FORUM

Security Primer

1. Cryptographic Security Standards
   - FIPS 140-2
   - NSA Suite B
2. Cryptographic Algorithms
   - Encryption Algorithms (AES)
   - Secure Hash Algorithms (SHA)
   - Key Establishment (ECDH)
   - Digital Signatures (DSA)

Nextera Video

VSF VIDEO SERVICES FORUM

Encryption Algorithms

- AES – Advanced Encryption Standard
  - Symmetric Key Algorithm
  - 128 bit block size, Key Sizes of 128, 192 and 256 bits
    - Plaintext -> Ciphertext
    - Key size specifies # transformation rounds (AES256 = 14 rounds)
  - CTR (Counter) Mode for low bandwidth traffic
  - GCM (Galois/Counter Mode) for high bandwidth traffic
  - Adopted by US Gov't and used worldwide
  - *NIST FIPS PUB 197 (2001)*

Nextera Video

VSF VIDEO SERVICES FORUM

Brute Force Attacks

- AES-128 (HDCP)
  - Requires 2^{128} -1 bit flips. The energy required is ~10^{18} joules, which is equivalent to consuming 30 gigawatts of power for one year, which is 262.7 TWh (more than 1% of the world energy production)

- AES-256
  - Fifty supercomputers that could check a billion billion (10^{18}) AES keys per second (if such a device could ever be made) would, in theory, require about 3×10^{51} years to exhaust the 256-bit key space

Nextera Video

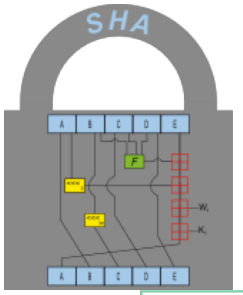
VSF VIDEO SERVICES FORUM

Secure Hash Algorithms

Mapping of arbitrary sized data to fixed size. Must be:

1. Deterministic
2. Quick to compute
3. Infeasible to generate a message from its hash value
4. A small change in message yields a large change in the digest
5. No two messages with the same hash value

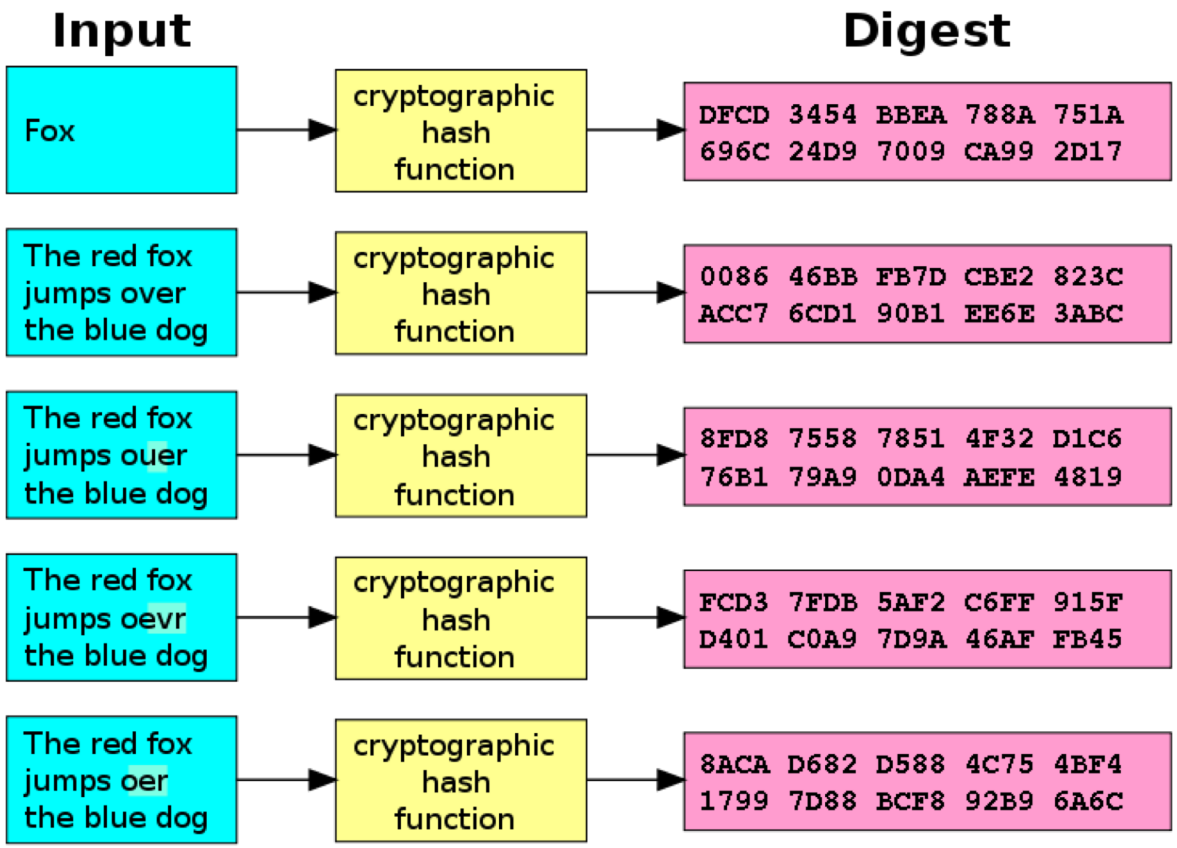
- Multiple rounds (up to 80) of AND, XOR, NOT, ROT
- *Published by NIST/FIPS PUB 180/202 (SHA 0/1/2/3 224-512)*



