

Essentials of HDCP 2.2 Authentication & Encryption Protocols for HDMI and DisplayPort

Neal Kendall – Marketing Manager
Teledyne LeCroy quantumdata Product Family
neal.kendall@teledyne.com



quantumdata™

HDCP 2.2 Webinar Agenda

- ◆ What is HDCP 2.2?
- ◆ Overview of Modern Cryptography
- ◆ HDCP 2.2 Authentication & Key Exchange, Pairing, Locality Check
- ◆ HDCP 2.2 Encryption
- ◆ HDCP 2.2 Compliance Testing
- ◆ Please Check out our other “Essentials of” Webinars:
 - ◆ [Essentials of DisplayPort Protocols](#)
 - ◆ [Essentials of HDCP 2.2 Protocols](#)
 - ◆ [Essentials of HDMI Fixed Rate Link \(FRL\) Protocols](#)
 - ◆ [Essentials of DisplayPort Display Stream \(DSC\) Protocols](#)

HDCP Overview



TELEDYNE LECROY
Everywhereyoulook™

Why HDCP?

- ◆ Remember the old days when you could copy movies on a VCR through an analog video interface cable?



What is HDCP?

- ◆ High-Bandwidth Digital Content Protection (HDCP) - A form of digital copy protection or “Digital Rights Management.”
- ◆ Developed by Intel Corporation in 2003.
- ◆ Licensing governed by Digital Content Protection, LLC (DCP).
- ◆ From DCP website:

“Digital Content Protection LLC (DCP) is an organization that licenses technologies for protecting premium commercial entertainment content. High-bandwidth Digital Content Protection (HDCP) is a specification developed by Intel Corporation to protect digital entertainment content across digital interfaces.”

- ◆ Provides a protection mechanism over the physical link, e.g. HDMI and DisplayPort.
- ◆ Control access—modification and distribution--of proprietary copyrighted material, i.e. television and motion picture content.
- ◆ HDCP 2.2 uses modern cryptography mechanisms.

HDCP Interoperability Problems

- ◆ Many people are aware of HDCP only because of interoperability problems while connecting DisplayPort or HDMI or devices.
- ◆ Some experts have said that HDCP is the most difficult thing to get right about HDMI and DisplayPort.

hdcp problems

All Shopping News Images Videos More Settings Tools

About 407,000 results (0.60 seconds)

HDMI = High-Definition Multimedia Interface. ... HDMI Handshake issues occur when the LCD or source does not accept the keys from HDMI Distribution equipment. HDMI / HDCP Handshaking issues = Problems with Video or Audio on your display (Mostly caused by an encryption named High-bandwidth Digital Content Protection (HDCP).)

Why HDCP Causes Errors on Your HDTV, and How to Fix It
[https://www.howtogeek.com/.../htg-explains-how-hdcp-breaks-your-hdtv-and-how-to... ▾](https://www.howtogeek.com/.../htg-explains-how-hdcp-breaks-your-hdtv-and-how-to...)
Feb 8, 2015 - There is a licensing body that **issues** licenses for **HDCP** devices. Each **HDCP** compliant device, like your Blu-ray player or Xbox, has a license and the ability to talk to the device it is outputting the signal to over the HDMI cable.

Why HDCP Causes Errors on Your HDTV, and How to Fix It
[https://www.howtogeek.com/.../htg-explains-how-hdcp-breaks-your-hdtv-and-how-to... ▾](https://www.howtogeek.com/.../htg-explains-how-hdcp-breaks-your-hdtv-and-how-to...)
Feb 8, 2015 - There is a licensing body that **issues** licenses for **HDCP** devices. Each **HDCP** compliant device, like your Blu-ray player or Xbox, has a license and the ability to talk to the device it is outputting the signal to over the HDMI cable.

HDCP / HDMI Handshake Troubleshooting and Guidelines
site.hdtvsupply.com/hdcp1.html ▾
HDMI / **HDCP** Handshaking **issues** = **Problems** with Video or Audio on your display (Mostly caused by an encryption named High-bandwidth Digital Content ...)

HDCP Communication Problems -
denon.custhelp.com/app/answers/detail/a_id/3341/~/hdcp-communication-problems ▾
An **HDCP** communication (syncing) issue occurs when a source device is not communicating properly or not fully compatible with the HDMI repeater in your ...

HDMI/DVI HDCP handshake problems & how to avoid them | EE Times
www.eetimes.com/document.asp?doc_id=1273716 ▾
Apr 11, 2007 - HDMI & DVI have a companion **high-definition content protection (HDCP)** system that sometimes leaves authorized consumers in mute, ...

What is an HDCP error? - YouTube

<https://www.youtube.com/watch?v=uLwf0ffB384> ▾
Jun 9, 2015 - Uploaded by HowToAV.tv
HowToAV.tv takes a look at how **HDCP** works - and how it can cause compliance **problems**, errors and a lack ...

HDCP Error: What It Is and How to Fix One - Lifewire
<https://www.lifewire.com/.../Home-Theater-How-Tos/Home-Theater-Key-Concepts> ▾
HDCP errors are caused when a device within a high-def setup is not **HDCP** ... great idea, it causes lots of **issues** for people who aren't even dealing with piracy.

What are the Functions of HDCP?

- ◆ HDCP supports three (3) primary functions:
 - ◆ **Authentication** – A protocol exchange initiated by the HDCP Transmitter to verify that a Receiver is licensed to receive HDCP content.
 - ◆ **Encryption** – The process by which HDCP encodes protected content such that only authorized devices can use it.
 - ◆ **Revocation (Renewability)** – Is a provision allowing HDCP to revoke the license of a receiver based on non-compliant behavior.



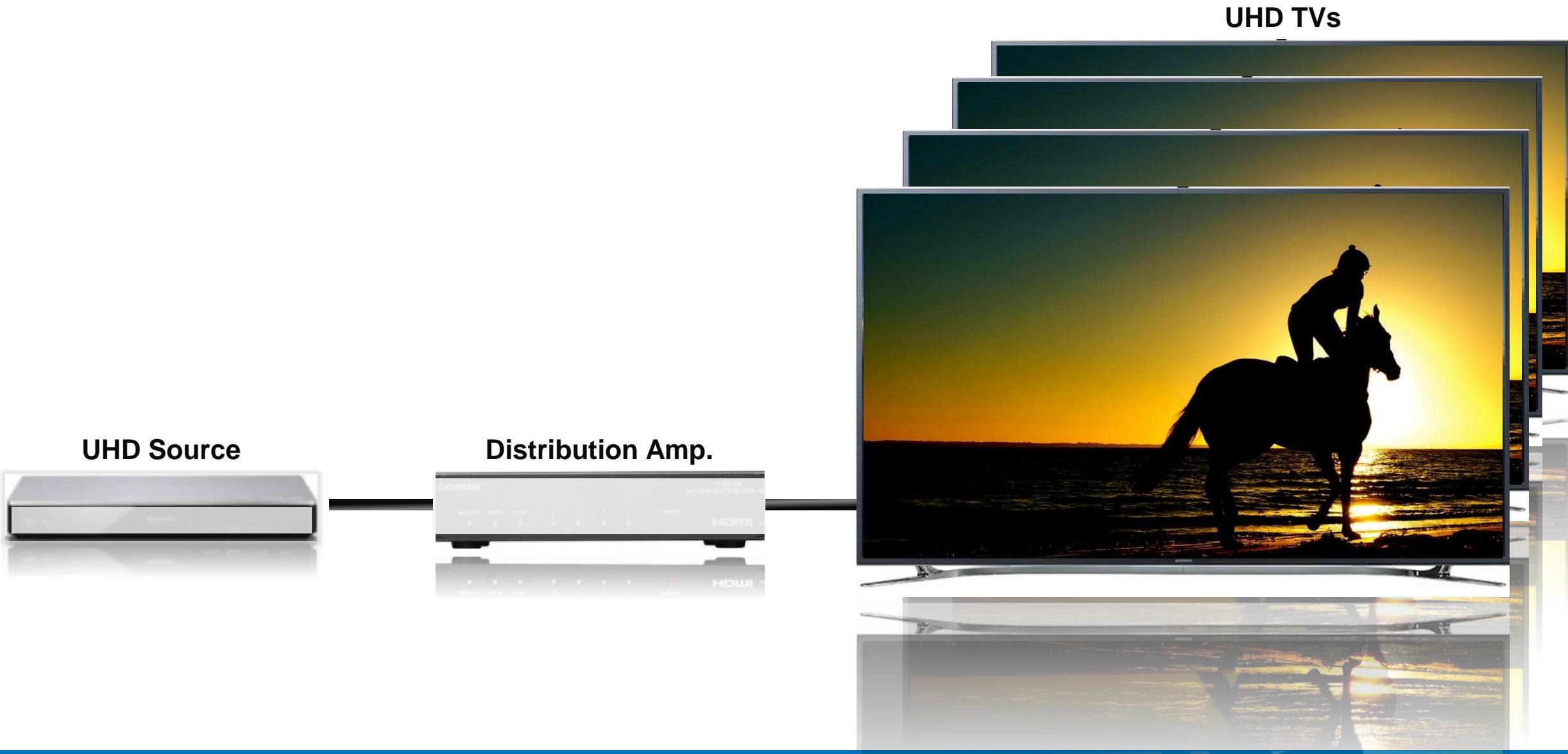
Basic HDCP 2.2 System - HDMI HDCP Transaction Channel - DDC



DisplayPort HDCP 2.2 Transaction Channel – Aux Channel



HDCP System with Distribution Device



Why HDCP 2.2?

- ◆ HDCP 1.x had some vulnerabilities.
- ◆ HDCP 2.2, not a continuation of HDCP 1.x.
- ◆ Robust, standards based link protection scheme.
 - ◆ RSA cryptography for key exchange during authentication.
 - ◆ Advanced Encryption Standard (AES) for encryption.
- ◆ New features:
 - ◆ “Pairing” to expedite authentication on subsequent authentications.
 - ◆ “Locality Check” to ensure the receiver is relatively close.

Overview of Modern Cryptography



TELEDYNE LECROY
Everywhereyoulook™

Cryptography

- ◆ **Definition:** Cryptography is the practice and study of techniques for securing communication in the presence of third party adversaries.
- ◆ Cryptographic functions include:

- ◆ Hashing



- ◆ Random Number Generation



- ◆ Encryption



- ◆ Digital Certificates and Digital Signatures

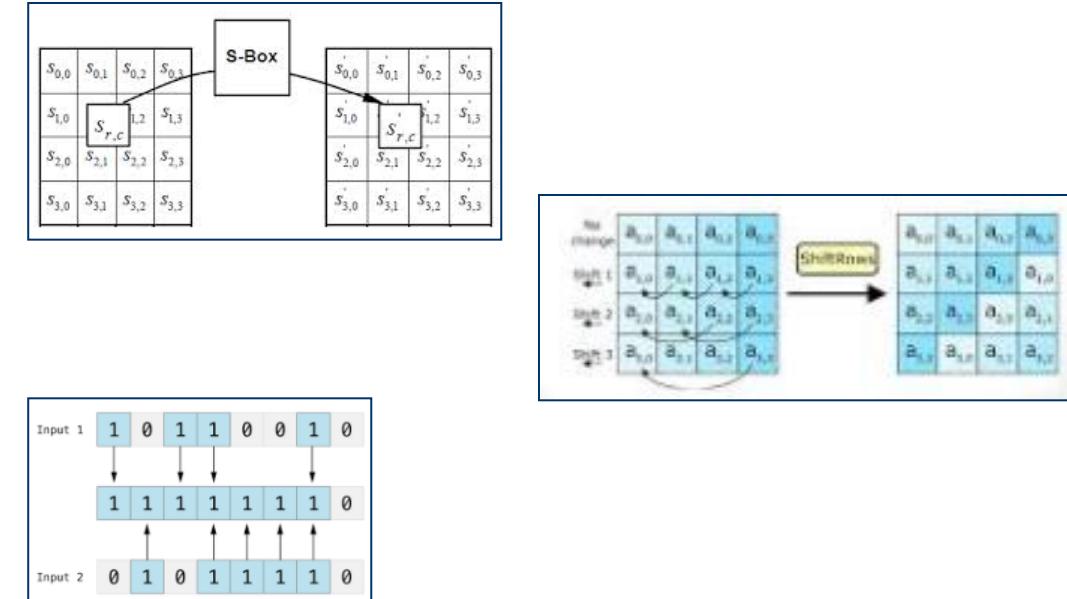


Cryptography

- ◆ Modern cryptography uses mathematical algorithms to transform information.
- ◆ There are three primitives to achieve this:
 - ◆ Substitution – Change the characters in a message.
 - ◆ Transposition – Rearrange the characters in a message.
 - ◆ Bitwise operation – XOR, AND, NOT, OR.

Note: These processes are often repeated multiple times.

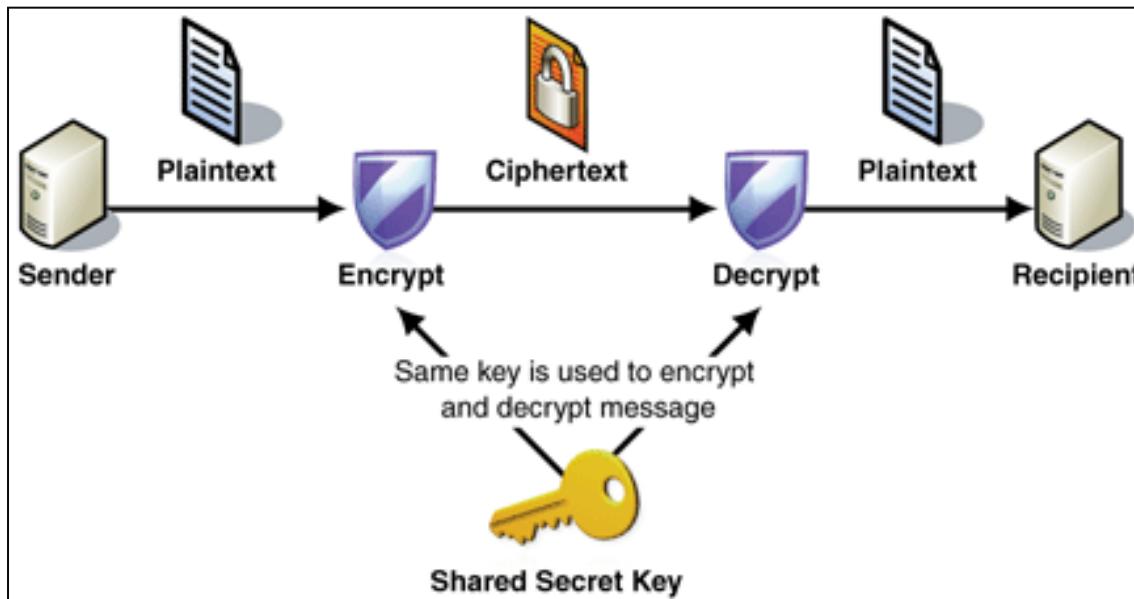
- ◆ HDCP uses cryptography to encrypt audio and video content.



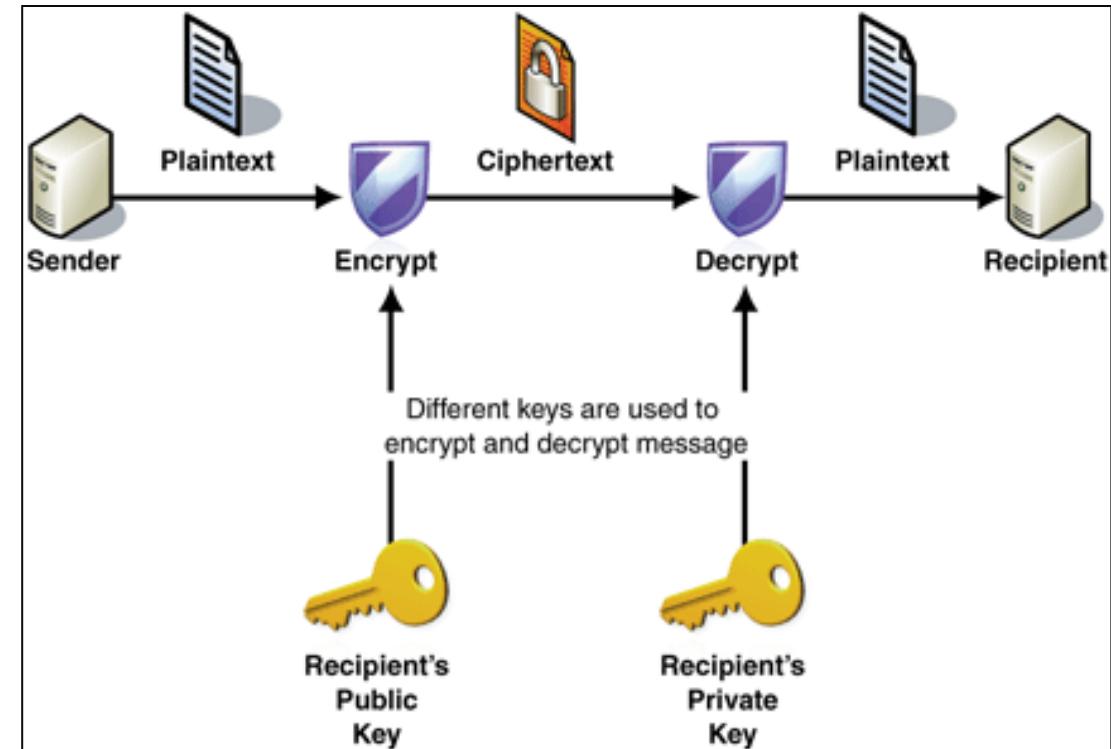
Types of Modern Cryptography

- ◆ Cryptographic systems can be categorized by the keys they use:
 - ◆ Symmetric-Key (Private-Key) Encryption. (AES)
 - ◆ Asymmetric-Key (Public-Key) Encryption. (RSA)

Symmetric (Private) Key Encryption (AES)



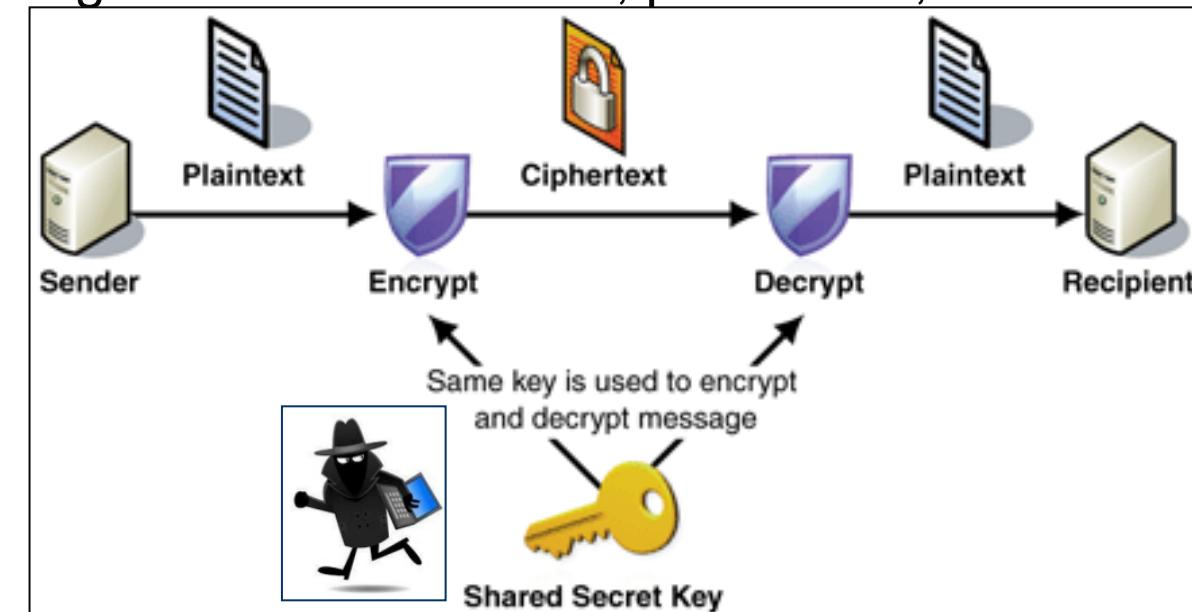
Asymmetric (Public) Key Encryption (RSA)



Types of Cryptography - Symmetric (Private) Key Encryption (AES)

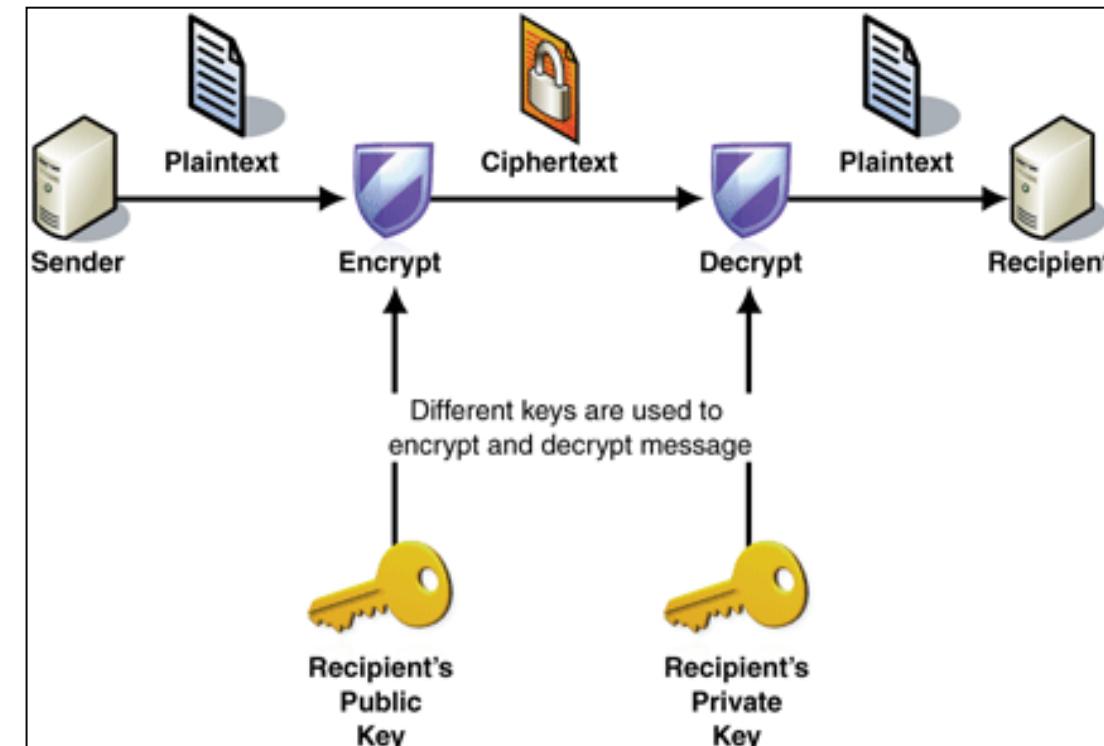
- ◆ **Definition:** A Cryptographic process using a ***shared, secret, private*** key for encrypting & decrypting information between two parties.
- ◆ The commonly used Data Encryption Standard (DES) and the newer, more robust Advanced Encryption Standard (AES) (used in HDCP 2.2) are forms of symmetrical block cipher techniques.
- ◆ Symmetric Key encryption is ***much faster*** than Asymmetric Key encryption.
- ◆ Used primarily when have to store data in a single place “*data at rest.*”
Examples are: storing data in a database and storing credit card numbers, passwords, etc.
- ◆ **Main drawbacks:**
 - ◆ Secret key needs to be ***stored*** securely.
 - ◆ Requires a *pre-agreed* upon secret key, or...
 - ◆ ...a *secure channel* to exchange the secret key.
 - ◆ Requires *separate keys for each authentication* party. There is an explosion in the number of keys required.

Note: In Consumer Electronic devices there is a need to exchange information with non-familiar devices



Cryptography – Asymmetric (Public) Key Encryption (RSA)

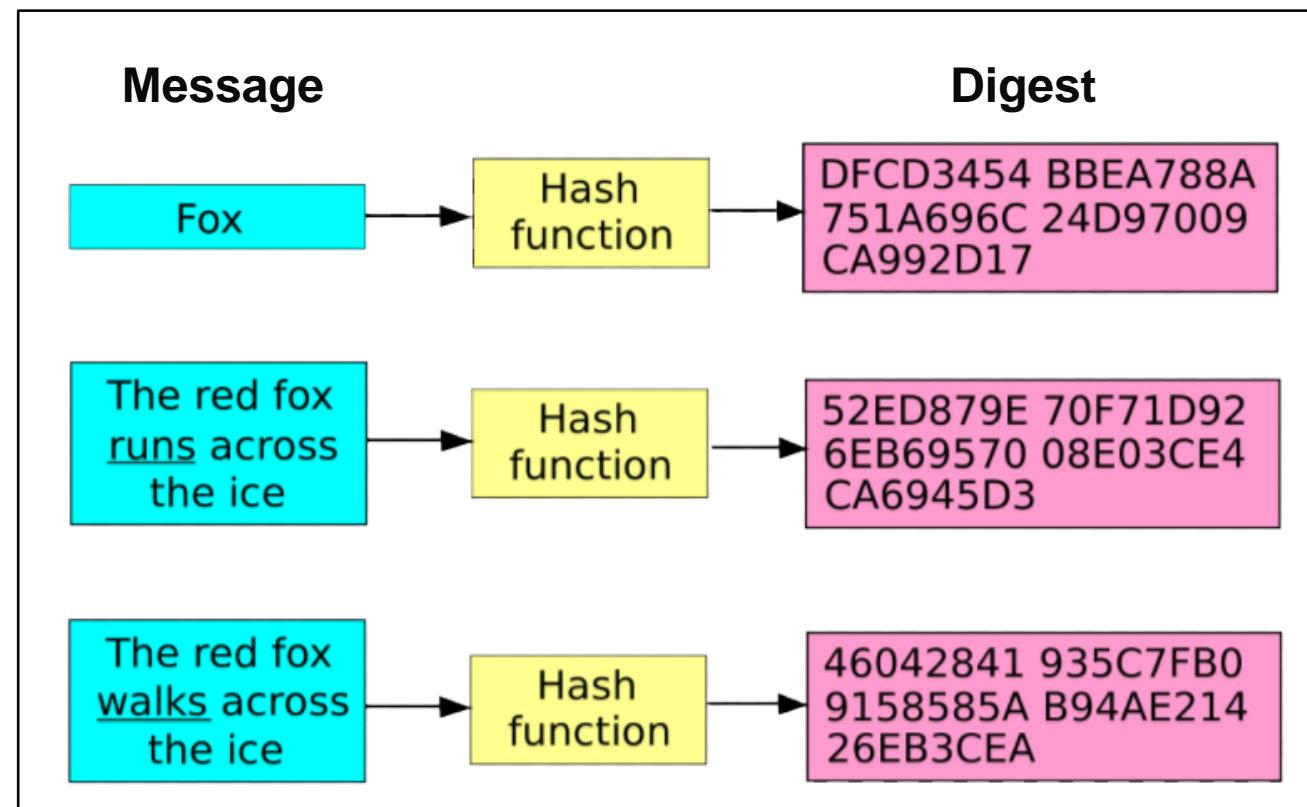
- ◆ A cryptographic system that uses pairs of keys: a **Public Key** which may be disseminated widely, and a **Private Key** which is known only to the owner—e.g. The Receiver.
- ◆ Invented to address the need for exchanging a secret key over an unsecured link.
- ◆ Used when there are separate device endpoints, e.g. web browsers, VPNs, secure shell, secure FTP.
- ◆ RSA is one of the first Asymmetric Key encryption systems and is widely used and used in HDCP 2.2.
- ◆ Because of the computational complexity of Asymmetric Key encryption, it is **very slow**.
- ◆ Used only for small blocks of data.
- ◆ Many modern systems are a **hybrid** between symmetric and asymmetric key encryption.
- ◆ **Often used to transfer a key that will be used for symmetric key encryption** (e.g. “Master Key” in HDCP 2.2).



Cryptography Hash Functions

Cryptographic Hash Functions – What Are They?

- ◆ **Definition:** A cryptographic hash function is a mathematical algorithm that can be used to map data of **arbitrary size** to data of a **fixed size**.
- ◆ They have been described as the “work horses” of modern cryptography.
- ◆ Cryptographic hash functions are said to be “**one-way functions**” because they cannot easily be reversed. The only way to recreate the input data (“message”) from an ideal cryptographic hash function’s output (“Digest”) is to attempt a brute-force search of possible inputs.
- ◆ **Wikipedia:** “SHA-2 is a set of cryptographic hash functions designed by the National Security Agency (NSA).”
- ◆ SHA-256 is a common type of Secure Hash Algorithm.
 - ◆ Used extensively in HDCP 2.2.
 - ◆ Produces a “Digest” of 256 bits regardless of the size of the message input.



Cryptographic Hash Functions – What Are They?

- ◆ The ideal cryptographic hash function has **five (5) main properties**:
 - ◆ A small change to a message should change the hash value so extensively that the new hash value appears **uncorrelated** with the old hash value.
 - ◆ It is **deterministic** so the same message always results in the same hash digest.
 - ◆ It is **quick to compute** the hash value for any message.
 - ◆ It is **infeasible** to generate a message from its hash value (“Digest”) except by trying all possible messages.
 - ◆ It is infeasible to find two different messages with the same hash value “**collision resistance**.”

Note: “Collision resistance” does not mean that no collisions exist; simply that they are hard to find.

(Every hash function with more inputs than outputs will necessarily have collisions.)

- ◆ In HDCP 2.2 SHA-256 Hash is used for:
 - ◆ Verifying the Receiver’s Certificate.
 - ◆ Verifying that the Receiver properly decrypted the Master Key (Km).
 - ◆ Verifying the Locality Check.
 - ◆ Storing the Master Key for Pairing.

SHA-256 produces a 256-bit (32-byte) hash value.

Data

The quick brown fox jumps over the lazy dog.

SHA-256 hash

ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

Calculate SHA256 hash

SHA-256 produces a 256-bit (32-byte) hash value.

Data

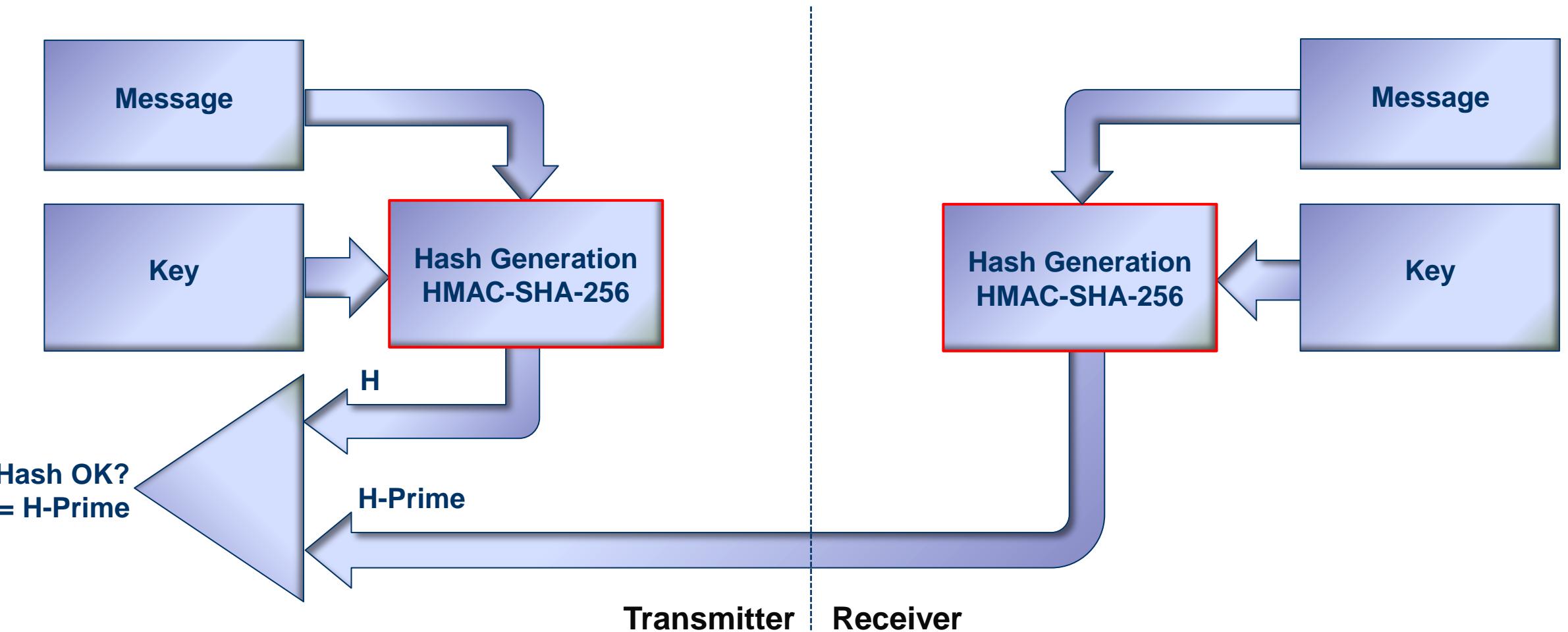
The quick brown fox jumps over the lasy dog.

SHA-256 hash

0f7e95846040fdc01abb3bf1981cd3eca4de5380380187453920406cd2cbfc35

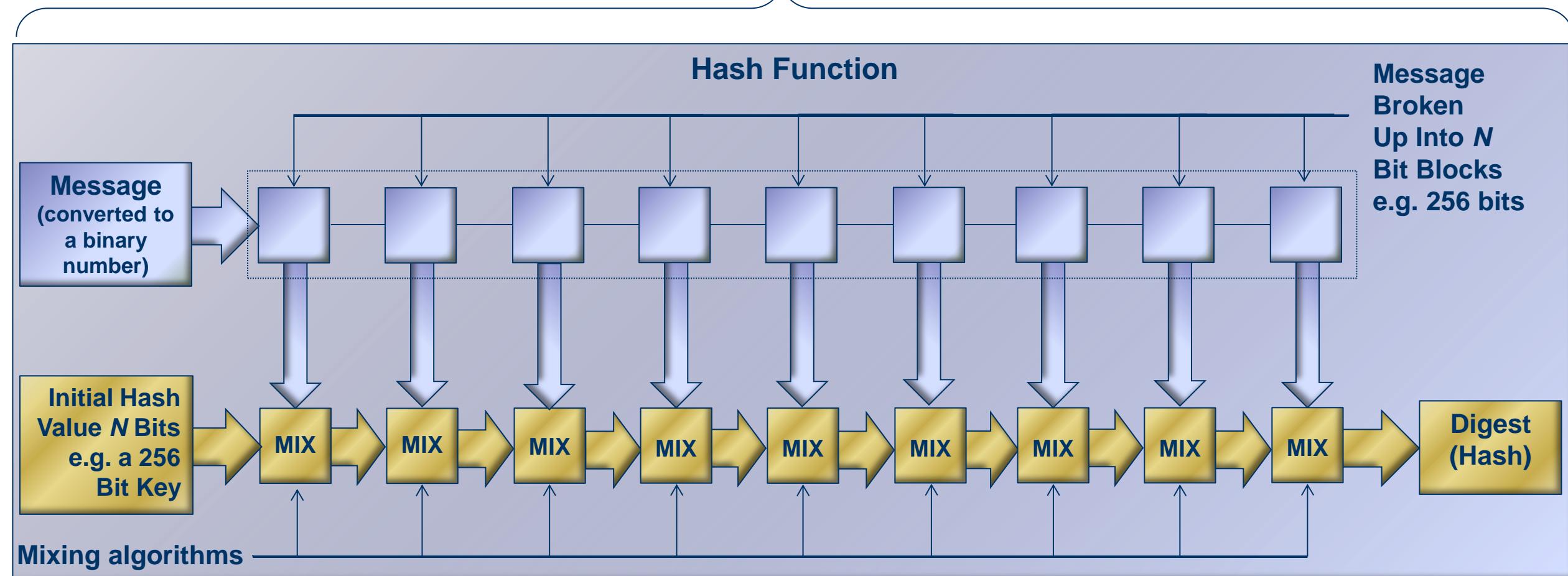
Calculate SHA256 hash

Hash Function Application



Cryptographic Hash Functions – How Do They Work?

- ◆ Mixing functions use bitwise operations such as AND, XOR, NOT, OR, Rotate.



Cryptography Random Number Generation

Cryptographic Random Number Generation

- ◆ Types of Random Number Generators:
 - ◆ **True** Random Number Generators – Use natural source of randomness such as thermal noise, network statistics, error counter information, etc.
 - ◆ **Pseudo**-Random Number Generators – Use initial randomly generated seed value. Uses deterministic algorithms.
- ◆ Measure of randomness is “Entropy”:
 - ◆ Entropy is the degree of randomness or ***the extent to which all possible outcomes are equally likely***. When entropy is high, it is ***infeasible to predict*** an output better than pure random chance. Dice throws and coin flips offer a high degree of entropy.
 - ◆ You can't infer the entropy from single instance of a “random” bit stream sample. You can only determine the level of entropy from knowing the process itself or empirically through a vast set of trials.



Cryptographic Random Number Generation

- ◆ HDCP 2.2 specifies randomness in generating numbers in terms of two levels of Entropy:
 - ◆ For generating **R-Tx**, **R-Rx**, **Riv**, **Rn** – Use pseudo-random generation with a *minimum entropy of 40 random bits out of 64-bits*.
 - ◆ For generating **Master Key (Km)** and **Session Key (Ks)** – Use **true** random number generator or a pseudo random number generator with a **true random number seed** (cryptographically secure pseudo random number generator) with *minimum entropy of 128 random bits out of the 128 bits*. This means that the 128 bit Master and Session Keys would have to be true random numbers.
- ◆ HDCP recommends NIST SP 800-90 standard for random number generator.



7533206878823911356146
9289849205421587384965
7658002911953490208577
7315977929516937604413
8758246879451413674490
1747676321055580371590
8949962108848481712871
3579800010877523099953
9503933440811390142538
3093850448135297727071
6498379800541667309513
1695722888148018950498
2400030309849861077238
6213354283785851108806
2125162503461876662520
4042743010056640419511
2775214293055220464507

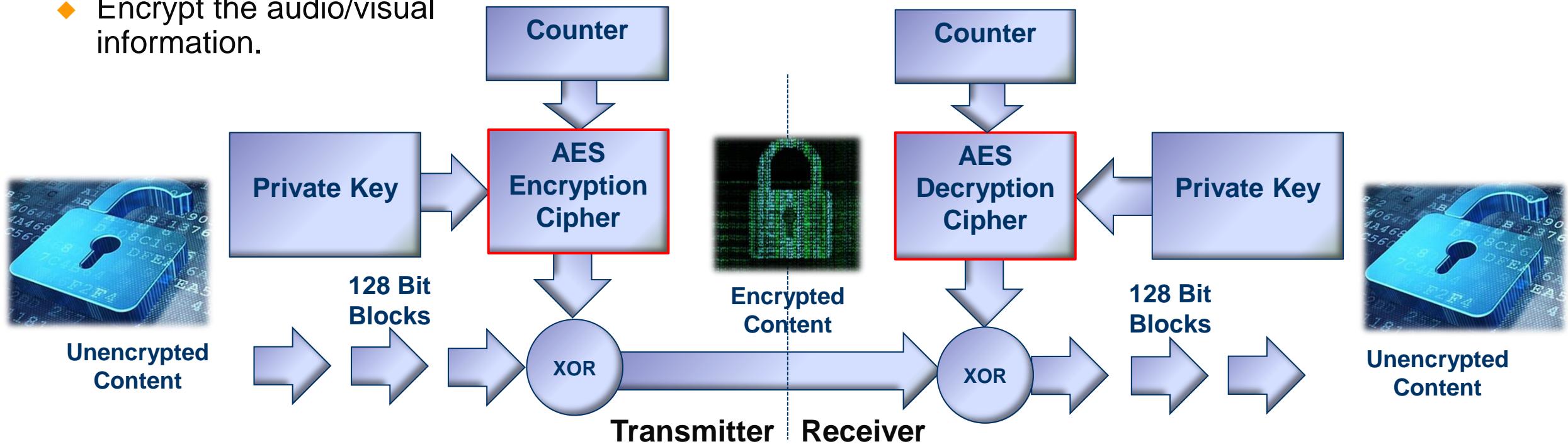


Cryptography

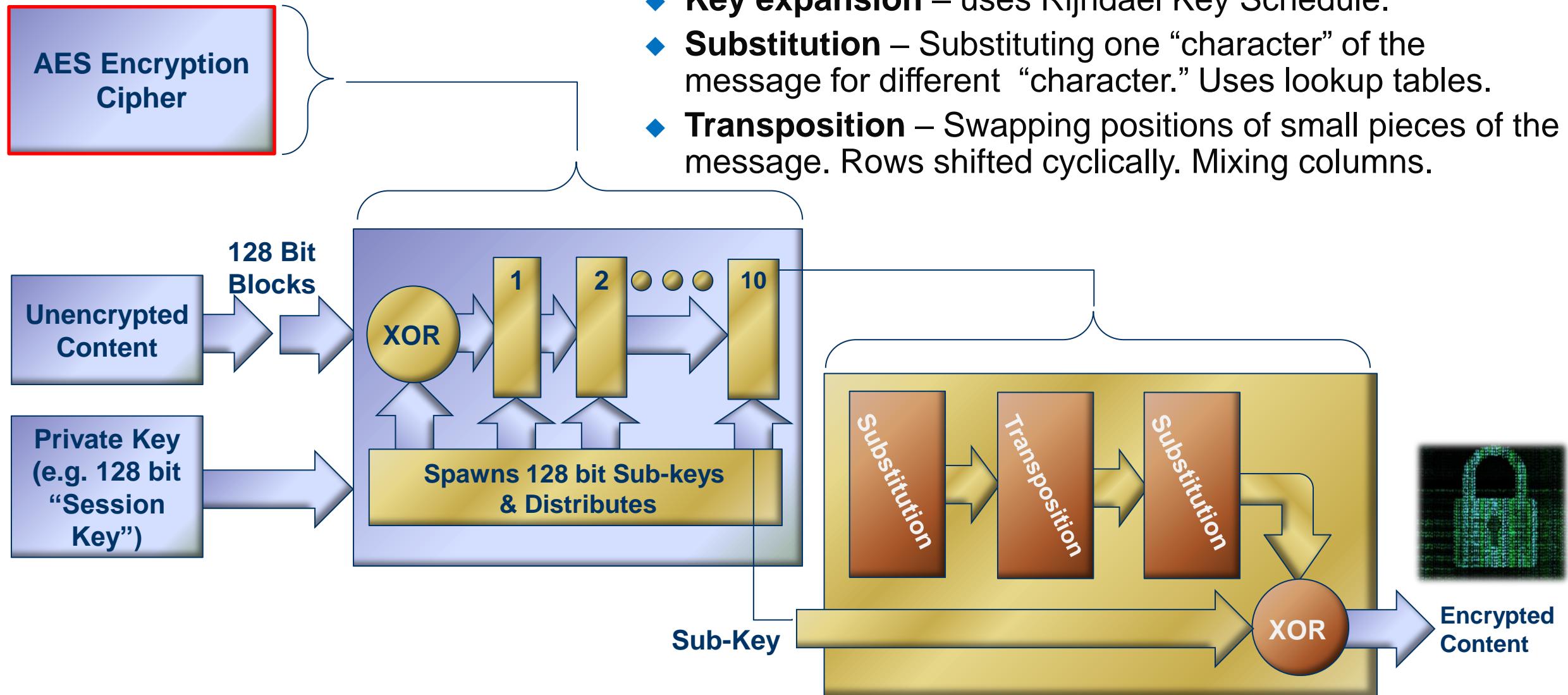
AES Encryption

AES Encryption

- ◆ AES is a **Symmetric (Private) Key** encryption mechanism. It uses a single shared private key.
- ◆ AES is a “block cipher” meaning that it operates on small blocks of data at a time.
- ◆ AES has five (5) different modes that it can be operated in. **HDCP uses Counter Mode** (below).
- ◆ AES is used in HDCP 2.2 for the following functions:
 - ◆ Encrypt the Master Key (Km) for storage to facilitate “Pairing.”
 - ◆ Encrypting and exchanging the Session Key (Ks).
 - ◆ Encrypt the audio/visual information.



AES Encryption – How Does it Work?



Cryptography

RSA Encryption

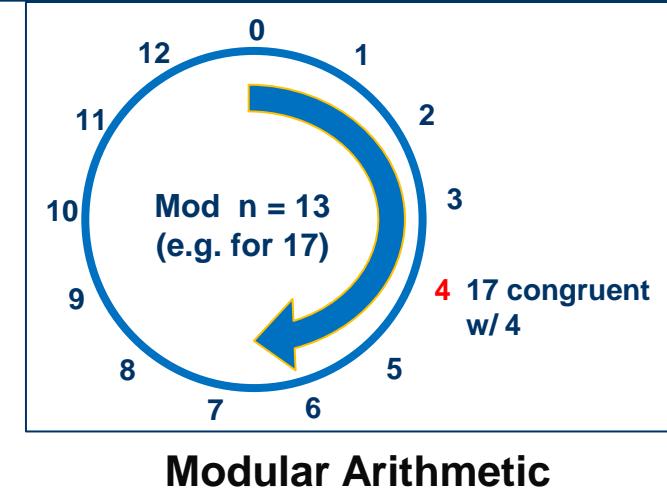
RSA Encryption

- ◆ RSA is the most widely used encryption algorithm.
- ◆ RSA is an Asymmetric Key encryption mechanism. It uses a public and a private key.
- ◆ RSA is used when there is a need to exchange *small quantities of private information* with multiple parties and *when there is no secure channel* to exchange a private (*shared*) key between parties.
- ◆ RSA is used in HDCP 2.2 to *verify the Receiver's certificate* and to *encrypt the Master key* before it is exchanged with a Receiver.
- ◆ Developed by MIT professors:

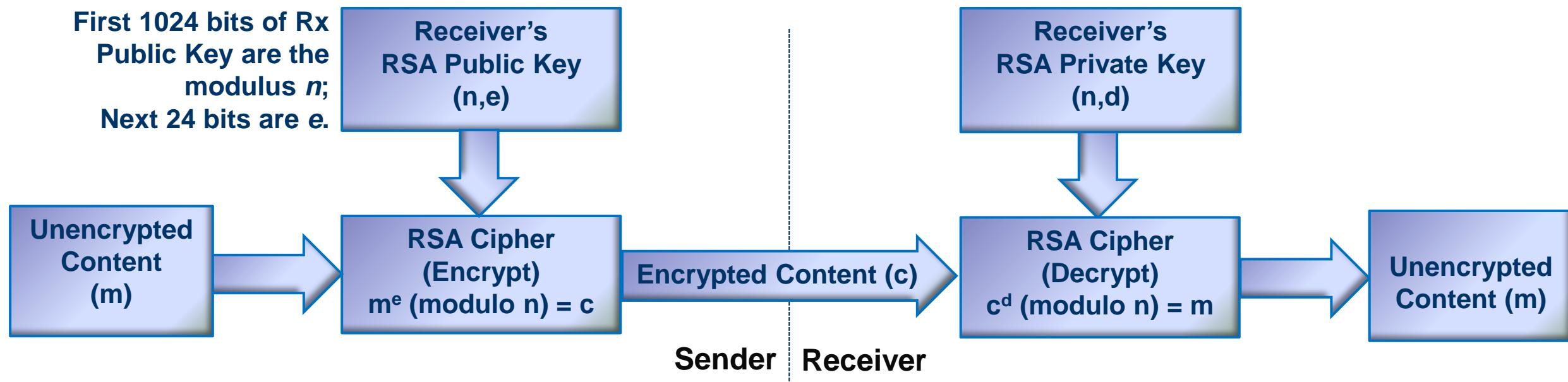


RSA Encryption

- ◆ RSA uses the concept of a **one-way function**; Multiplying 2 prime numbers is easy but *reversing* the process to find the product's 2 prime numbers (prime factorization) is very difficult.
- ◆ Uses modular arithmetic, or “clock arithmetic.”
- ◆ The n is the product of 2 large prime numbers; it is used as the modulo in the clock arithmetic.
- ◆ Choosing values of e and d is an important factor. Calculation uses what is called a Phi function such that: $e * d \pmod{\Phi} = 1$.