Nextera Video

VSF
VIDEO SERVICES FORUM

SHA Example



Nextera Video

VSF VIDEO SERVICES FORUM

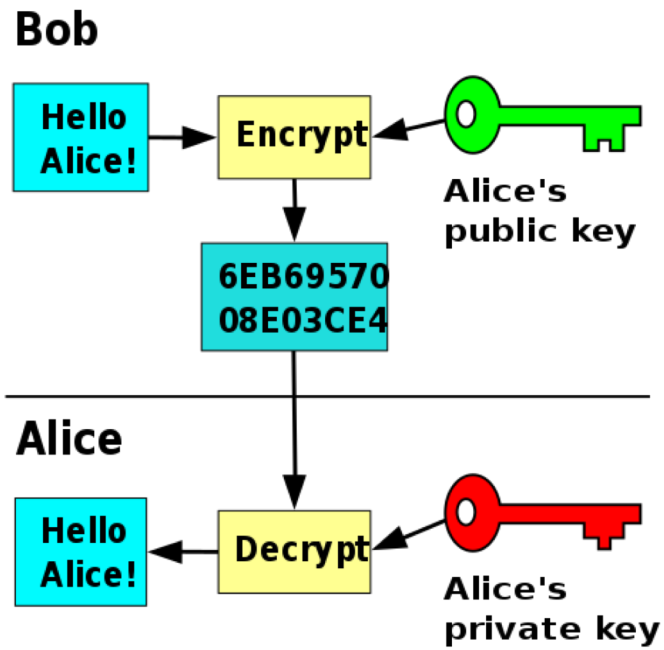
Key Establishment

1. Public Key Encryption
2. Digital Signatures
3. Public Key Infrastructure (PKI)

Nextera Video

VSF VIDEO SERVICES FORUM

Public Key Encryption



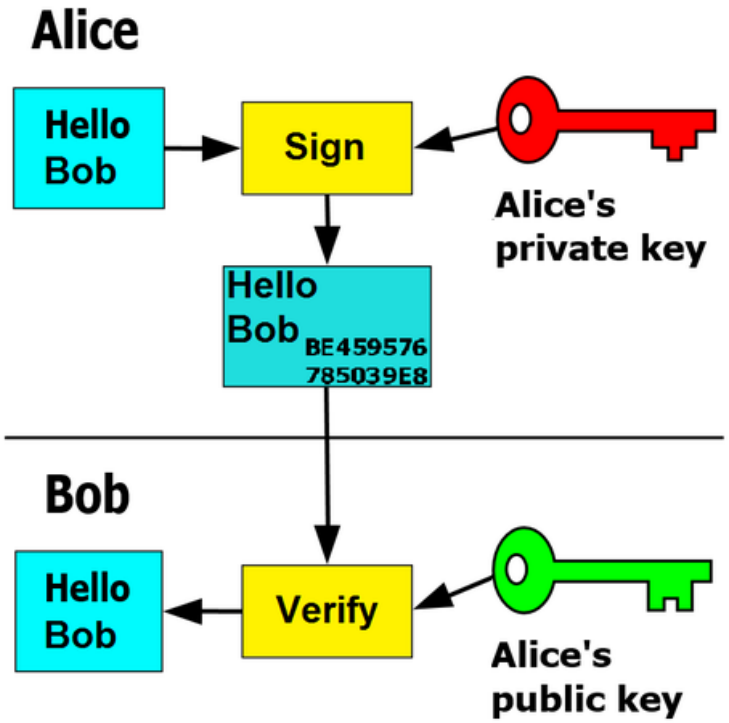
- Simple & Effective
- Subject to man-in-the middle attacks