Modular Arithmetic



Cryptography Digital Signatures and Digital Certificates

Digital Certificates and Digital Signatures

- ◆ Digital Certificates:
 - ◆ A Digital Certificate is electronic information or document that is issued by a trusted third party—a “Certificate Authority” (CA)—that provides a way for a sender to verify that a receiver is a trusted party for private communication.
 - ◆ Digital Certificates contain an owner identifier and a public key.
- ◆ Digital Signatures:
 - ◆ A Digital Signature is a *mechanism* or *method* to verify the *authenticity* of a digital message or document (which could be a Digital Certificate).
 - ◆ Verifying authenticity means verifying that the message was generated by the assumed sender, i.e. the owner, and that it has not been tampered with.
 - ◆ Digital Signatures use RSA (public and private keys) and hashing to affect the signature.
 - ◆ It is infeasible to re-generate the Digital Signature without the private key used in the signature.

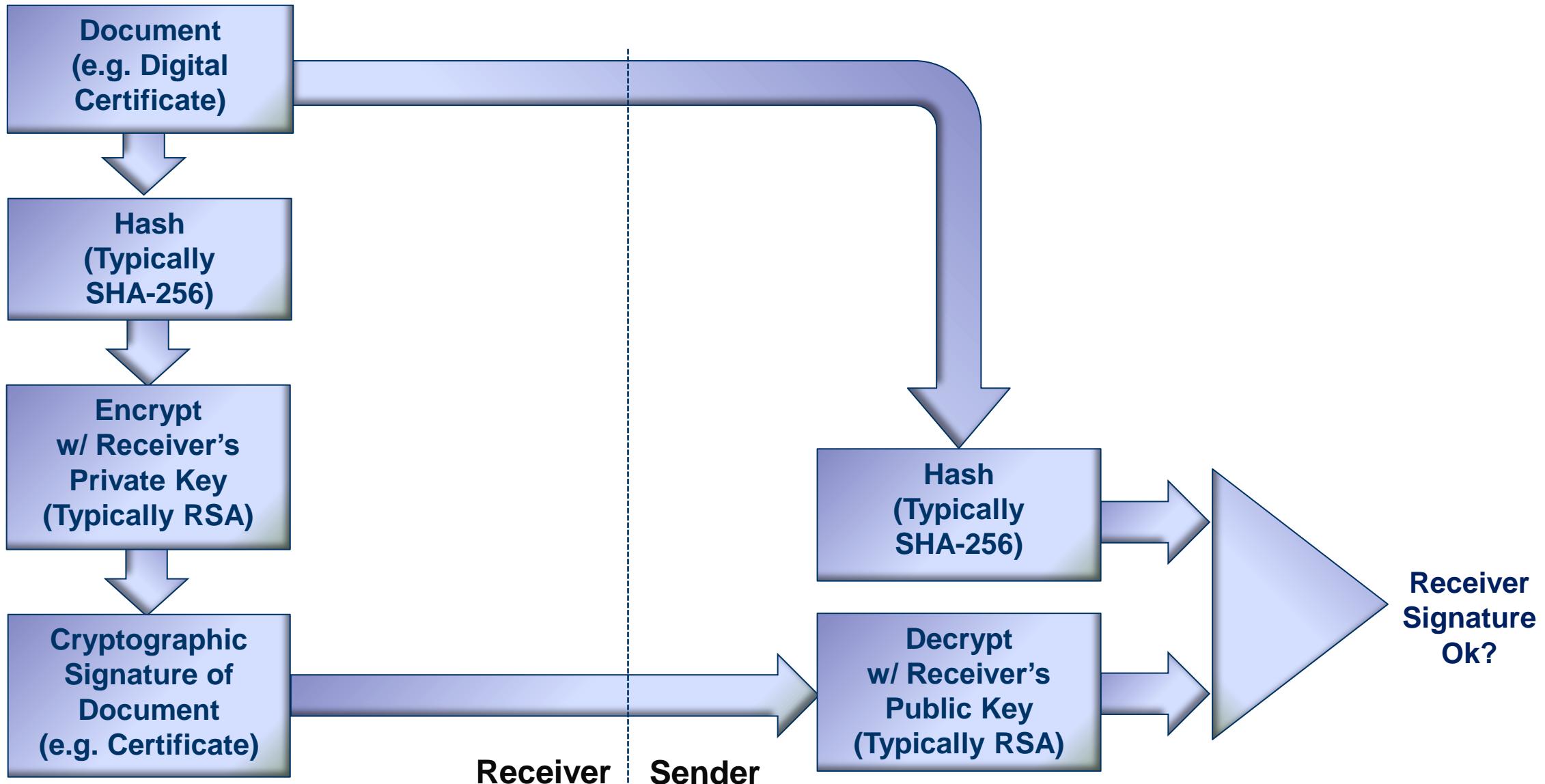


Digital Certificates and Digital Signatures

- ◆ In HDCP 2.2, the Trusted Third party is Digital Content Protection, LLC (DCP) who issues the HDCP Receiver's certificate.
- ◆ DCP applies a Digital Signature to the HDCP Receiver's certificate by applying a hash function (Hash-256) and RSA encrypts it with the Receiver's private key.
- ◆ This Digital Signature associates the RSA public key (which is part of the certificate that gets hashed and encrypted) with the Receiver ID, i.e. the owner of the Digital Certificate.



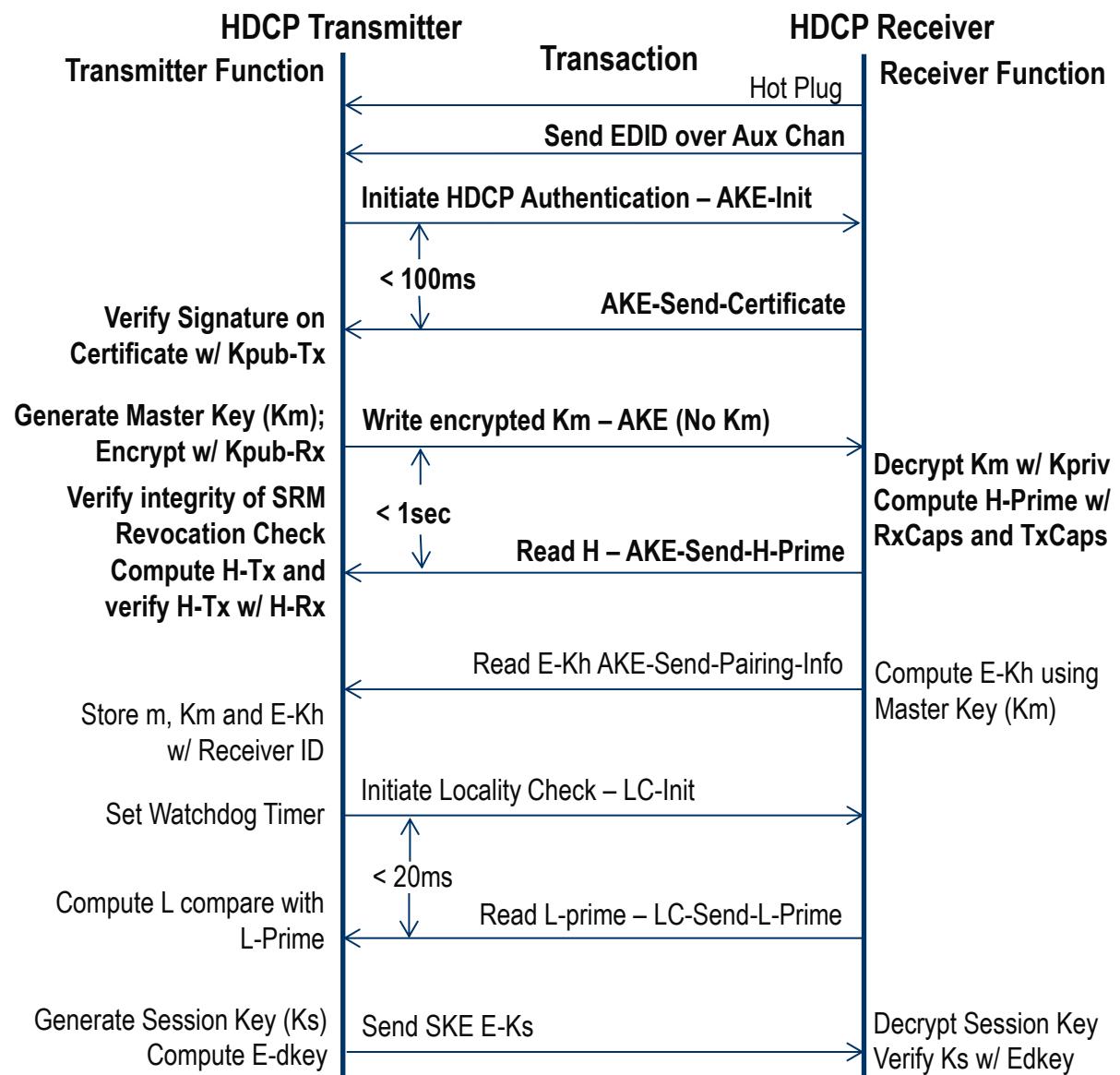
Digital Signatures and Digital Certificates Application



HDCP 2.2 Authentication and Key Exchange



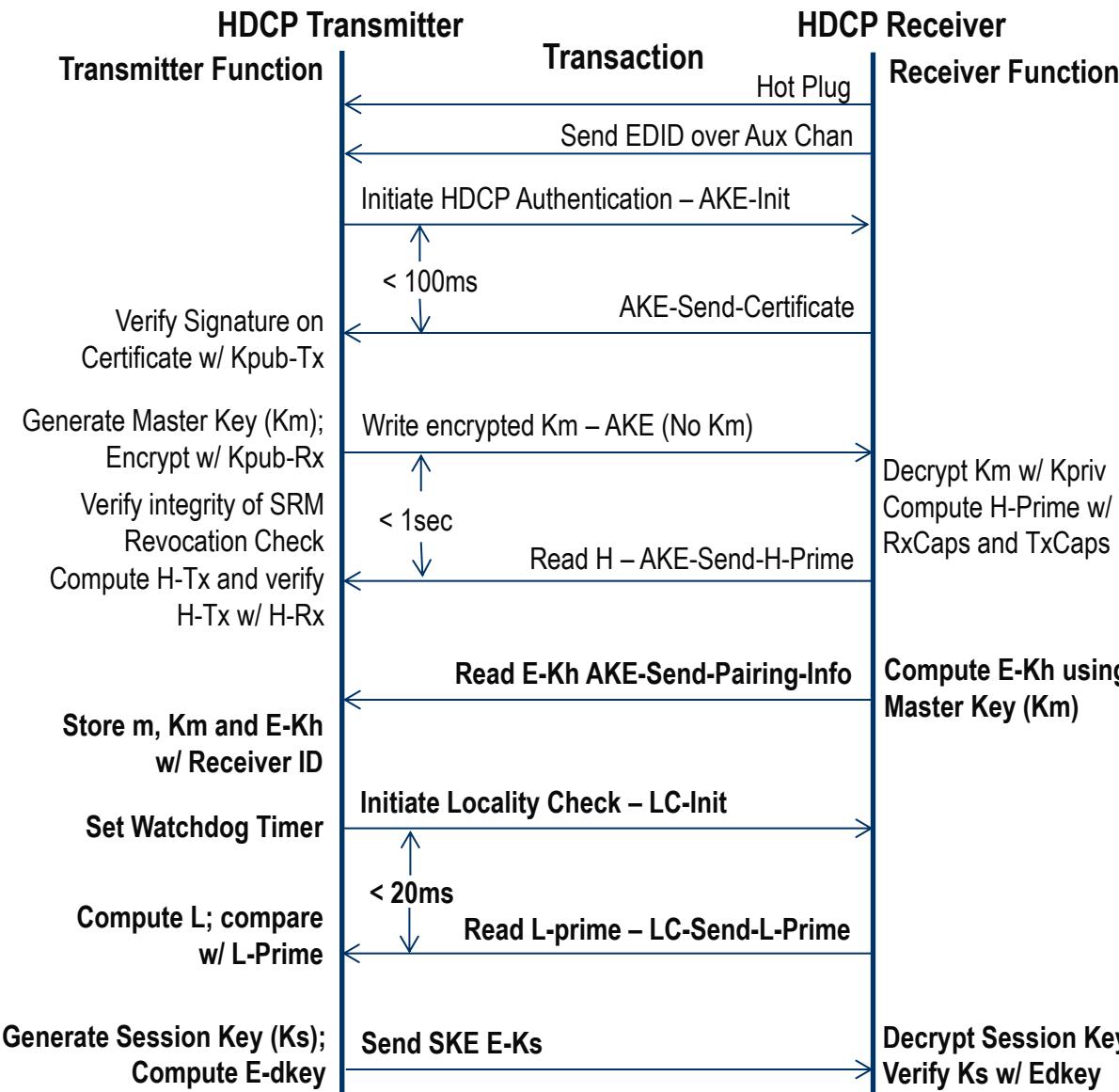
HDCP 2.2 Authentication and Key Exchange Sequence



Authentication and Key Exchange

- Hot plug asserted from the Receiver.
- Transmitter reads EDID from Receiver.
- Initiate Authentication (AKE-Init) – Transmitter sends initiation message (AKE-Init) which contains a 64 bit pseudo-random value (R-Tx) and TxCaps parameters. TxCaps parameters are the HDCP capabilities of the transmitter.
- AKE-Send-Cert – Receiver sends Cert-Rx which contains a 64 bit pseudo-random value (R-Rx) and RxCaps parameters in response to Transmitter read. RxCaps parameters are the HDCP capabilities of the receiver. (Must be transmitted within 100 ms of AKE-Init.)
- Transmitter extracts Receiver ID from Cert-Rx - Verifies Signature on Cert-Rx using Kpub-Rx (a 1048 bit RSA public key of a receiver) using the following steps:
 - Transmitter generates Km (a 128-bit Master Key). Km is then encrypted using E-Kpub (a 1024 bit value).
 - Write encrypted Km-AKE – Transmitter sends AKE-Km message to receiver containing the E-Kpub.
 - Receiver decrypts Km w/ Kpriv-Rx (Receiver private key RSA).
 - Receiver computes H-prime (256-bit) w/ RxCaps & TxCaps.
 - Read H (AKE-Send-H-prime) – Receiver sends AKE-Send-H-Prime in response to Transmitter read. H-prime must be within 1 Sec from time the Transmitter writes AKE-Km message.
 - Transmitter verifies receiver with revocation list.
- Transmitter computes H-Tx; compares with H-Rx (H-Prime).

HDCP 2.2 Authentication...Pairing, Locality Check, Session Key Exchange



Pairing

- Transmitter-Receiver Pairing is performed using the following steps:
 - Read E-Kh – AKE-Send-Pairing-Info – Receiver sends E-Kh using encryption of Km in response to Transmitter read.
 - Transmitter stores m, Km and E-Kh with Receiver ID (a 40 bit value [20 ones and 20 zeros] that uniquely identifies a licensed receiver).

Locality Check

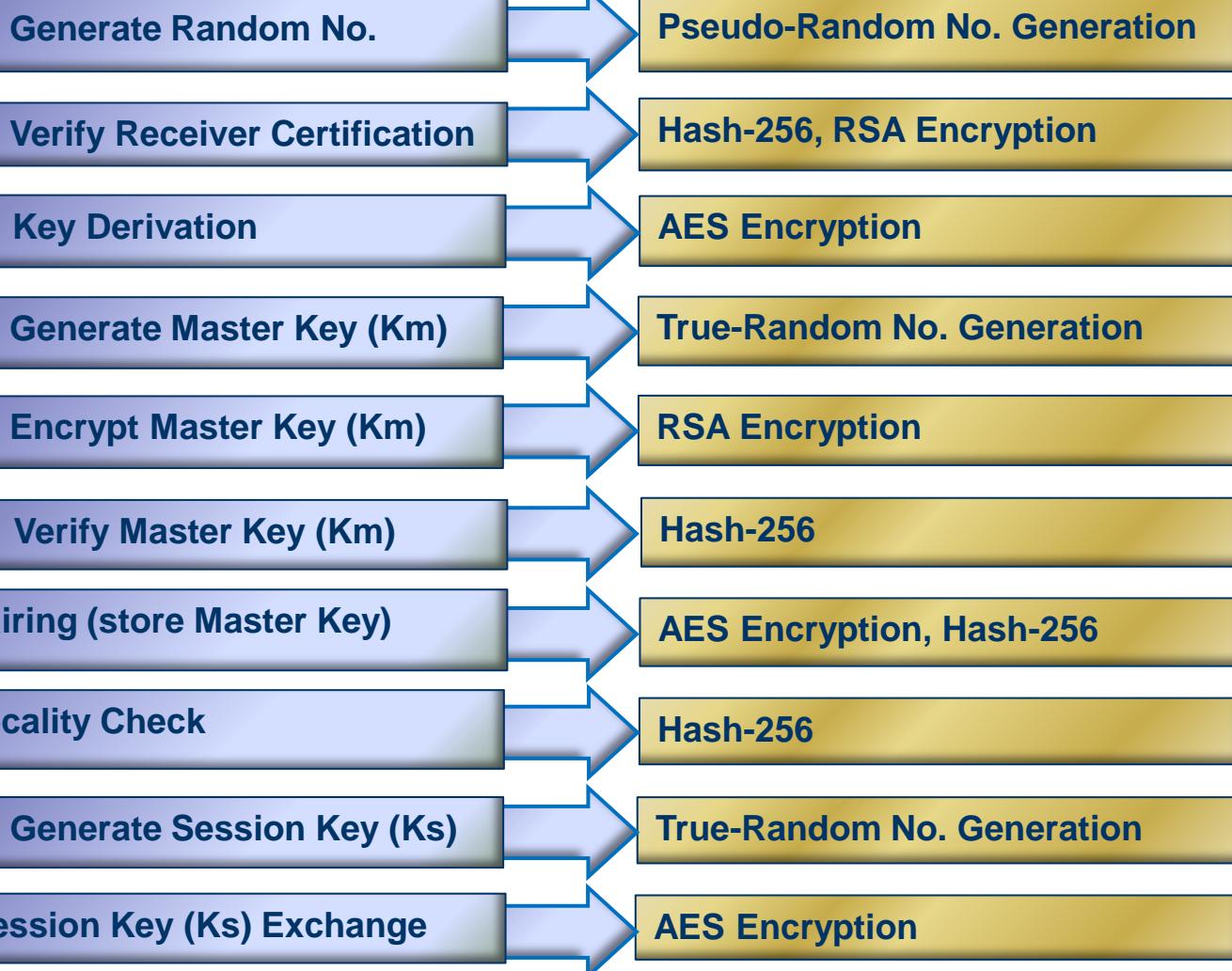
- Locality Check is performed by Transmitter using the following steps:
 - Transmitter sets a watchdog timer.
 - Initiate Locality Check – Transmitter sends LC-Init to receiver.
 - Receiver computes L-Prime (256 bit value).
 - Read L - Receiver transmits LC-Send-L-Prime in response to Transmitter read.
 - Transmitter computes L and compares w/ L-prime from receiver.

Session Key Exchange

- Session Key Exchange involves the following steps:
 - Transmitter generates a 128-bit pseudo-random Session key (Ks) and a 64-bit pseudo-random number R-iv.
 - Derives/computes 128-bit E-dkey using Ks.
 - Transmitter sends E-dkey to receiver.
 - Receiver derives Ks, verifies that it's equal to E-dkey received.

HDCP 2.2 Cryptographic Summary

Authentication & Key Exchange

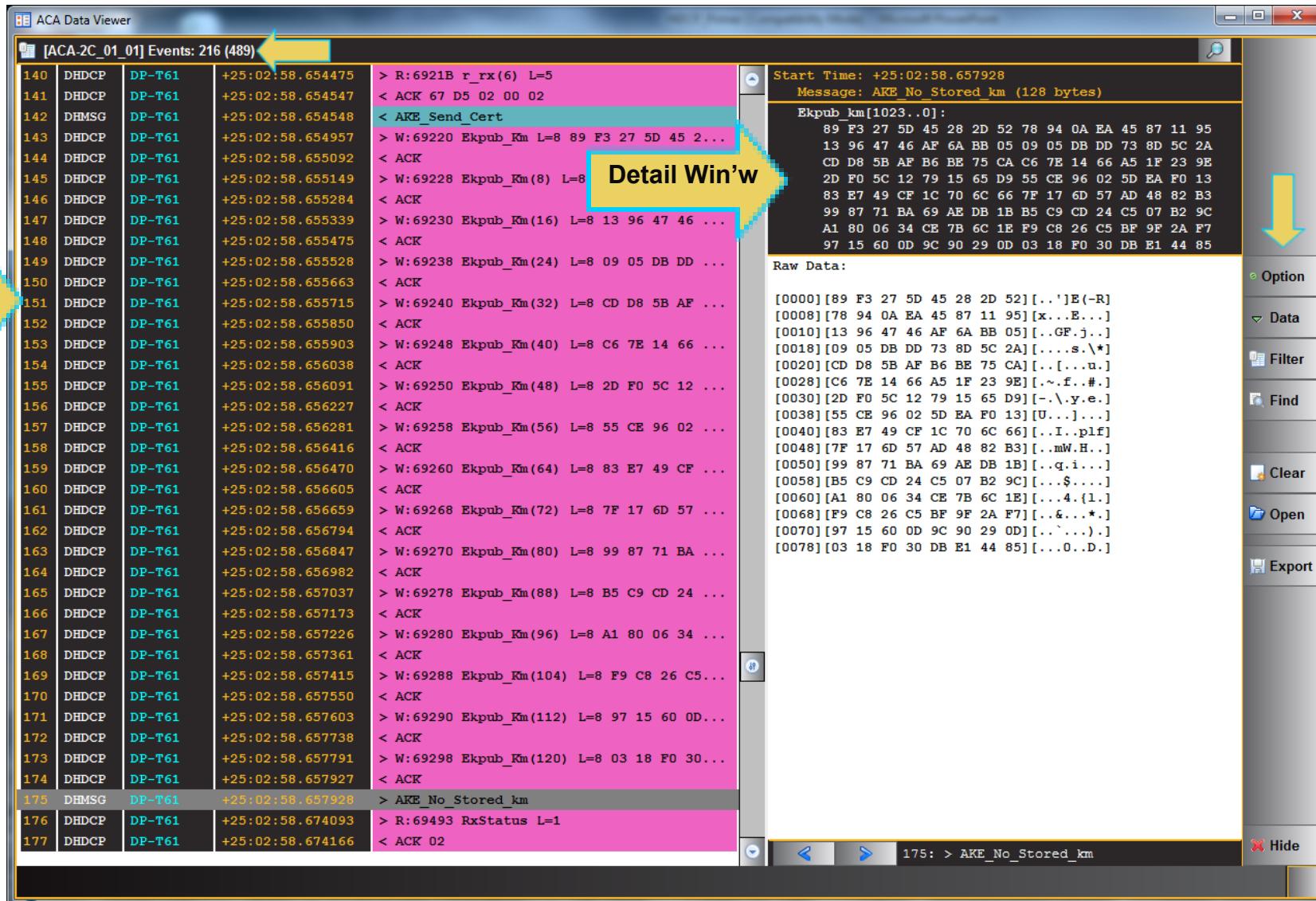


Content Encryption



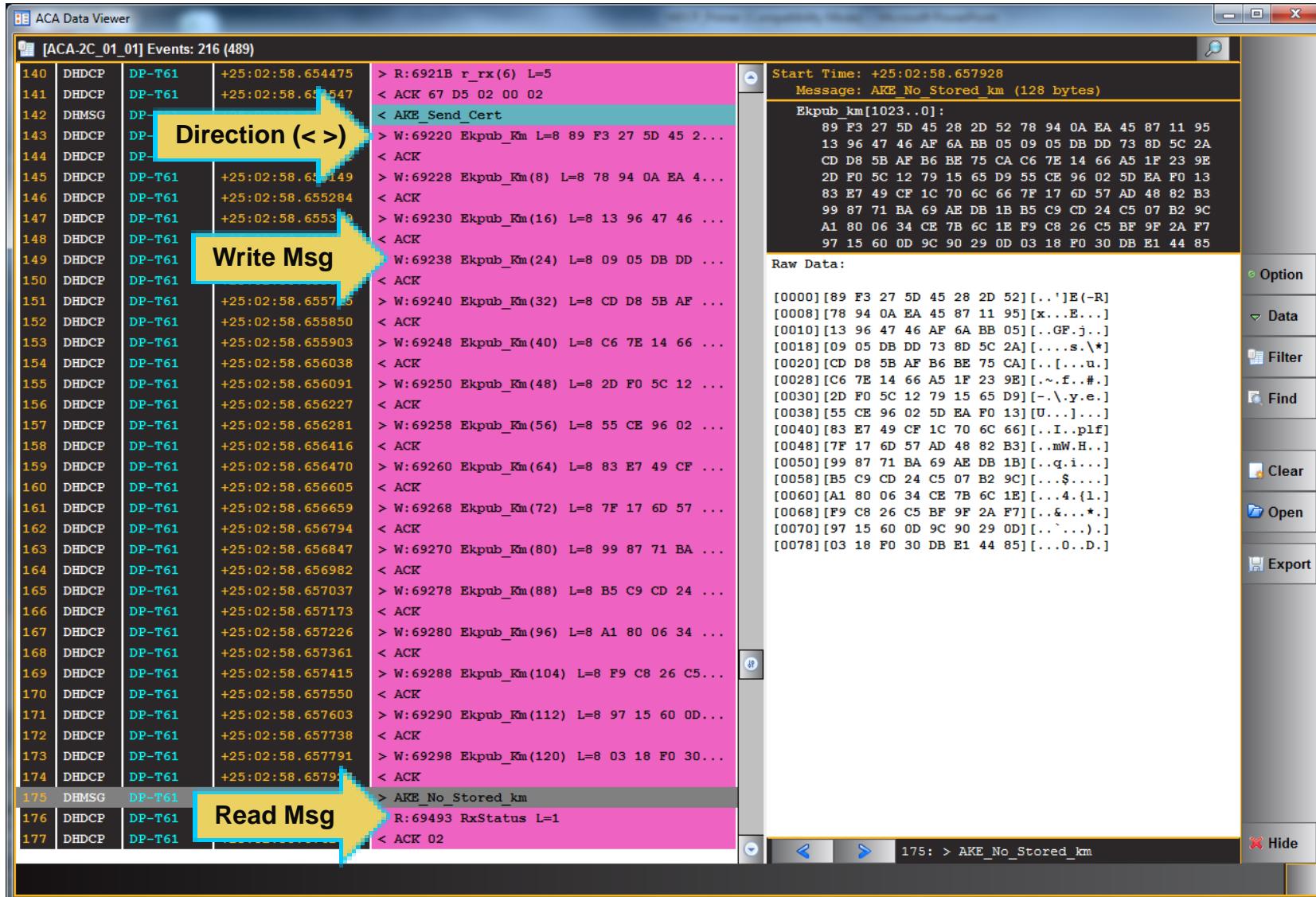
Brief Introduction to Aux Channel Protocol Analyzer

Auxiliary Channel Analyzer (ACA) Utility



- The Name of transaction log file on top banner.
- Control buttons are on the right.
- Two main panels:
 - Transaction Log Panel
 - Detail Panel (shows details for selected transaction)

Auxiliary Channel Analyzer (ACA) Utility

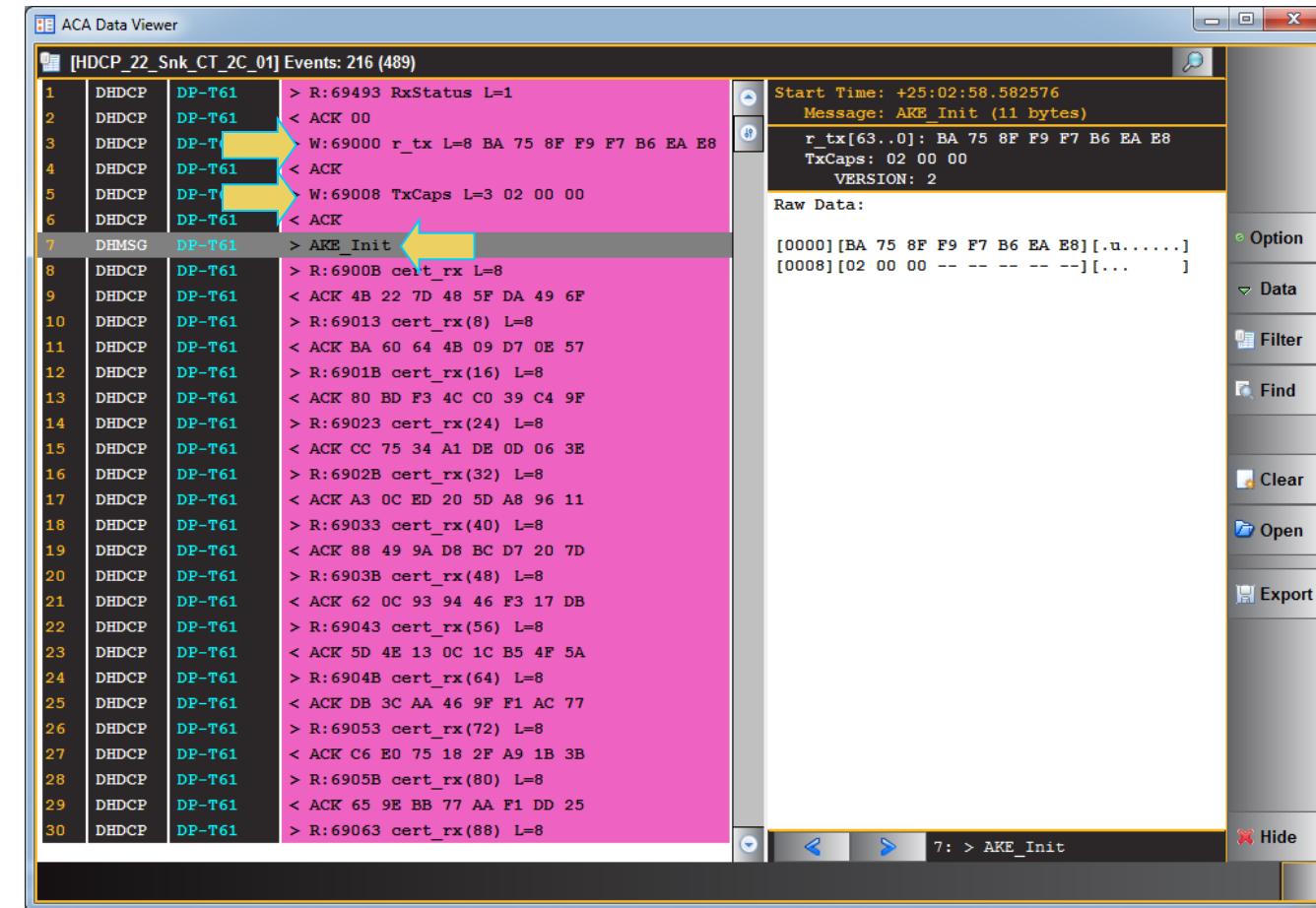
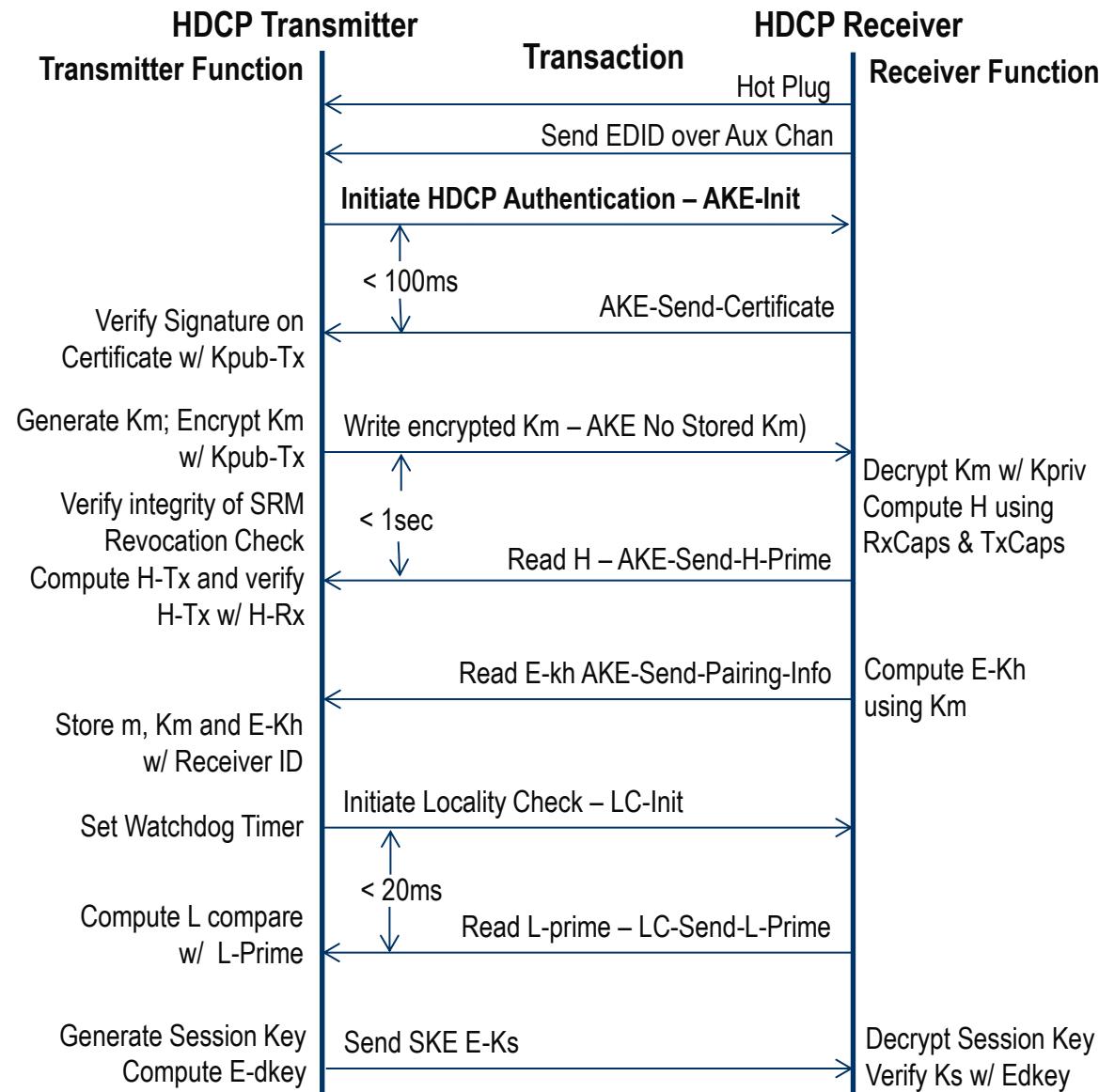


- HDCP transactions can be logged from either a 980 module's Tx port(s) or the module's Rx port.
- HDCP transactions can either be Reads ("R:") or Writes ("W:") or an acknowledgement ("ACK").
- The "<" or ">" indicate the direction of transmission from the perspective of the monitoring port. In this case the monitoring port is the 980 Tx. The > means a message going from the 980 Tx to the sink DUT.

HDCP Authentication

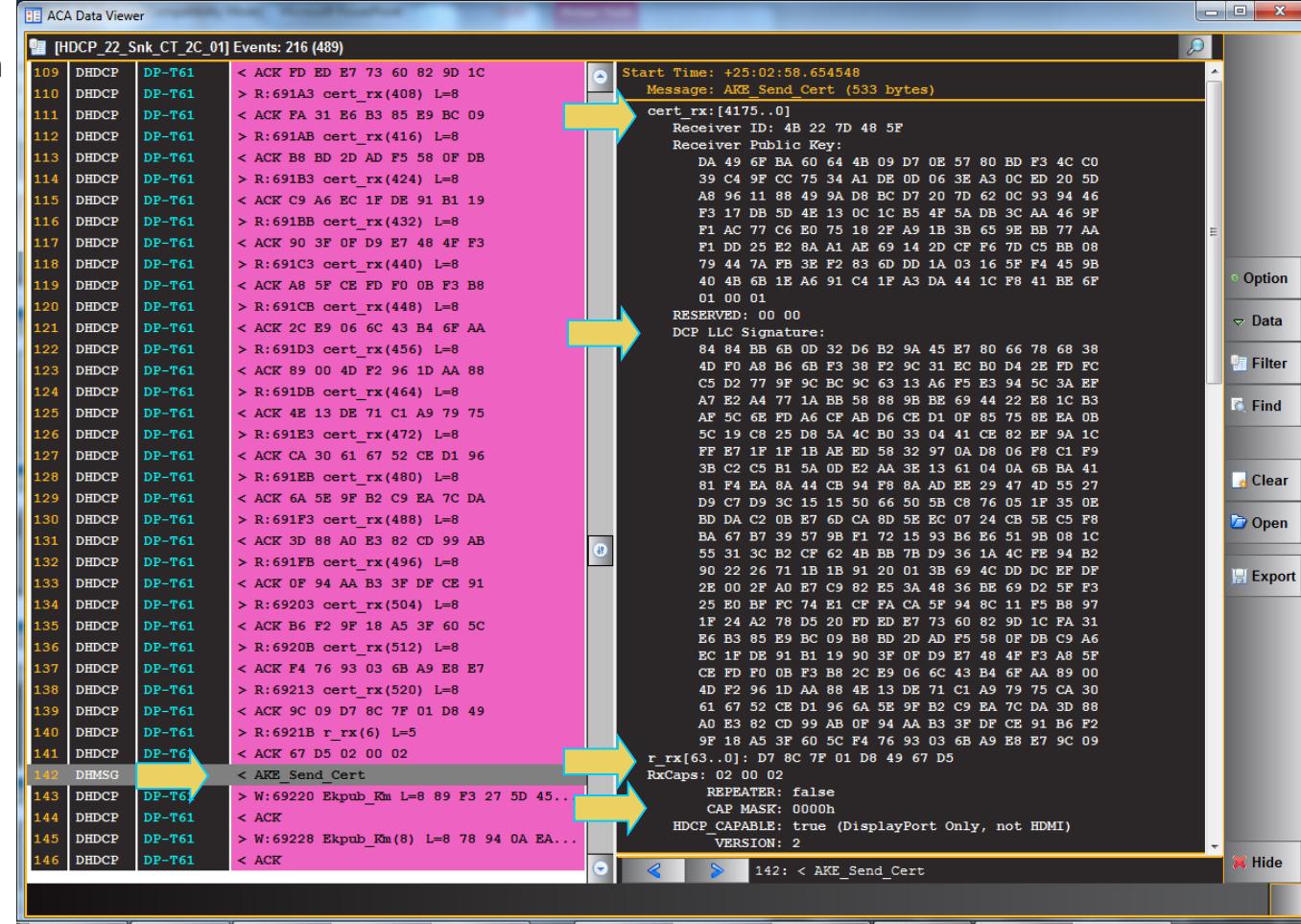
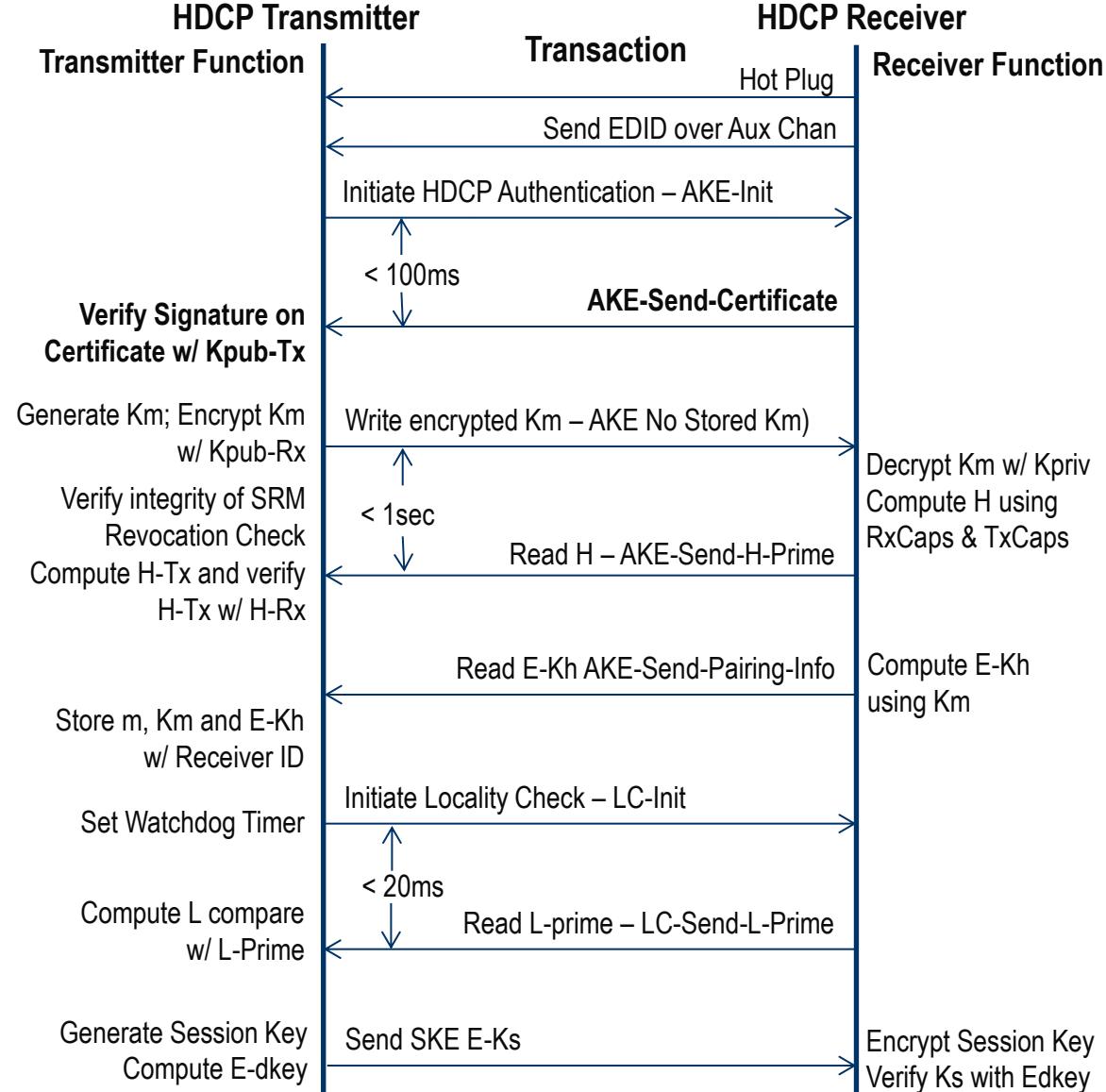
Verifying the Receiver Certificate

HDCP 2.2 Sequence – AKE Initiation, Send Random Number and TxCaps



- ◆ Transmitter initiates Authentication and Key Exchange
 - ◆ Sends R-Tx (64 bit pseudo-random number) later used in the encryption of the Master Key (Km).
 - ◆ Sends TCaps (Transmitter HDCP capabilities [Version]).

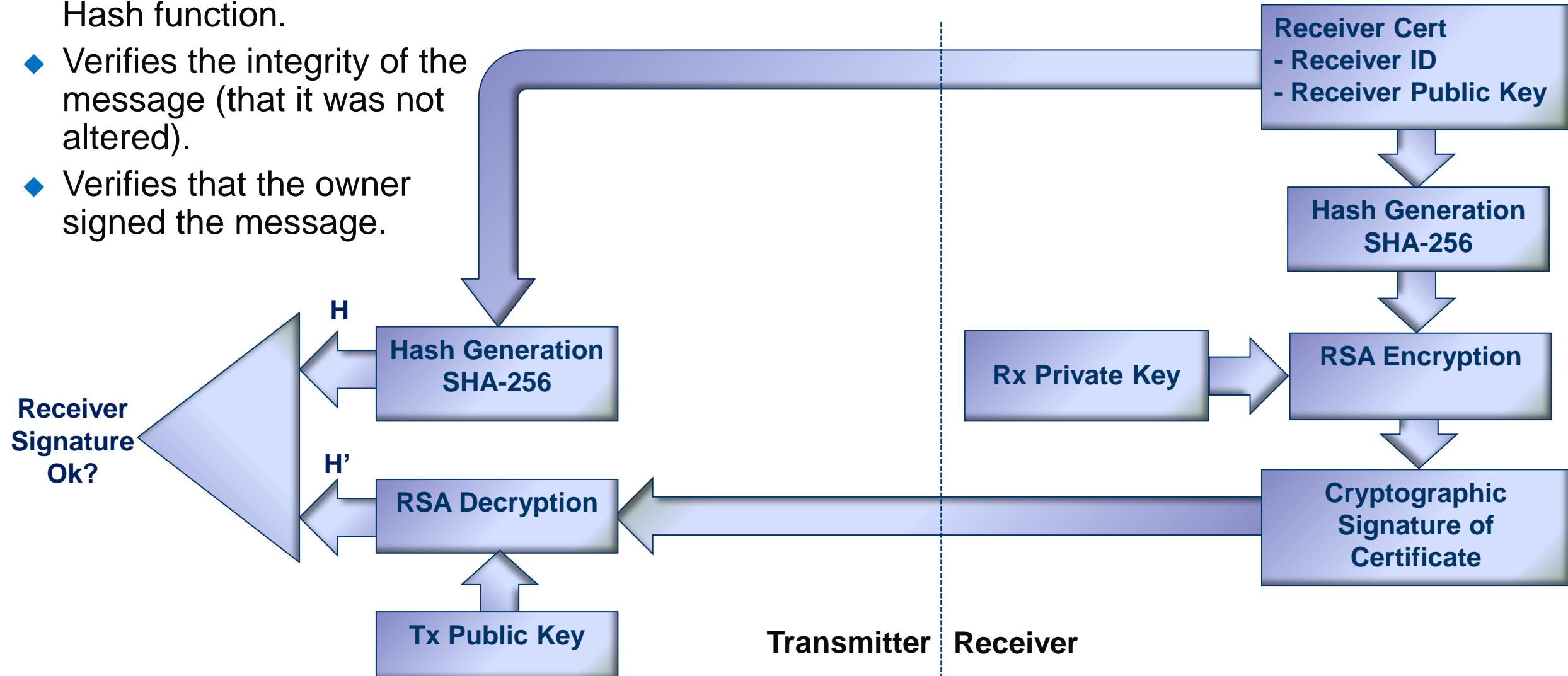
HDCP 2.2 Sequence – Transmitter Reads Receiver Certificate



- ◆ Transmitter reads Receiver Certificate. Certificate contains:
 - ◆ Receiver ID – Unique receiver ID; 40 bits: 20 ones & 20 zeros
 - ◆ Receiver Public Key – Unique 1040 bit RSA public key ($k_{pub_{rx}}$).
 - ◆ DCP signature – Calculated over all fields in certificate.

HDCP 2.2 – Verifying Signature on Receiver Certificate

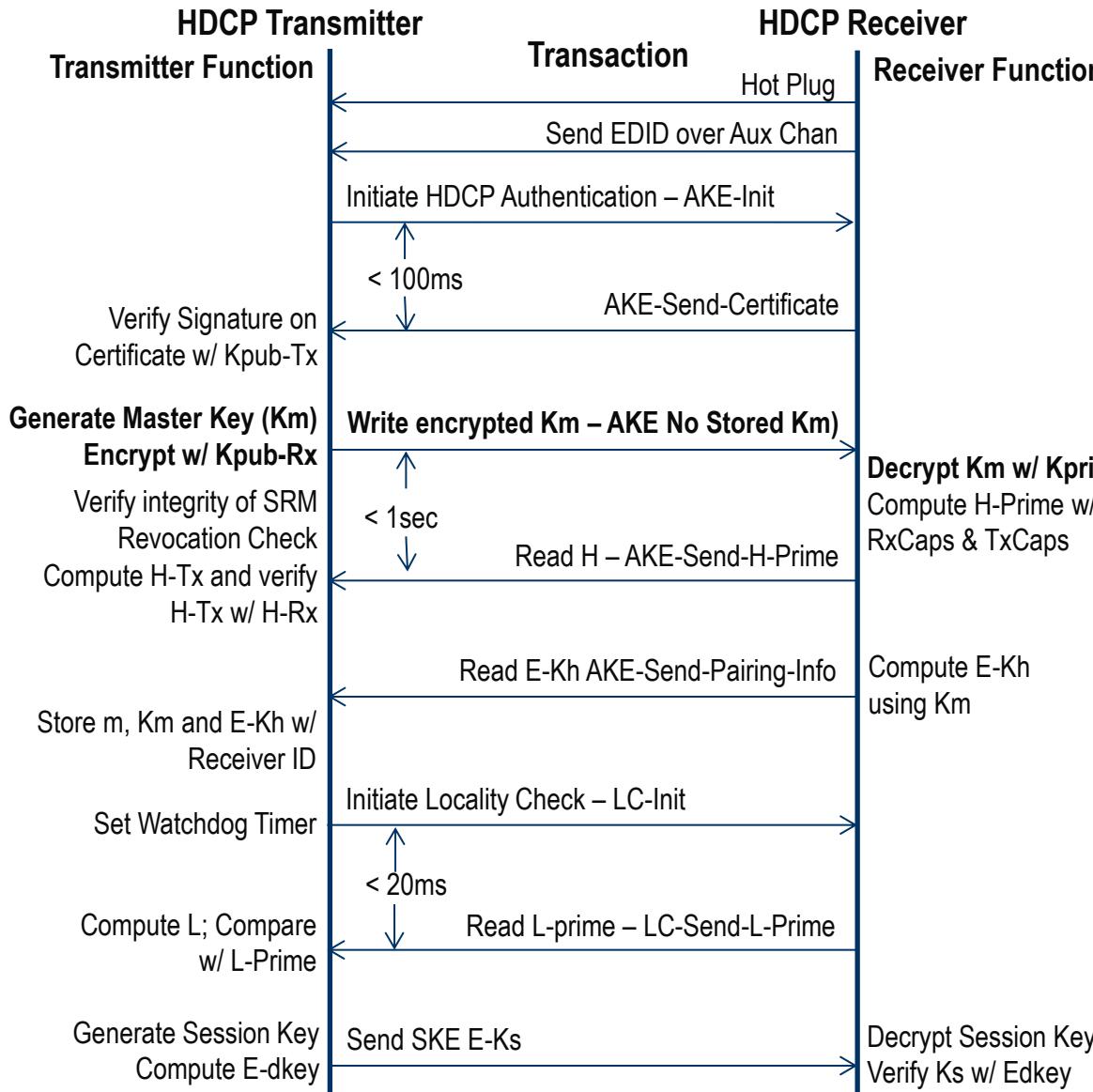
- ◆ Transmitter verifies that the Receiver's certificate is authentic using Hash function.
- ◆ Verifies the integrity of the message (that it was not altered).
- ◆ Verifies that the owner signed the message.