Nextera Video

VSF VIDEO SERVICES FORUM

Digital Signatures

- A mathematical scheme for verifying the authenticity of digital messages



Nextera Video

VSF
VIDEO SERVICES FORUM

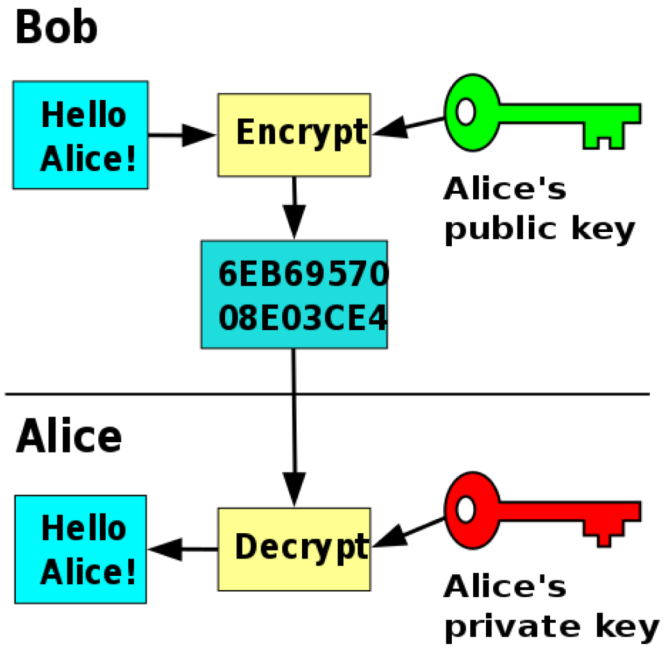
Digital Signature Algorithm (DSA)

- Gov't Standard for Digital Signatures *(NIST FIPS 186-4)*
  1. Specify Hash Function (SHA)
  2. Specify Key Length L&N (3072, 256)
  3. Choose prime numbers p, q, & g that may be shared
  4. Randomly choose a secret private key
  5. Compute a Public Key
  6. Sign the Key by hashing a random number (PS3)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
  - OpenSSL

Nextera Video

VSF VIDEO SERVICES FORUM

How to transfer Encryption Keys?



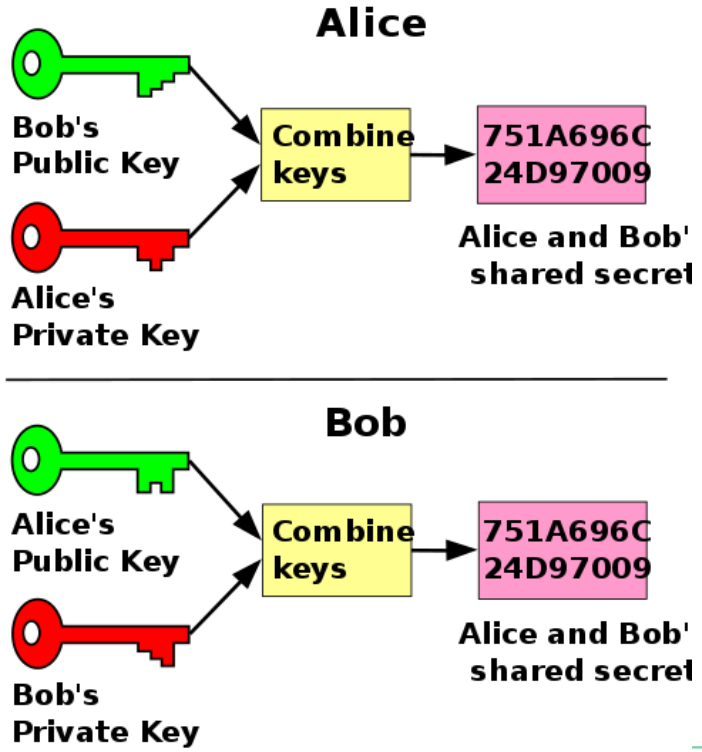
- Paper key list via Trusted Courier
- What if we could jointly establish a secret key over an insecure channel?