HDCP Authentication

Generating, Exchanging the Master Key

HDCP 2.2 Sequence – Transmitter Sends Encrypted Master Key to Receiver



ACD Data Viewer

[HDCP_22_Snk_CT_2C_01] Events: 216 (489)

Start Time: +25:02:58.657928
Message: AKE_No_Stored_km (128 bytes)

Ekpub_Km[1023..0]:
 89 F3 27 5D 45 28 2D 52 78 94 0A EA 45 87 11 95
 13 96 47 46 AF 6A BB 05 09 05 DB DD 73 8D 5C 2A
 CD D8 5B AB BE 75 CA C6 7E 14 66 A5 1F 23 9E
 2D F0 5C 12 79 15 65 D9 55 CE 96 02 5D EA F0 13
 B3 E7 49 CF 1C 70 6C 66 7F 17 6D 57 AD 48 82 B3
 99 87 71 BA 69 AB DB 1B B5 C9 CD 24 C5 07 B2 9C
 A1 80 06 34 CE 7B 6C 1E F9 C8 26 C5 BF 2A F7
 97 15 60 OD 9C 90 29 0D 03 18 F0 30 DB E1 44 85

Raw Data:

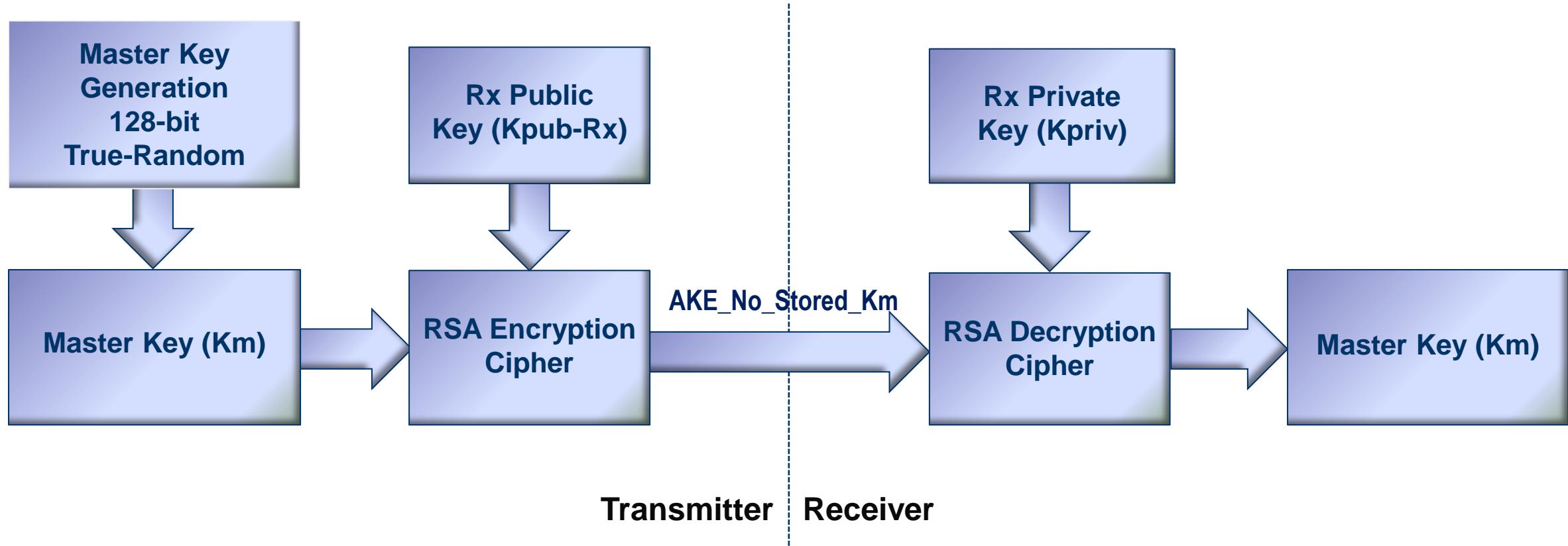
```
[0000][89 F3 27 5D 45 28 2D 52][...E(-R)
[0008][78 94 0A EA 45 87 11 95][x...E...]
[0010][13 96 47 46 AF 6A BB 05][..GF...]
[0018][09 05 DB DD 73 8D 5C 2A][...s.\*]
[0020][CD D8 5B AB BE 75 CA][...u...]
[0028][C6 7E 14 66 A5 1F 23 9E][~.f.#]
[0030][2D F0 5C 12 79 15 65 D9][~.y.e.]
[0038][55 CE 96 02 5D EA F0 13][U...]
[0040][83 E7 49 CF 1C 70 6C 66][..I.,plf]
[0048][7F 17 6D 57 AD 48 82 B3][..W.H.]
[0050][99 87 71 BA 69 AB DB 1B][..q.i...]
[0058][B5 C9 CD 24 C5 07 B2 9C][...$...]
[0060][A1 80 06 34 CE 7B 6C 1E][..4.(1.]
[0068][F9 C8 26 C5 BF 9F 2A F7][..5.*.]
[0070][97 15 60 OD 9C 90 29 0D][...]
[0078][03 18 F0 30 DB E1 44 85][...0.D.]
```

175: > AKE_No_Stored_km

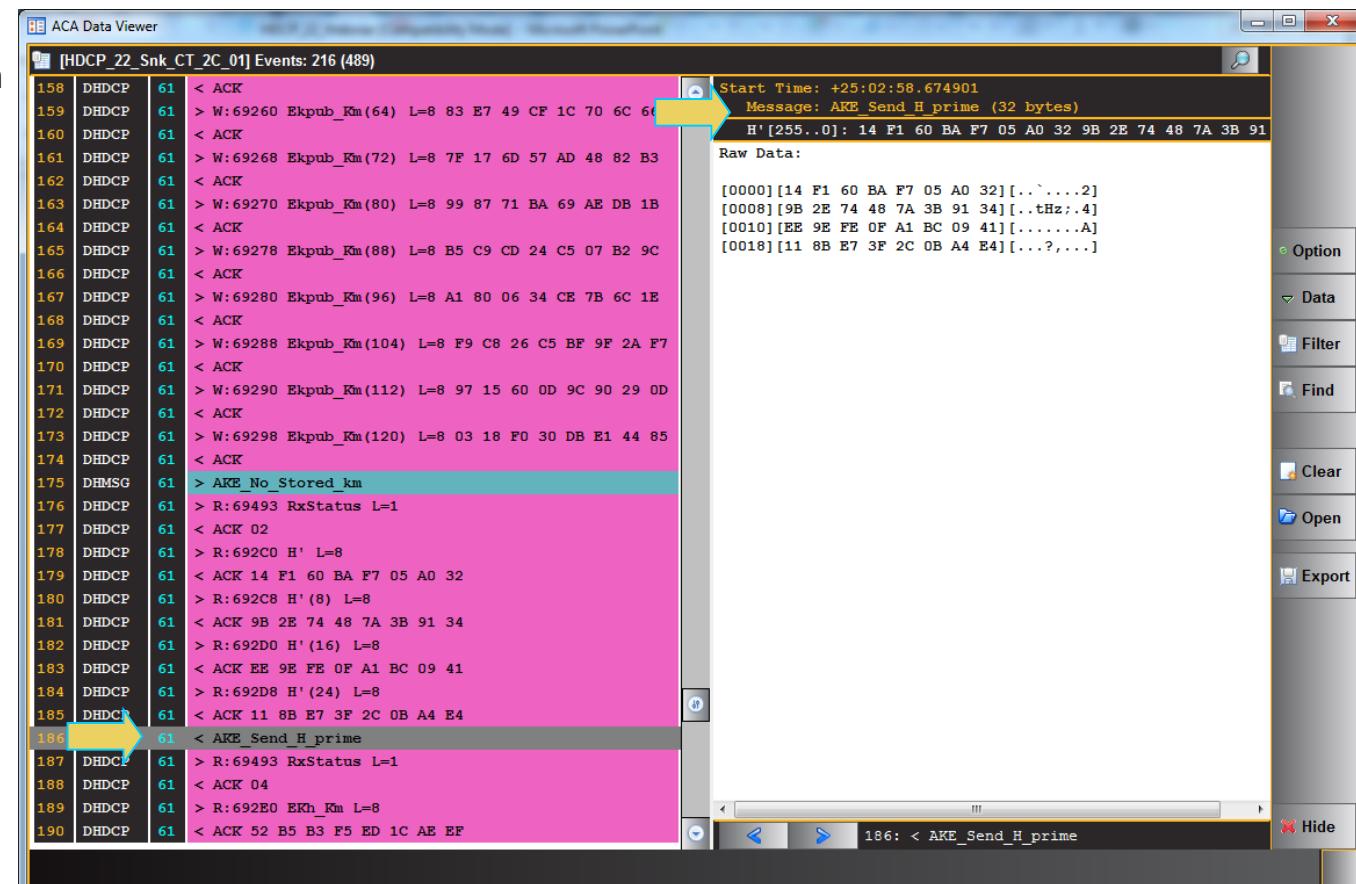
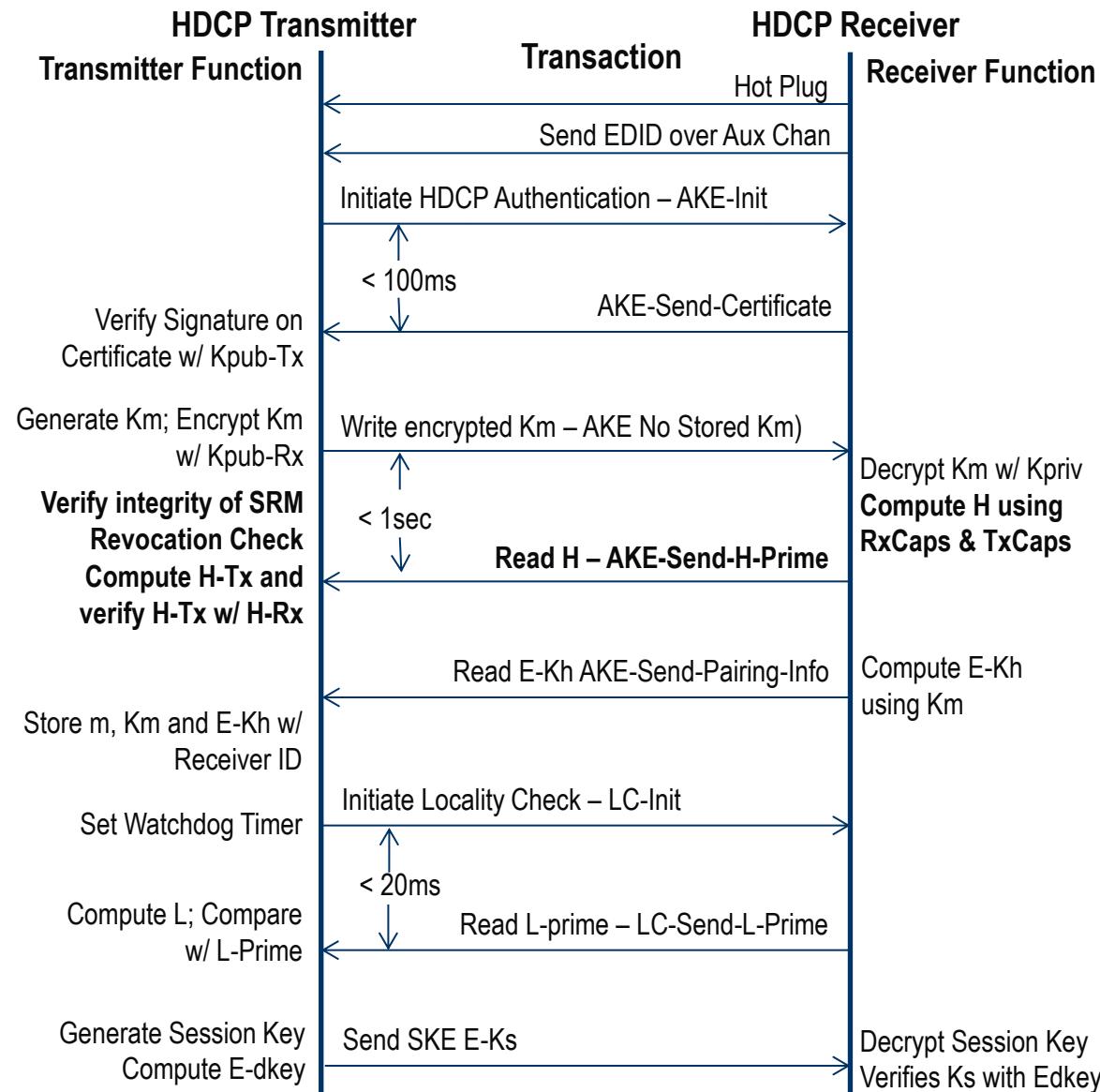
- Transmitter writes Ekpub_Km message with Master Key to Receiver (since there is no stored Master Key [Km]):

HDCP 2.2 – Generating, Encrypting and Exchanging Master Key

- ◆ Master Key (K_m) is a 128-bit key produced by the Transmitter's True-random number generator.
- ◆ Master Key is encrypted with the Receiver's public key and sent to the Receiver.



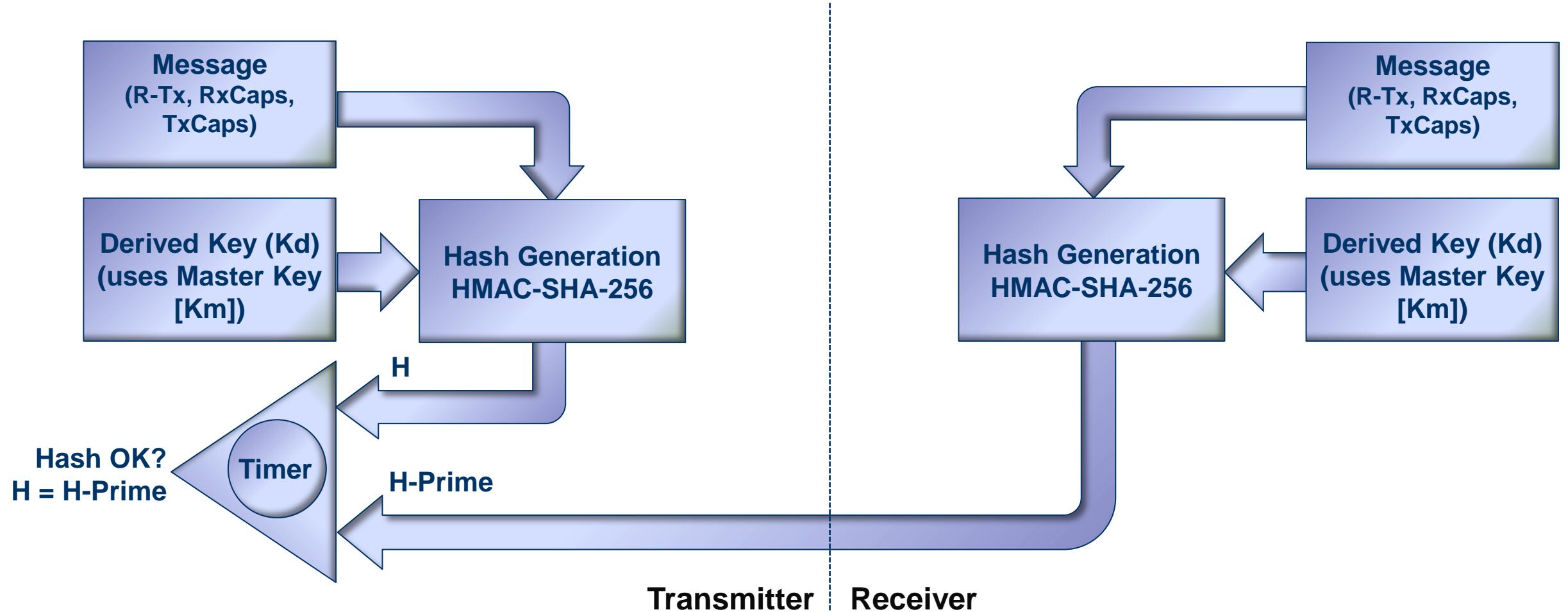
HDCP 2.2 Sequence – Transmitter Reads Receiver H-Prime



- Transmitter reads Receiver's H-Prime.
- This verifies the integrity of the Master Key, i.e. that it was received and decrypted properly.

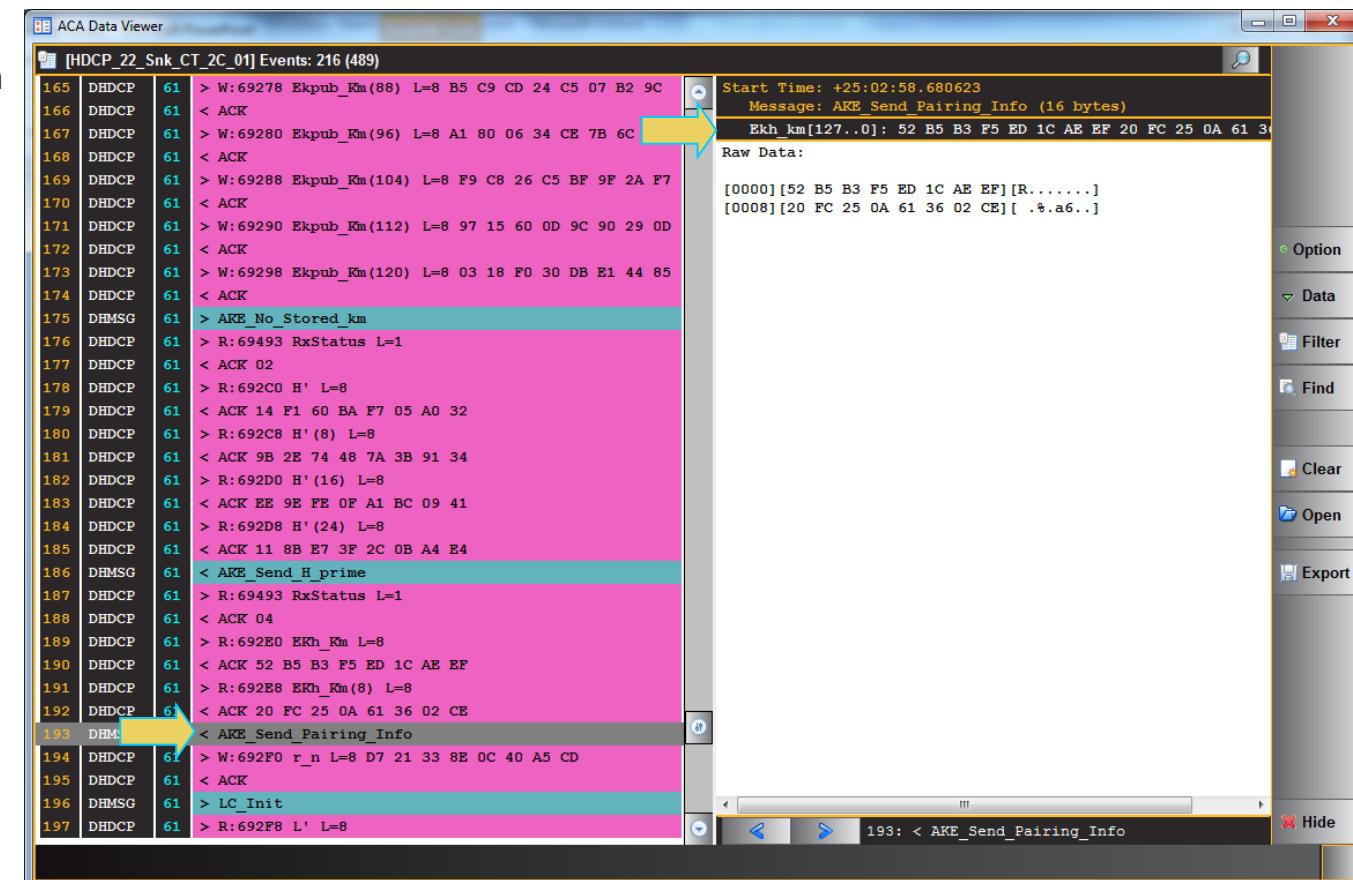
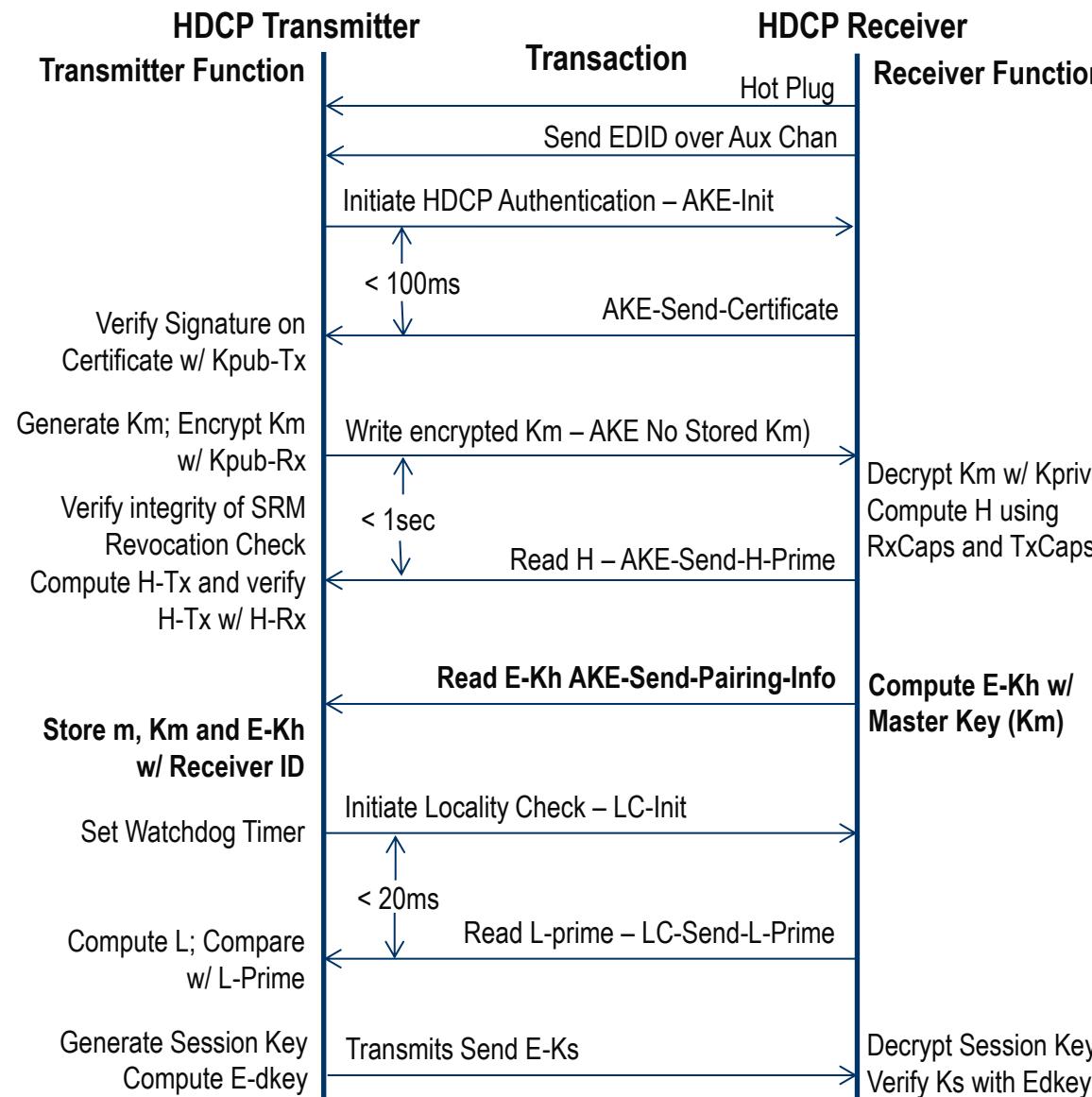
HDCP 2.2 – Verifying Master Key Exchange & Integrity with H=H-Prime

- ◆ Master Key is verified by using it on both the Transmitter and Receiver in a hash function to hash a message comprised of RTx, RxCaps and TxCaps.



HDCP Authentication Pairing

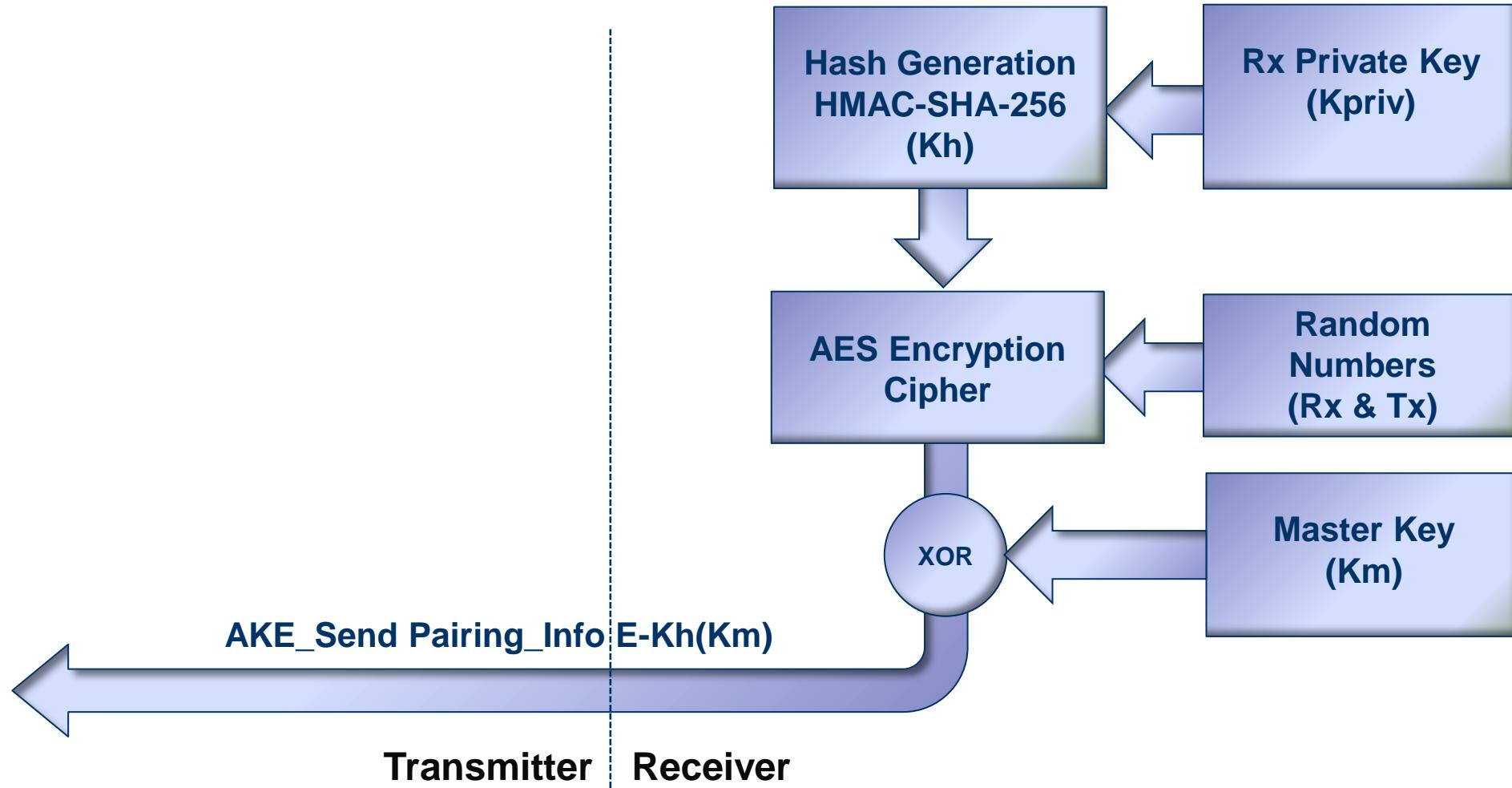
HDCP 2.2 Sequence – Transmitter Reads Pairing Info



◆ Transmitter reads Receiver's E-Kh AKE Send Pairing info.

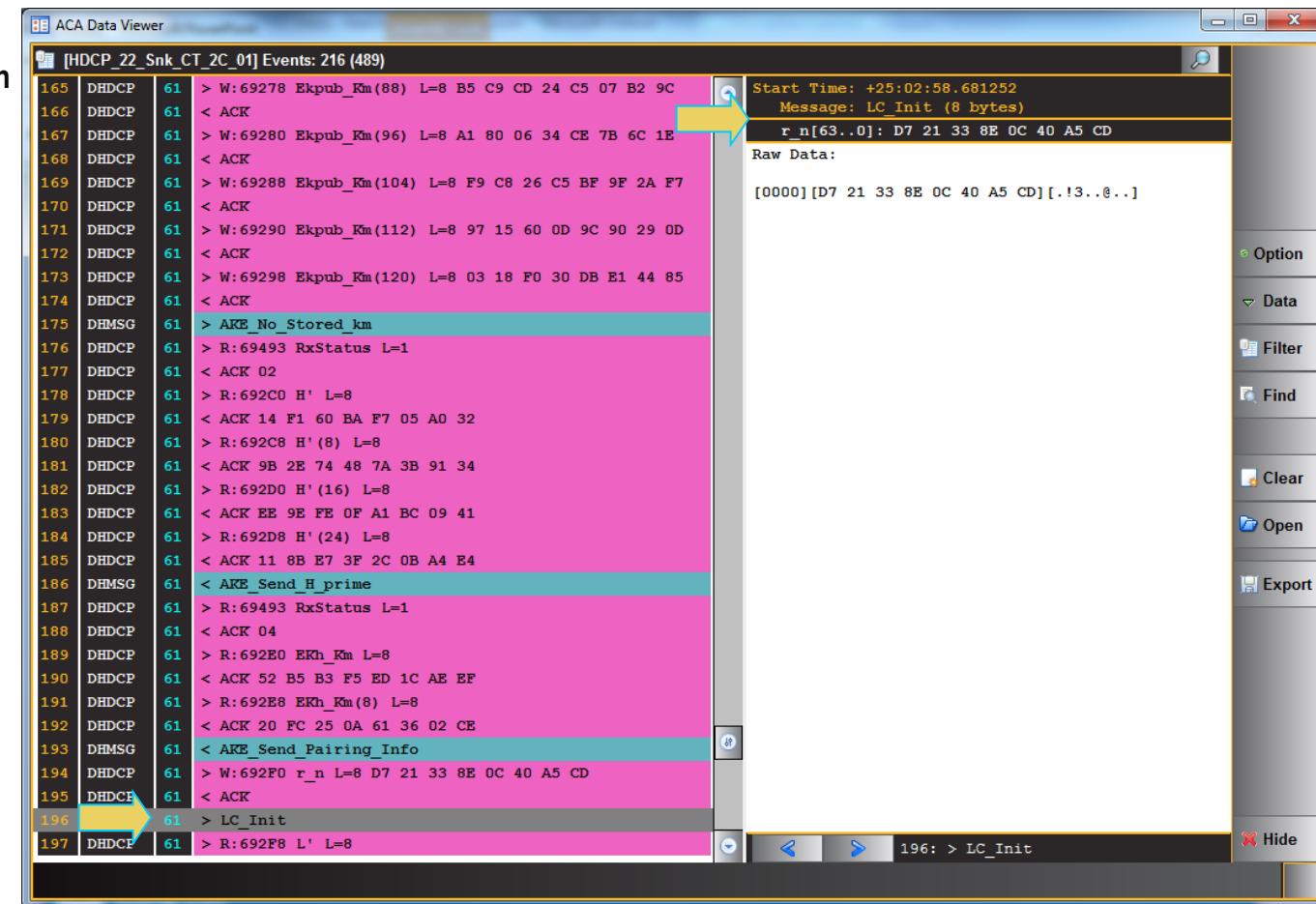
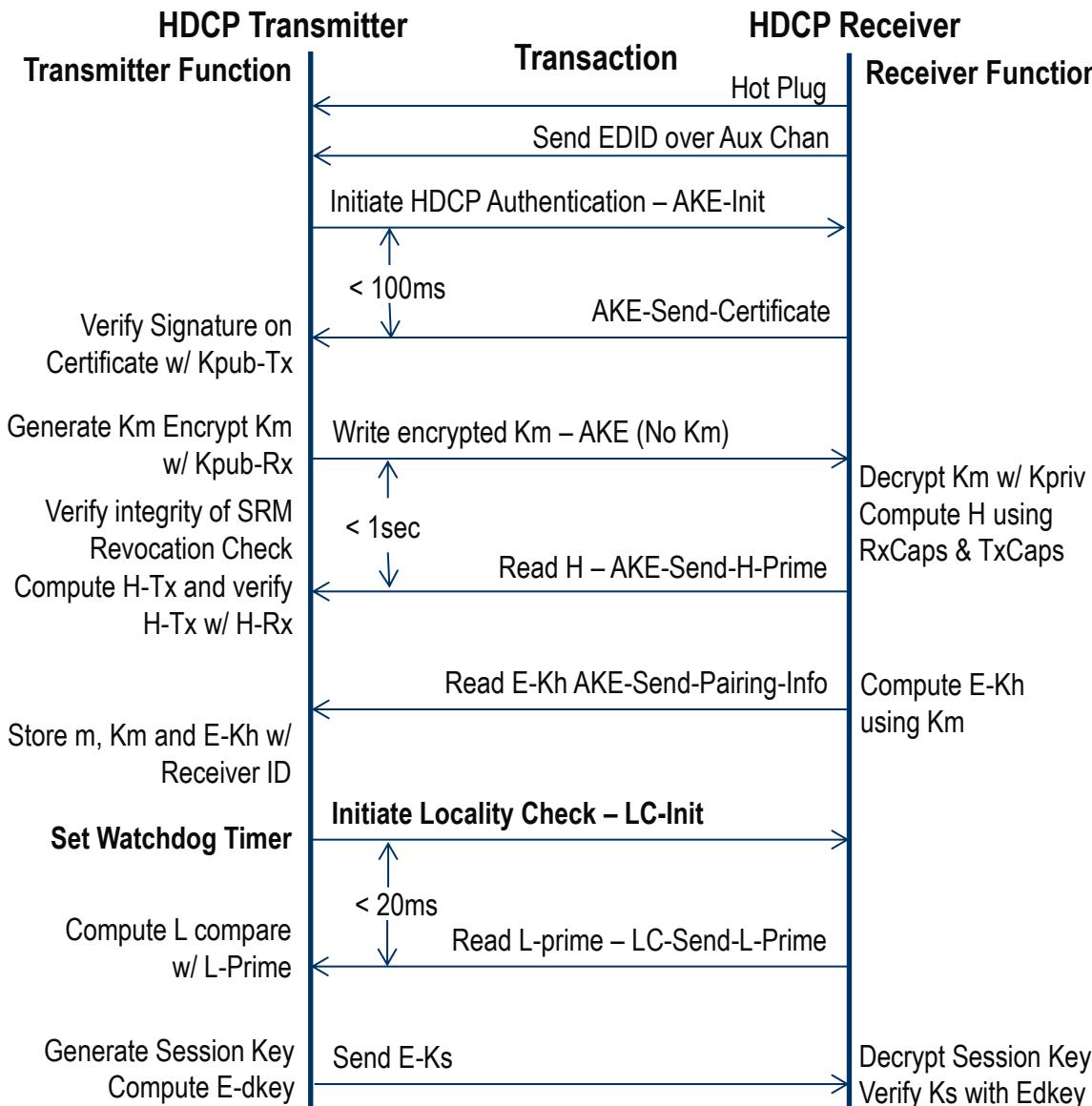
HDCP 2.2 – Master Key Storage for Pairing

- ◆ Master Key (K_m) is encrypted by Receiver and sent to Transmitter for storing to support pairing the next time these two devices authenticate together.



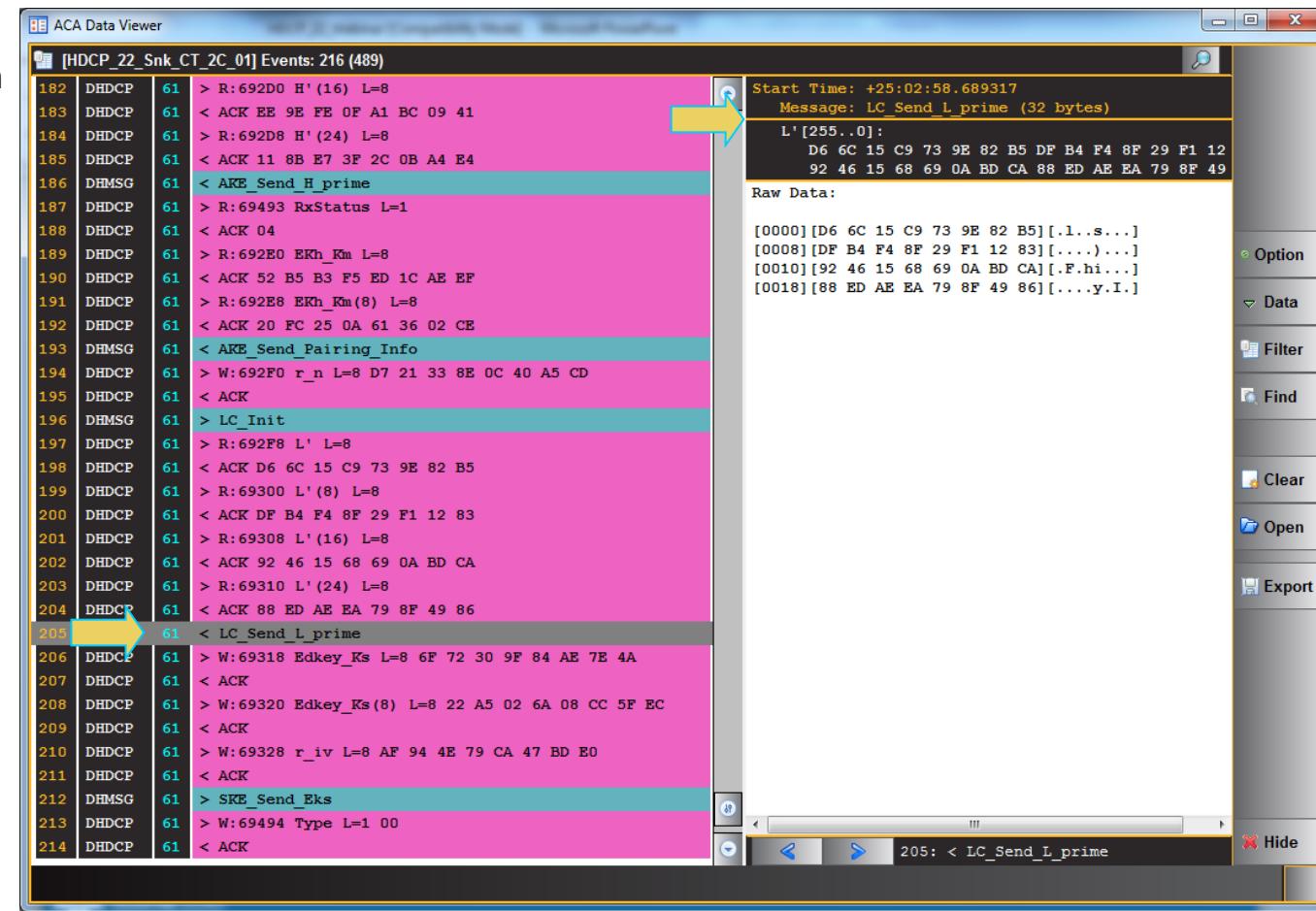
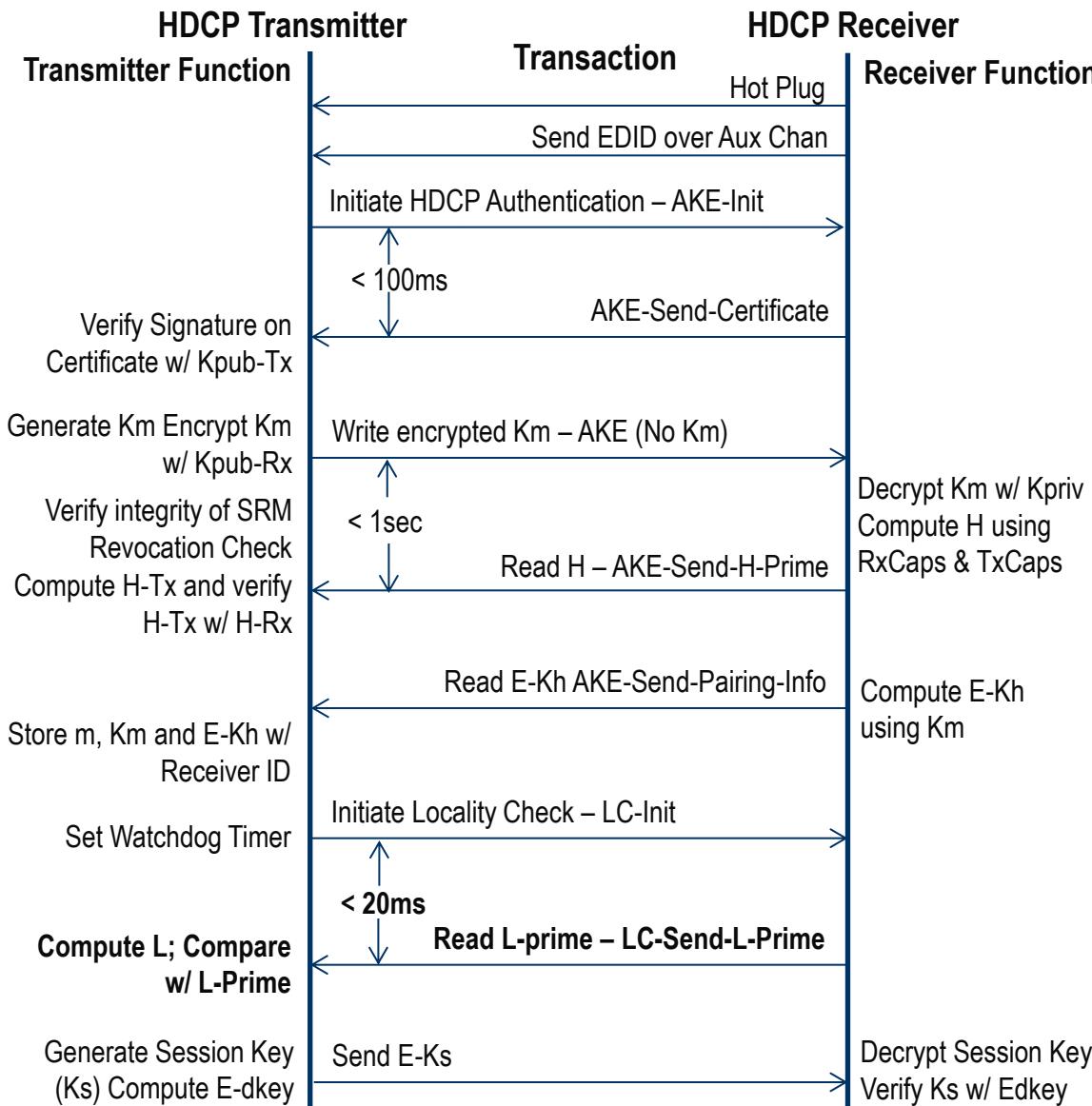
HDCP Authentication Locality Check

HDCP 2.2 Sequence – Transmitter Initiates Locality Check



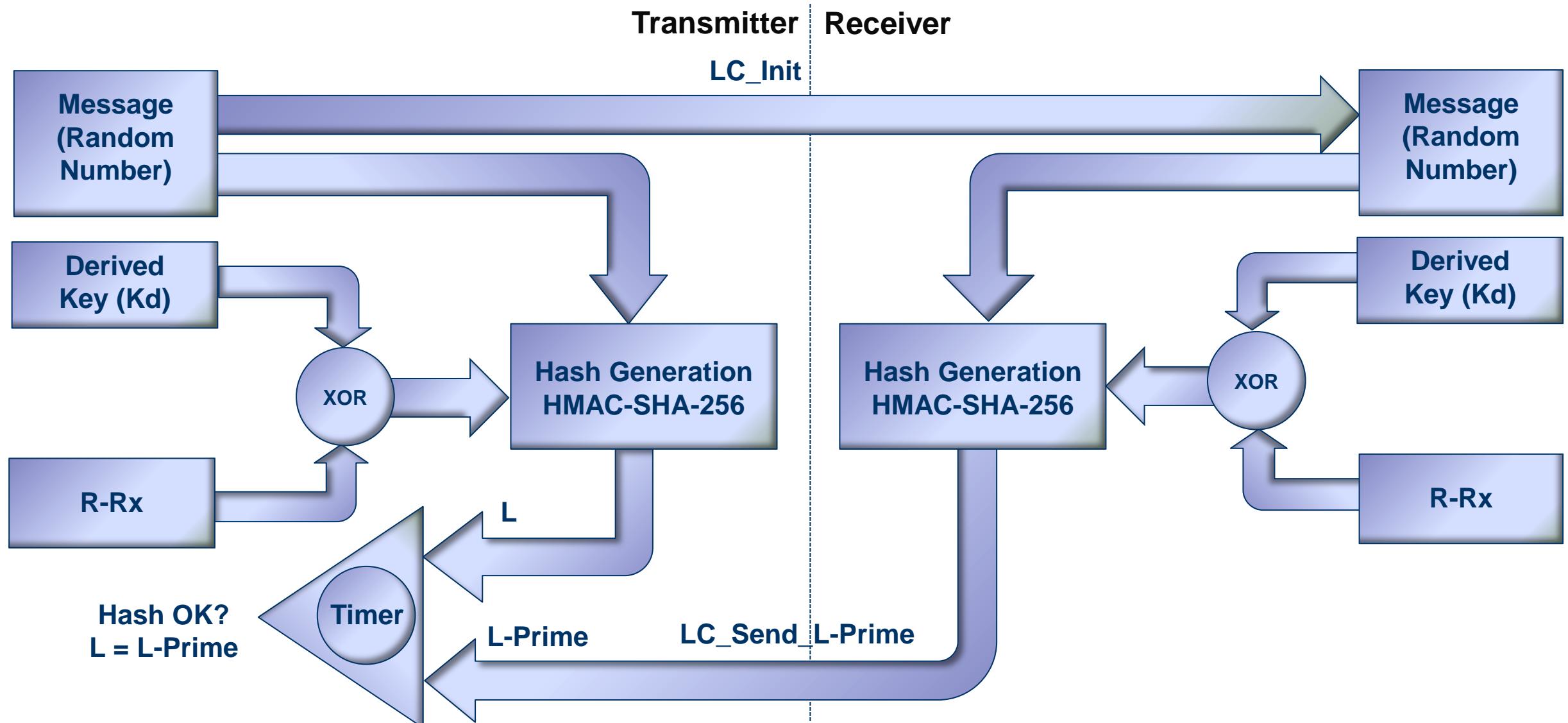
- Transmitter initiates Locality Check.
- Transmitter sends a random number (Rn) to the Receiver.
- Transmitter sets a timer.