Nextera Video

VSF VIDEO SERVICES FORUM

Key Agreement

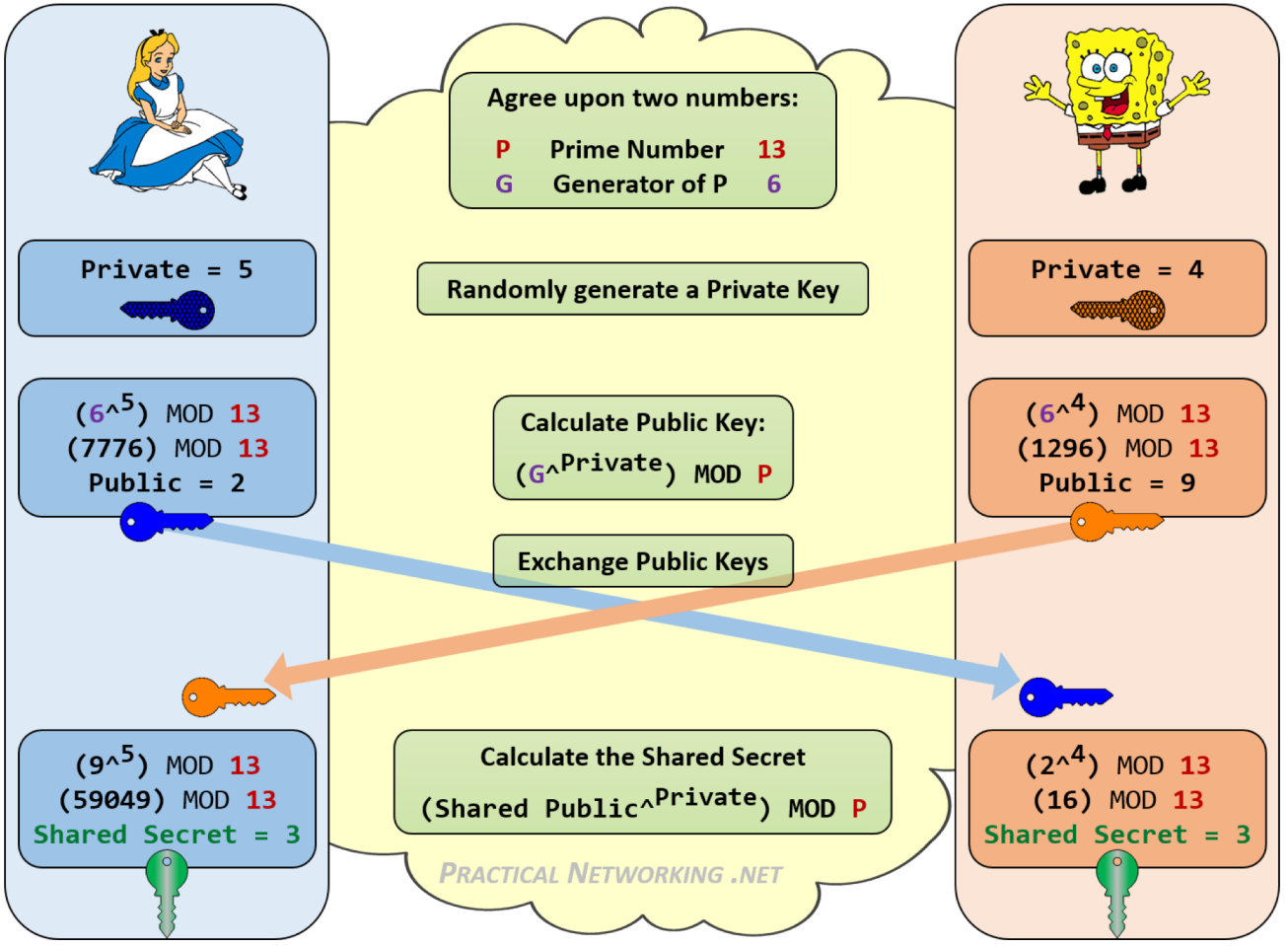
- Two or more parties agree on a key whereby both influence the outcome (perfect forward secrecy)
- Diffie-Hellman protocol first



Nextera Video

VSF VIDEO SERVICES FORUM

Diffie Hellman Key Exchange (Ephemeral)