HDCP 2.2 Sequence – Transmitter Verifies Locality



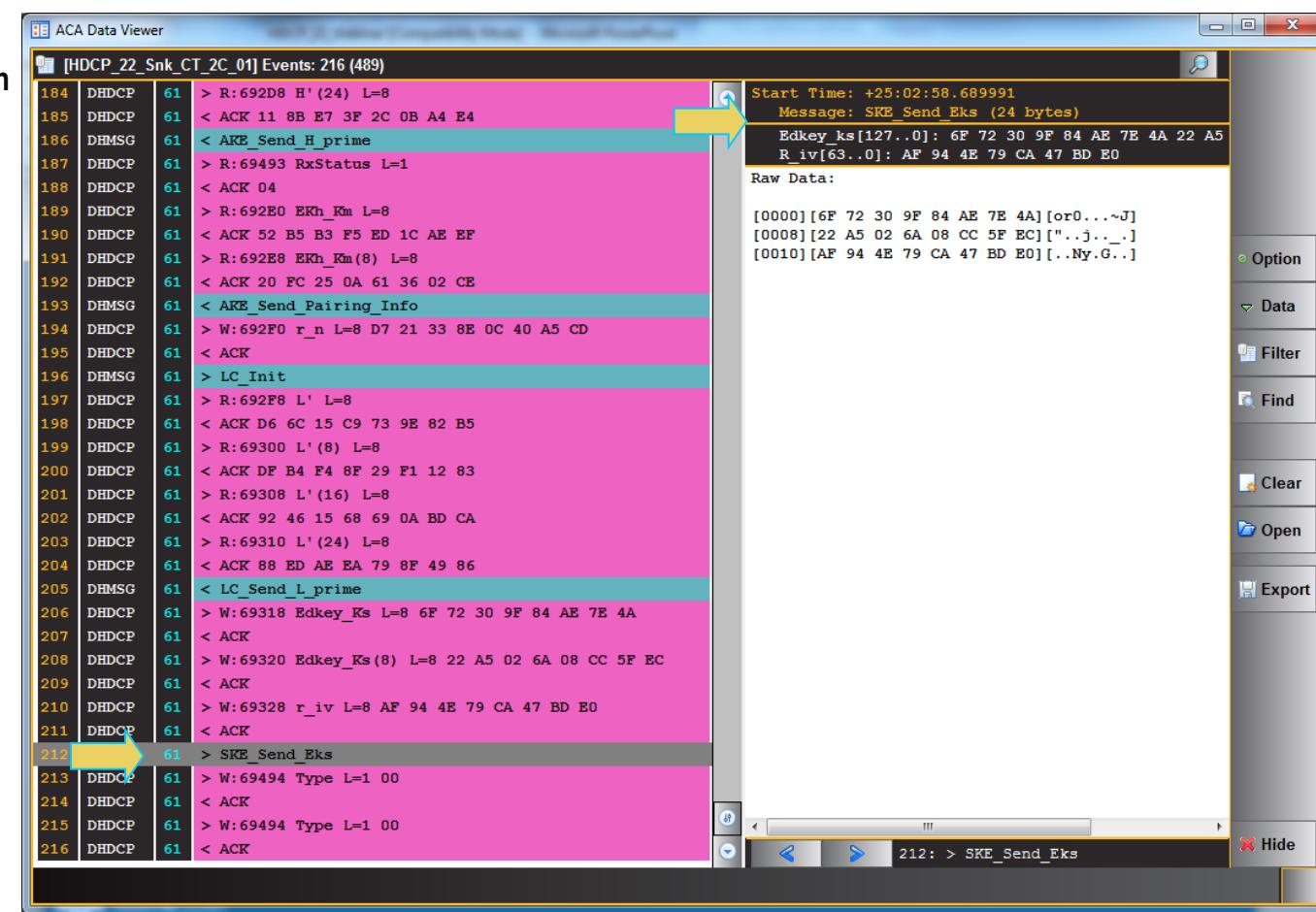
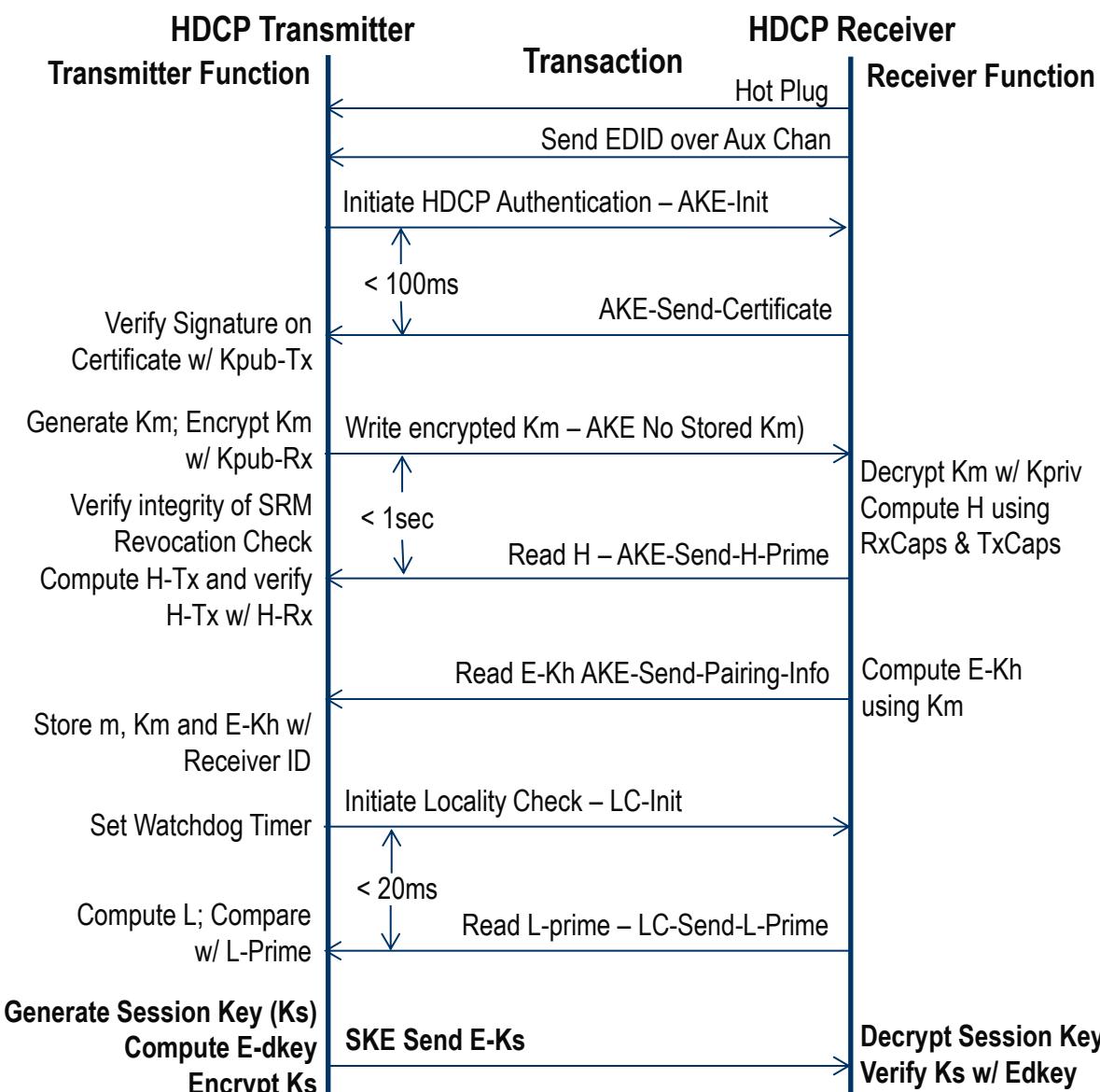
- Transmitter checks for an L-Prime (256-bit number) by comparing it to its L value (256-bit number).
- Verifies that L Prime is return within 20 msec.
- L and L-Prime are generated from the Rn with Hash SHA-256.

HDCP 2.2 Sequence – Transmitter Verifies Locality



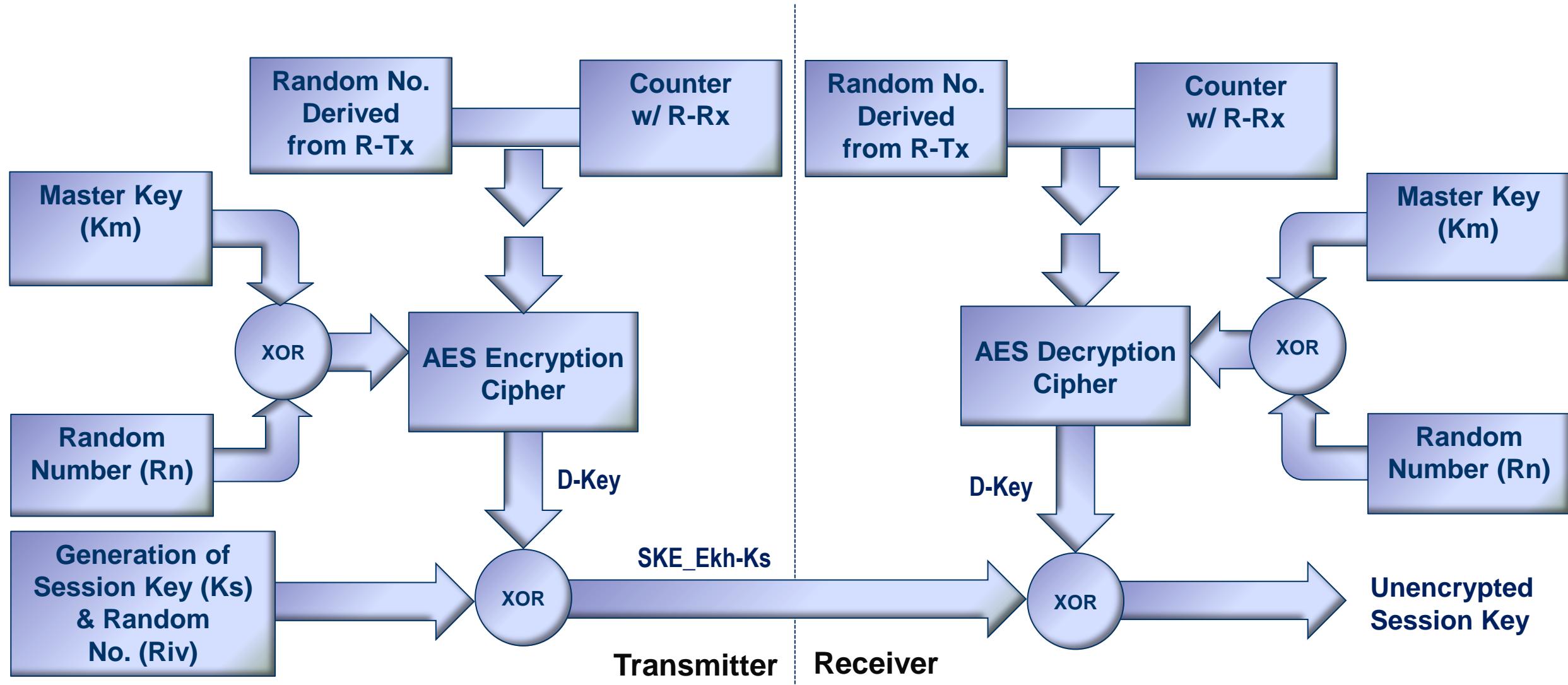
HDCP Session Key Exchange

HDCP 2.2 Sequence – Session Key Generation and Exchange



- Transmitter generates random Session Key (Ks).
- The Session Key is AES-encrypted using Master Key (Km)
- Transmitter sends Session Key (Km) to Receiver with a pseudo-random number (Riv) in SKE E-Ks write message.

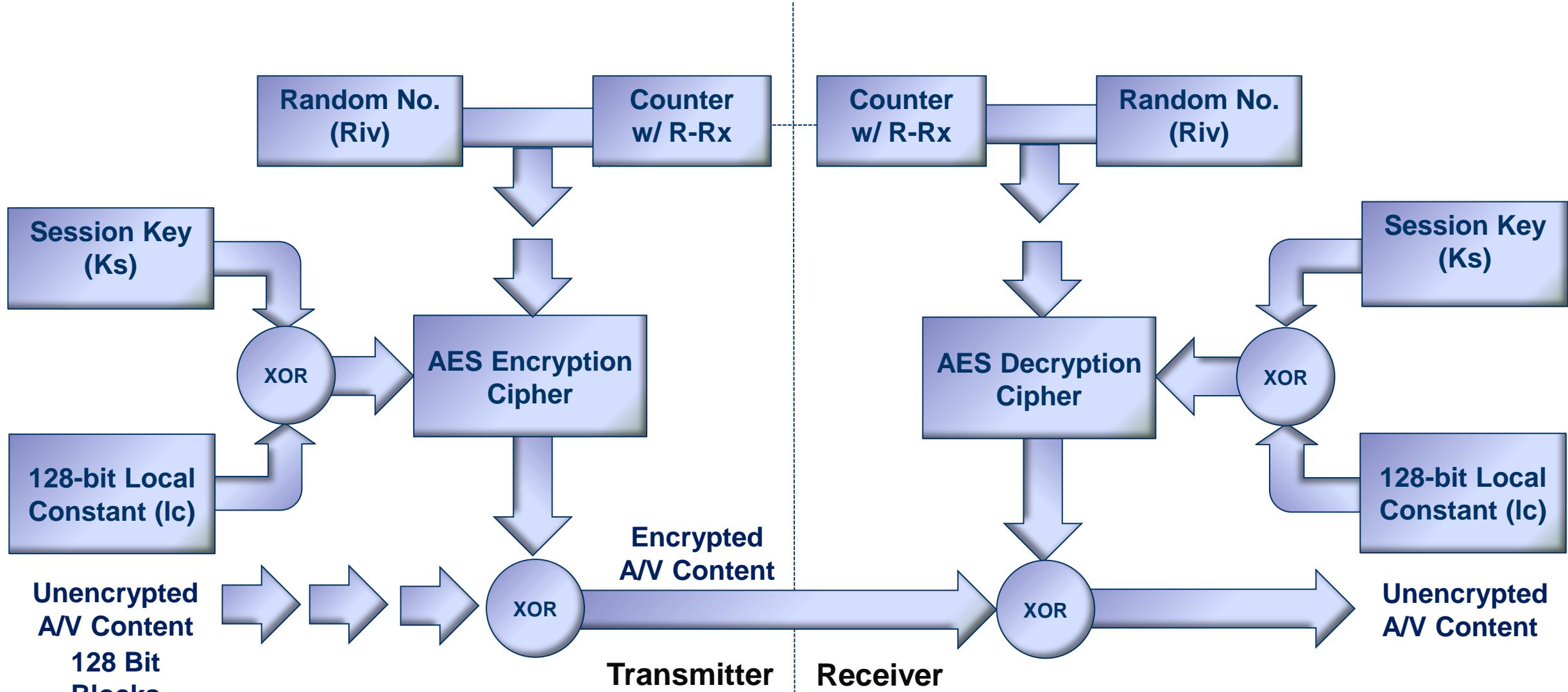
HDCP 2.2 – Session Key Generation, Encryption and Exchange



HDCP 2.2 Encryption



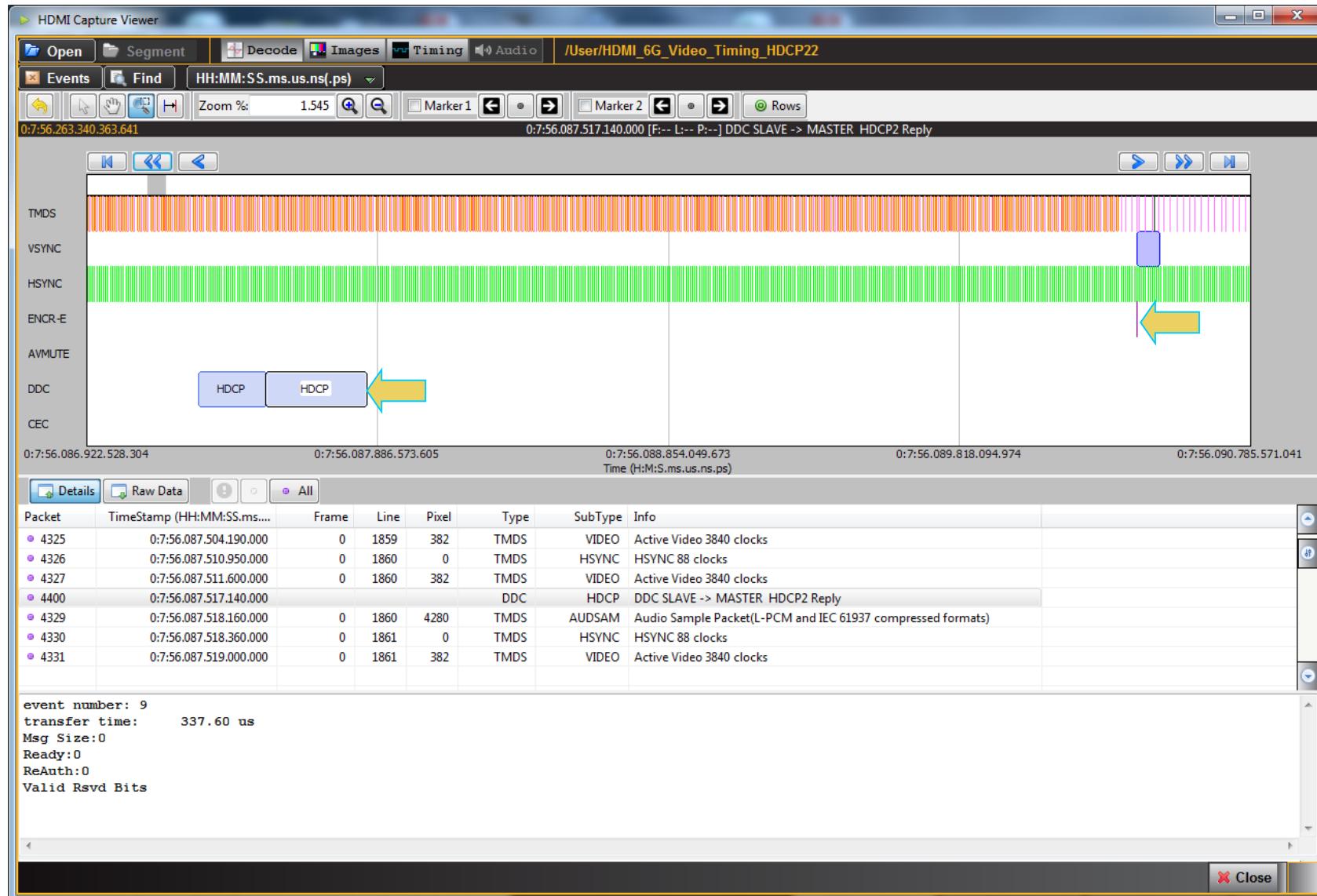
HDCP 2.2 – A/V Content Encryption



HDCP Encryption Status Signaling (HDMI)

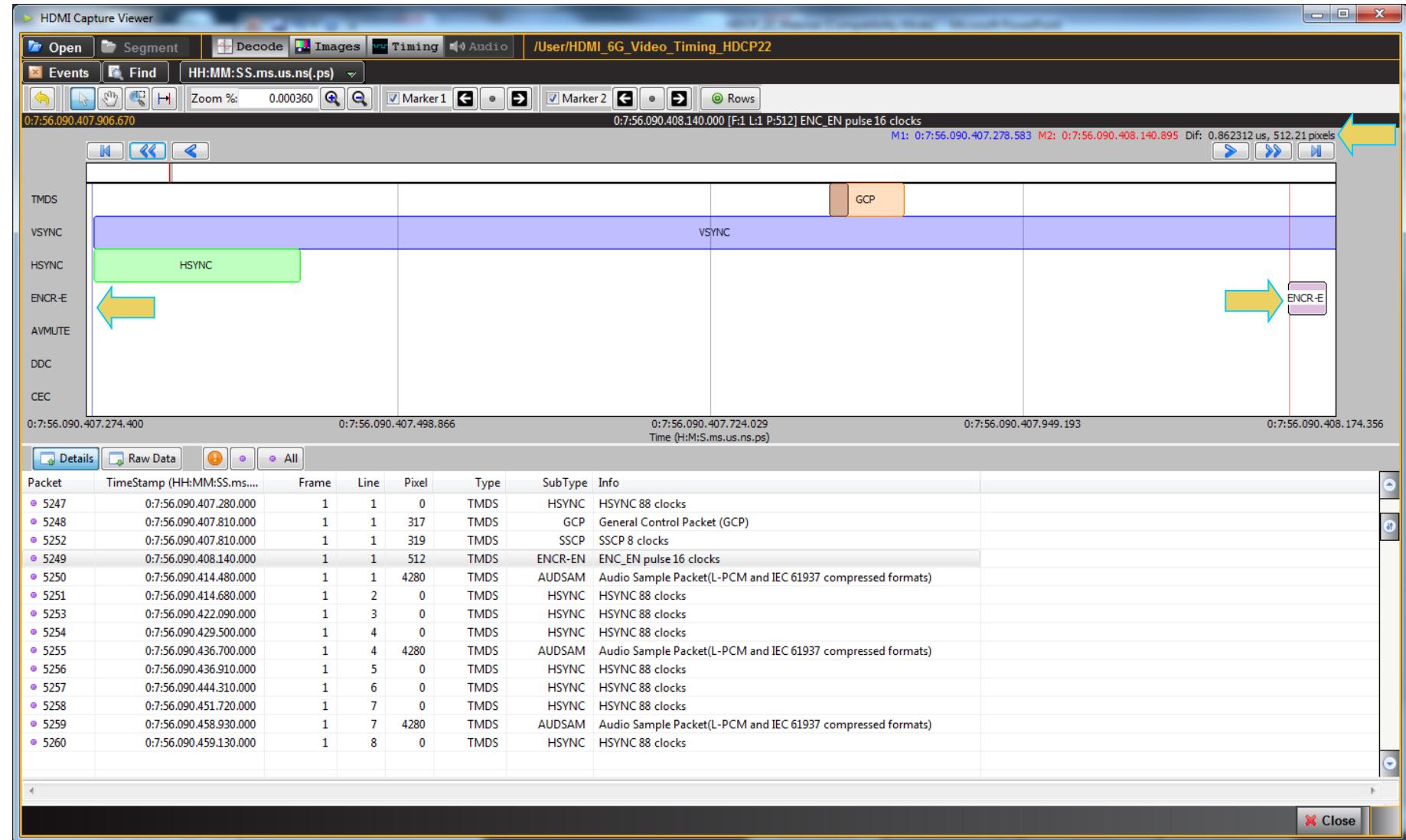
- ◆ HDCP Transmitter indicates to the Receiver to begin decrypting of the HDCP protected incoming stream using the Encryption Control Signals (CTL3, CTL2, CTL1, CTL0).
 - ◆ These signals (Encryption Enable Pulse) must be transmitted within a 16-clock “Window of Opportunity” starting at 512 pixel clocks following the active edge of Vsync.
- ◆ “Keep out Period” (Applies to HDMI)
 - ◆ No Data Islands (e.g. InfoFrames, Audio, Control Data) or Video data should be transmitted during this “Keep out Period” starting from 508th pixel after the active edge of Vsync and continuing to 650 pixels after the active edge of Vsync.