Nextera Video

VSF VIDEO SERVICES FORUM

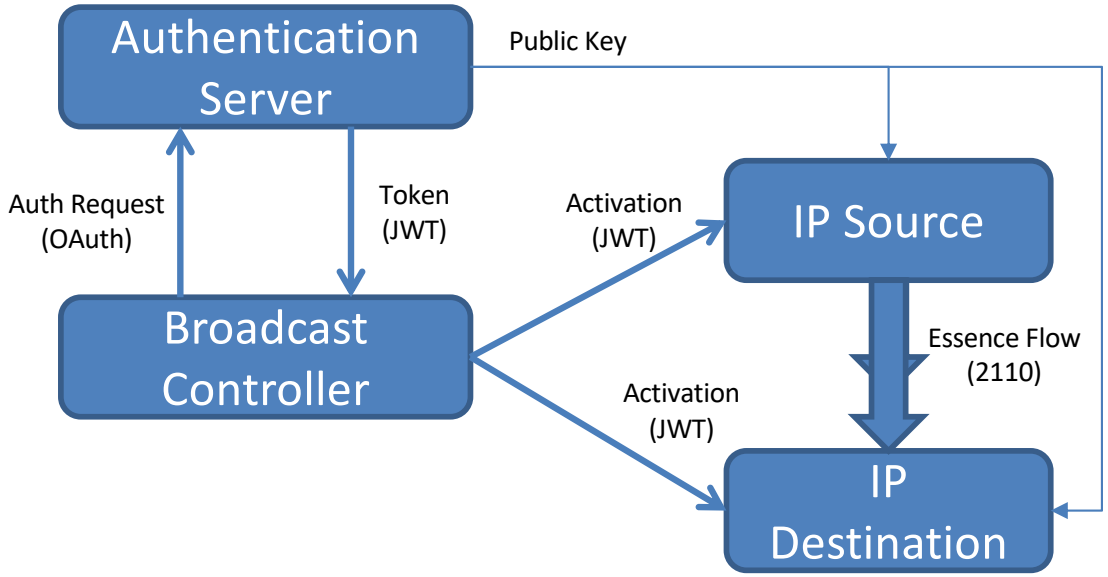
Public Key Infrastructure (PKI)

- A set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.

Nextera Video

VSF VIDEO SERVICES FORUM

NMOS BCP-003-01 Example



Nextera Video

VSF VIDEO SERVICES FORUM

Core Technologies

- PKI (Public Key Infrastructure)
- HTTPS (HTTP over TLS)
  - Connection Security (Encrypted Control Signals)
- REST (HTTPS PUT & GET)
- JSON (Key-Value Parameter sets)
- OAuth 2.0
  - Clients Authenticate with Authentication Server
- JWT (JSON Web Token)
  - Client Authorization (issue access tokens) – RSA with SHA-256

Nextera Video

VSF VIDEO SERVICES FORUM

NMOS Security Goals

- **Confidentiality -** Data passing between client and the APIs is unreadable to third parties.
- **Identification -** The client can check whether the API it is interacting with is owned by a trusted party.
- **Integrity -** It must be clear if data travelling to or from the API been tampered with.
- **Authentication -** The client can check if packets actually came from the API it is interacting with, and vice versa.

Nextera Video

VSF VIDEO SERVICES FORUM

NMOS Cipher Suite

- TLS ECDHE ECDSA WITH AES 128 GCM SHA256
- TLS ECDHE ECDSA WITH AES 256 GCM SHA384
- TLS ECDHE ECDSA WITH AES 128 CBC SHA256
- TLS ECDHE ECDSA WITH AES 256 CBC SHA384
- TLS ECDHE RSA WITH AES 128 GCM SHA256
- TLS ECDHE RSA WITH AES 256 GCM SHA384
- TLS DHE RSA WITH AES 128 GCM SHA256
- TLS DHE RSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 128 CBC SHA256
- TLS ECDHE RSA WITH AES 256 CBC SHA384
- TLS DHE RSA WITH AES 128 CBC SHA256
- TLS DHE RSA WITH AES 256 CBC SHA256
- TLS ECDHE ECDSA WITH AES 128 CCM 8 ←======= **Minimum Requirement**

Johnny Quest Decoder Ring:

TLS = Transport Layer Security
ECDHE = Elliptic Curve Diffie-Hellman Ephemeral KE
ECDSA = Elliptic Curve Digital Signature Algorithm
AES = Advanced Encryption Standard (#bits)
GCM = Galois/Counter Mode
CBC = Cipher Block Chaining (XOR)
SHA = Secure Hash Algorithm (#bits)
CCM = Counter with CBC-MAC(Cyber Block Chaining Message Authentication Code)

Nextera Video

VSF VIDEO SERVICES FORUM

Summary

- Security is crucial in the internet age
  - Especially if you have high value content
- The US Government has been working on this for years
  - Leverage work from NIST, NSA, DoD
- NMOS Control Security is a great first step
  - https, Authentication Servers, etc.
- For Highest Security, Essence encryption is readily available
  - Compatible with any transport (2110, 2022, RTP, etc)

Nextera Video

VSF VIDEO SERVICES FORUM