HDCP 2.2 Encryption Enable Pulse (HDMI)



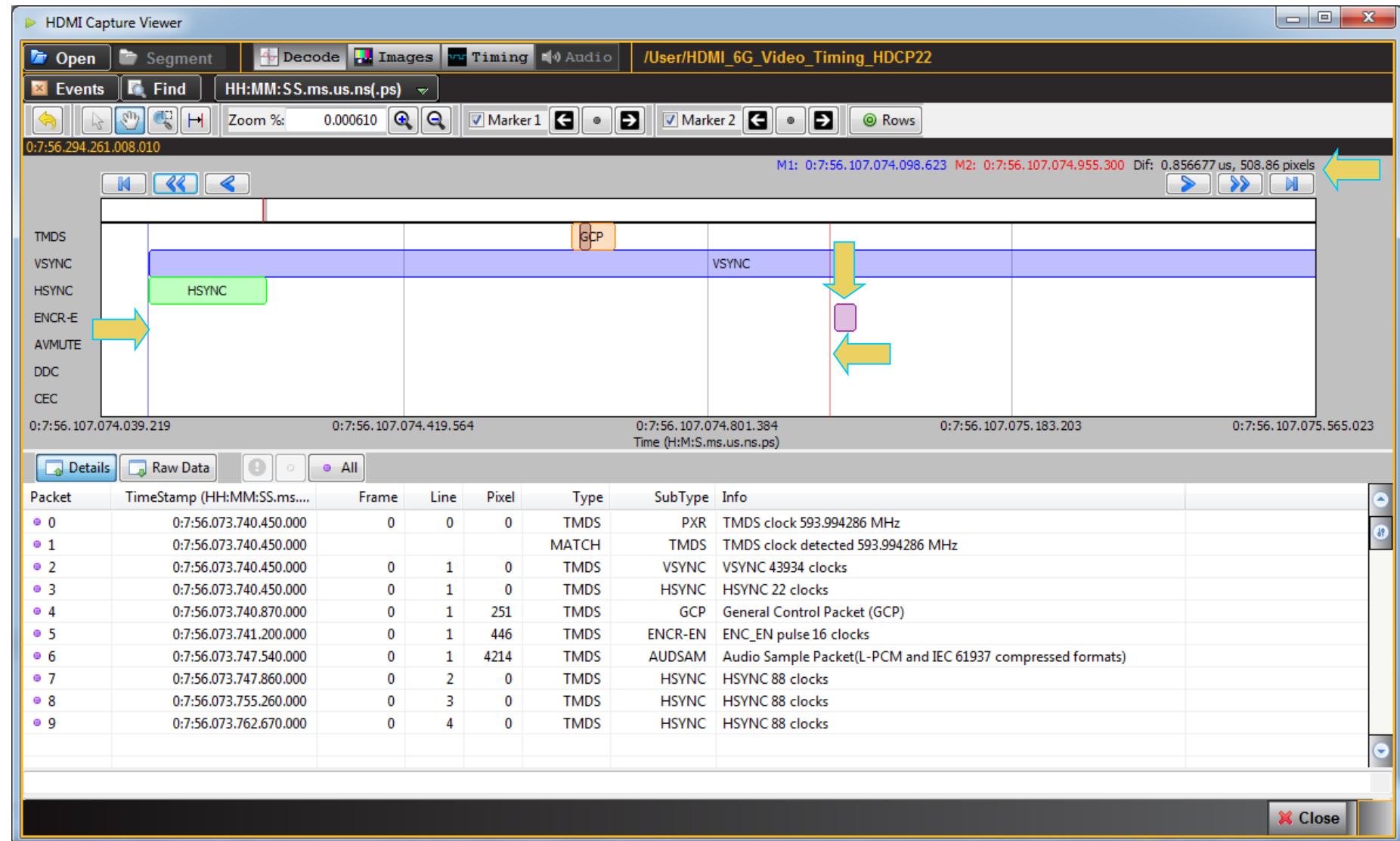
- ◆ HDMI-HDCP stream indicating Video, Encryption Enable Pulse and HDCP authentication messages.

HDCP 2.2 Encryption Enable Pulse (HDMI)



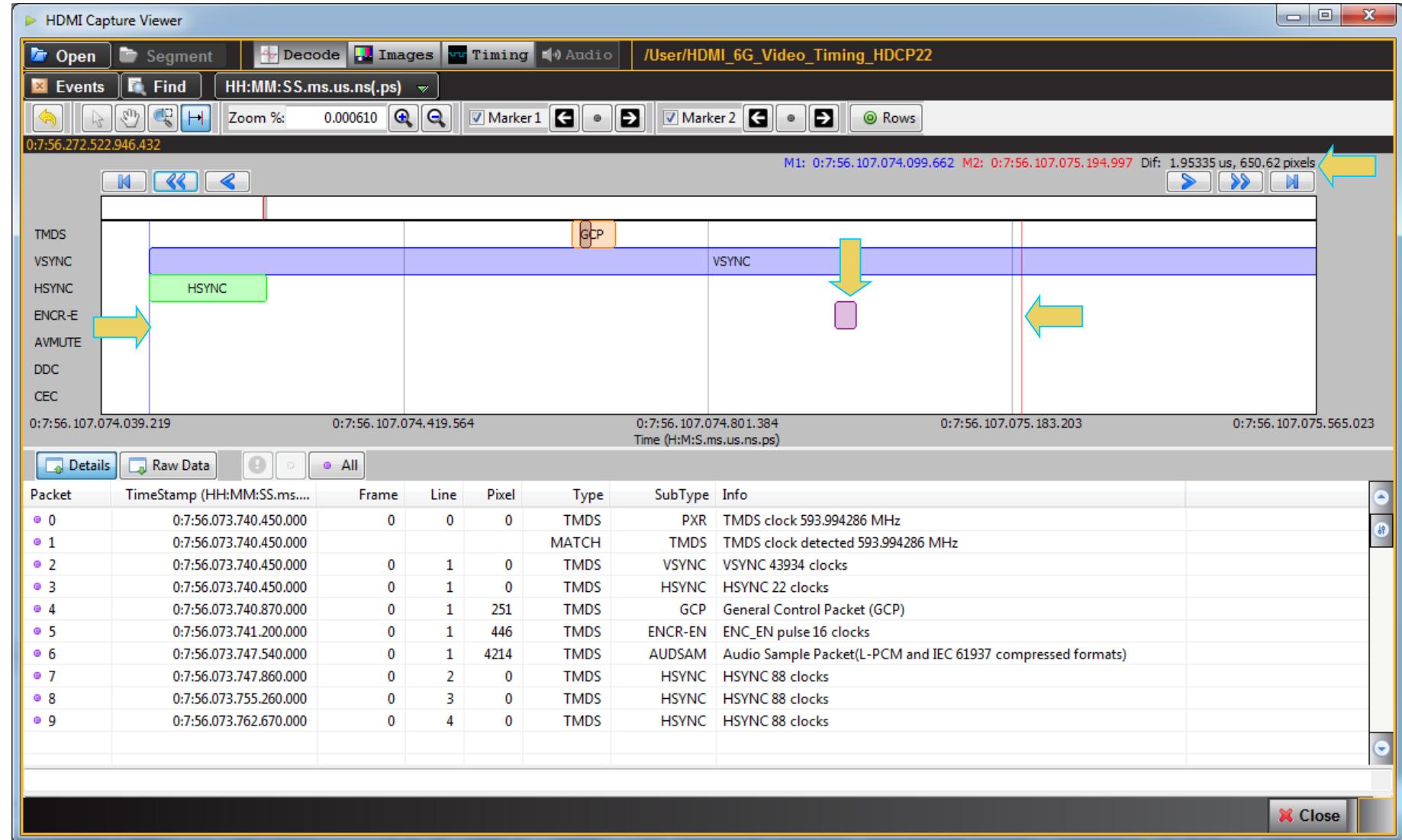
- ◆ HDMI-HDCP stream indicating Video, Encryption Enable Pulse and HDCP authentication messages.
- ◆ Encryption Enable pulse has to occur 512 pixels following active edge of Vsync.

HDCP 2.2 Keep-out Region (HDMI)



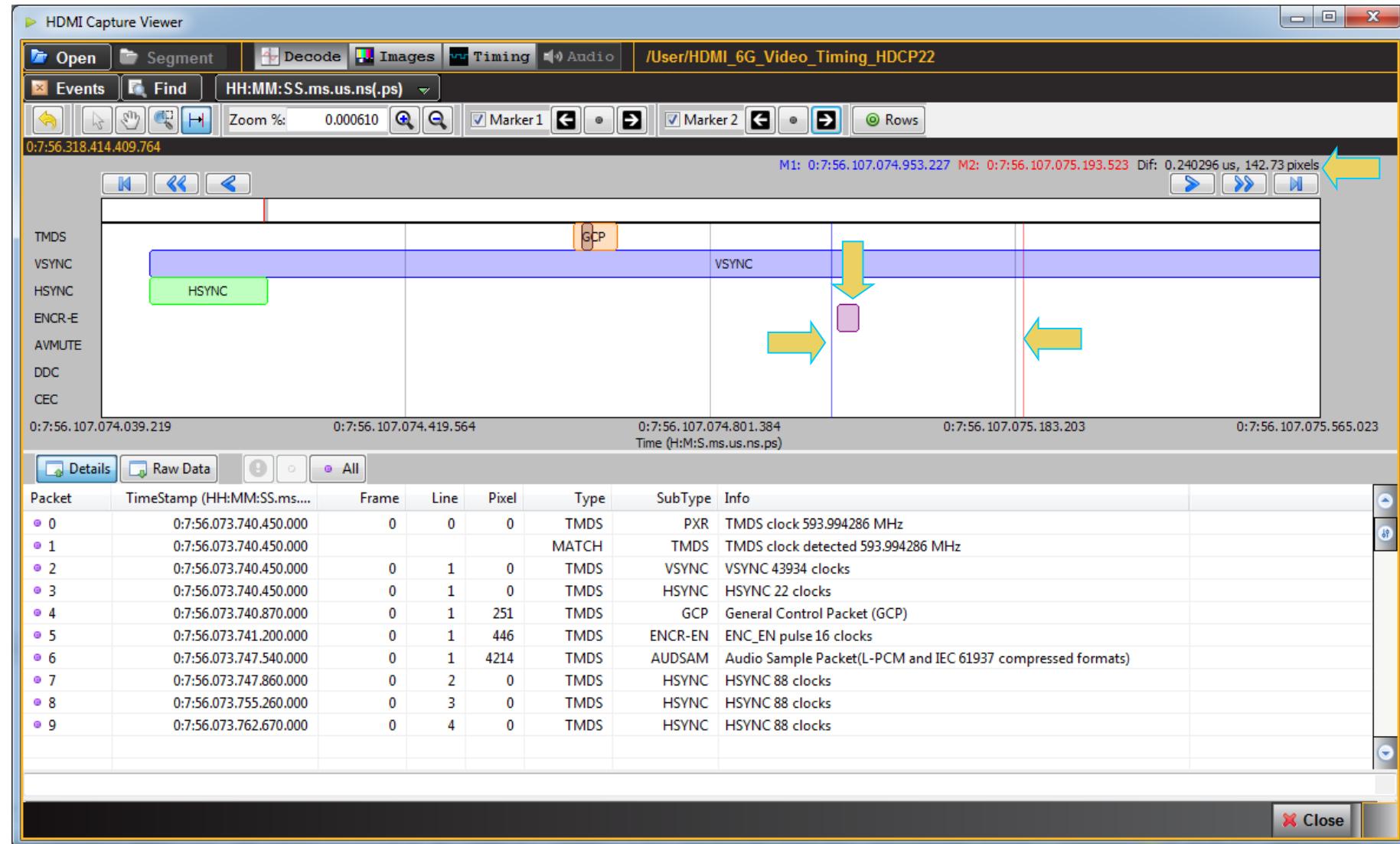
- ◆ HDMI-HDCP Keep-out region beginning 508 pixels following active edge of Vsync.
- ◆ No data islands are supposed to be occurring after that time to the 650th pixel following active edge of Vsync.

HDCP 2.2 Keep-out Region (HDMI)



- ◆ HDMI-HDCP Keep-out region beginning 508 pixels following active edge of Vsync.
- ◆ No data islands are supposed to be occurring after that time to the 650th pixel following active edge of Vsync.

HDCP 2.2 Keep-out Region (HDMI)



- ◆ HDMI-HDCP Keep-out region 142 pixels.
- ◆ No Video or Data Islands allowed.

HDCP 2.2 Compliance Tests



HDCP Compliance Testing

- ◆ Licensing governed by Digital Content Protection LLC (DCP).
- ◆ From DCP website:

"The Compliance test is intended as an aid to the correct implementation of the Compliance Rules for hardware and software implementations of the HDCP Specification in a Licensed Product. The DCP LLC strongly recommends that you complete this testing for each hardware model or software version of a Licensed Product before releasing any product and at a sufficiently early date in design, as well as during production, to avoid product compliance redesign delays."

Teledyne LeCroy – HDMI, DisplayPort and HDCP Testing



980B Test Platform

Supports all HDCP 2.2 compliance tests, source, sink, repeater for both HDMI and DisplayPort.

HDCP 2.2 Compliance Test – Transmitter 1A Test Series (with Receiver)

Test 1A-01: Regular Procedure: With previously connected Receiver (With stored Km)
Verify the Transmitter's implementation of the HDCP protocol when an HDCP Receiver (that was previously connected) is attached.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-02: Regular Procedure: With newly connected Receiver (Without stored Km)
Verify the Transmitter's implementation of the HDCP protocol when an HDCP Receiver (not previously connected) is attached.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-03: Regular Procedure: Receiver disconnect after AKE_Init
Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the write of AKE_Init with a new r_tx value.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-04: Regular Procedure: Receiver disconnect after Km
Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the exchange of Km.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-05: Regular Procedure: Receiver disconnect after locality check
Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected after locality check is initiated.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-06: Regular Procedure: Receiver disconnect after Ks
Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the exchange of Ks.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer

Test 1A-07: Regular Procedure: Receiver sends REAUTH_REQ after Ks
Verify the Source DUT restarts authentication after the receiver sends REAUTH_REQ following the exchange of Ks.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-08: Irregular Procedure: Rx certificate not received.
Verify the Source DUT considers it a failure of authentication when the certificate is not received from the Rx during AKE.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

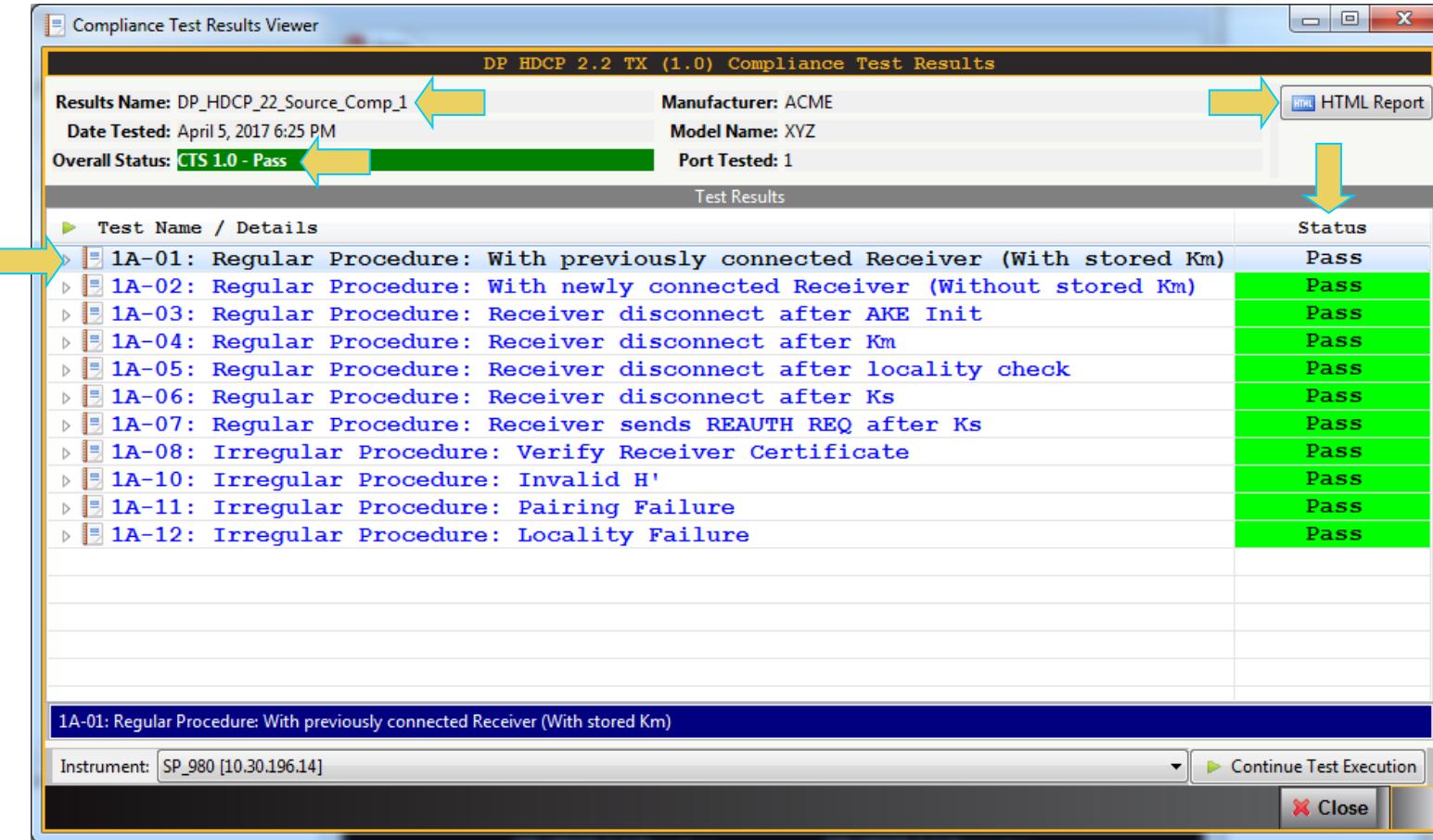
Test 1A-09: Irregular Procedure: Verify Receiver Certificate
Verify the Source DUT considers it a failure of authentication when verification of Receiver certificate fails.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-11: Irregular Procedure: Invalid H'
Verify the Source DUT considers it a failure of authentication if the Receiver provides a value for H' that does not match H, or does not respond with H' in the allotted time.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-12: Irregular Procedure: Pairing Failure
Verify the Source DUT considers it a failure of authentication if the Receiver does not send AKE_Send_Pairing_Info.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

Test 1A-13: Irregular Procedure: Locality Failure
Verify the Source DUT considers it a failure of authentication if the Receiver provides a value for L' that does not match L, or does not respond with L' in the allotted time.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

HDCP 2.2 Compliance Test – Test Results Viewer



- ◆ HDCP 2.2 source Compliance Test for results shows name at the top.
- ◆ HDCP 2.2 source Compliance Test results file shows Pass/Fail results of each test, overall Pass/Fail results.
- ◆ You can generate an HTML report (button top right).
- ◆ We will look at two example tests in the following slides: 1A-01 (a regular test) and 1A-12 tests (irregular test).

HDCP 2.2 Compliance Test – Example Test 1A-01

Compliance Test Results Viewer
DP HDCP 2.2 TX (1.0) Compliance Test Results

Results Name: DP_HDCP_22_Source_Comp_1
Manufacturer: ACME
Date Tested: April 5, 2017 6:25 PM
Overall Status: CTS 1.0 - Pass

Test Name / Details

	Status
1A-01: Regular Procedure: With previously connected Receiver	Pass
Iter 01:	Pass

TX AUTH:MSG:HPD_DIS ts:92013725911.04 us
TX UNAUTH::ENTER
TX MSGR:Disable ENC_EN ts:92013726074.88 us
TX MSGR:Disable ENC_EN ts:92013727272.96 us
TX UNAUTH:MSG RD:HPD_DIS ts:92013728317.44 us
TX UNAUTH:MSG RD:INVALID_VER ts:92013727098.88 us
TX UNAUTH:MSG RD:INVALID_VER ts:92013728296.96 us
RX UNAUTH::ENTER Rep:no DevCnt:0 Dep:0
RX UNAUTH:NO VIDEO Present
TX UNAUTH:MSG RD:VALID_VER ts:92015726848.00 us
TX UNAUTH:MSG RD:HPD_EN ts:92017727057.92 us
TX UNAUTH:AKE_INIT ts:92017727569.92 us
TX UNAUTH:MSG RD:AKE_Init ts:92017727569.92 us
RX UNAUTH:RCVD:AKE_Init ts:92017727508.48 us
RX UNAUTH:**Test Cond.** auth
RX UNAUTH:HDCP2 Version not read.
RX AKE::enter
RX MSGR:WROTE to DPCD:AKE_Send_Cert:534 ts:92017727723.52
TX UNAUTH:MSG RCVDAKE_Send_Cert ts:92017779476.48 us
TX UNAUTH:RxCaps 2 0 2
TX AKE:Snd Stored_KM ts:92017794007.04 us
TX AKE:MSG RD:AKE_Stored_km ts:92017794007.04 us
RX AKE:MSG RCVDAKE_Stored_km ts:92017793955.84 us
RX AKE:**Test Cond.** auth
RX MSGR:WROTE to DPCD:AKE_Send_H_prime:33 ts:92017794979.84
RX LC:MSG SND:AKE_Send_Cert ts:92017793955.84 us
TX AKE:MSG RCVDAKE_Send_H_prime ts:92017797140.48 us
TX LC:Snd LC_Init ts:92017798256.64 us
TX LC:MSG RD:LC_Init ts:92017798256.64 us
RX LC:MSG RCVDAKE_Init ts:92017798195.20 us
RX MSGR:WROTE to DPCD:LC_Send_L_prime:33 ts:92017799157.76
RX LC:MSG SND:AKE_Send_H_prime ts:92017798195.20 us

1A-01: Regular Procedure: With previously connected Receiver (With stored Km)
1A-02: Regular Procedure: With newly connected Receiver (With stored Km)
1A-03: Regular Procedure: Receiver disconnect after AKE Init

Instrument: SP_980 [10.30.196.14] Continue Test Execution Close

- ◆ You can explode out the results for any test to view the details.
- ◆ Example shows details of test 1A-01 which passes.
- ◆ The details are useful for pinpointing the root cause in the event of a failure.
- ◆ Example could be the sending of the KM (master key) (indicated).
- ◆ You can also view the ACA transactions to confirm a failure (next slide).

HDCP 2.2 Compliance Test – Example Test 1A-06 Failure

Compliance Test Results Viewer

HDMI HDCP 2.2 TX (1.0) Compliance Test Results

Results Name: HDMI_HDCP_22_PC Manufacturer: ACME
Date Tested: May 17, 2016 3:57 PM Model Name: XYZ
Overall Status: CTS 1.0 - Fail Port Tested: 1

Test Results

Test Name / Details Status

1A-01: Regular Procedure: With previously connected Receiver (With stored Km)	Pass
1A-02: Regular Procedure: With newly connected Receiver (Without stored Km)	Pass
1A-03: Regular Procedure: Receiver disconnect after AKE Init	Pass
1A-04: Regular Procedure: Receiver disconnect after Km	Pass
1A-05: Regular Procedure: Receiver disconnect after locality check	Pass
1A-06: Regular Procedure: Receiver disconnect after Ks	Fail
Iter 01:	Fail

1A-01: Regular Procedure: With previously connected Receiver (With stored Km)

1A-02: Regular Procedure: With newly connected Receiver (Without stored Km)

1A-03: Regular Procedure: Receiver disconnect after AKE Init

1A-04: Regular Procedure: Receiver disconnect after Km

1A-05: Regular Procedure: Receiver disconnect after locality check

1A-06: Regular Procedure: Receiver disconnect after Ks

Iter 01:

- Clear Ready
- RX HPD Deasserted regular ts:5115282636.80 us
- RX HPD Asserted regular ts:5115432673.28 us
- RX UNAUTH::ENTER
- RX UNAUTH:HDMI/VIDEO Present
- RX UNAUTH:MSG RD:ENC_DIS ts:5115992064.00 us
- RX UNAUTH:RCVD:AKE_Init ts:0.00 us
- RX UNAUTH:**Test Cond.** hpd
- RX AKE:MSG SND:AKE_Send_Cert ts:5117223004.16 us
- RX AKE:MSG RCV:AKE_No_Stored_km ts:5118022901.76 us
- RX PAIR::ENTER
- RX PAIR:MSG RD:AKE_Send_H_Prime ts:5118037442.56 us
- RX LC:MSG SND:AKE_Send_Pairing_Info ts:5118050856.96 us
- RX LC:MSG RCV:LC_Init ts:5118052044.80 us
- RX LC:MSG SND:LC_Send_L_prime ts:5118058301.44 us
- RX LC:MSG RCV:SKE_Send_Eks ts:5118072350.72 us
- RX SKE::ENTER
- RX SKE:MSG RCV:SKE_Send_Eks ts:5118072350.72 us
- RX HPD Deasserted irregular ts:5118072606.72 us
- RX HPD Asserted irregular ts:5118272634.88 us
- RX UNAUTH:MSG RD:ENC_EN ts:5118292039.68 us

Encryption Enabled

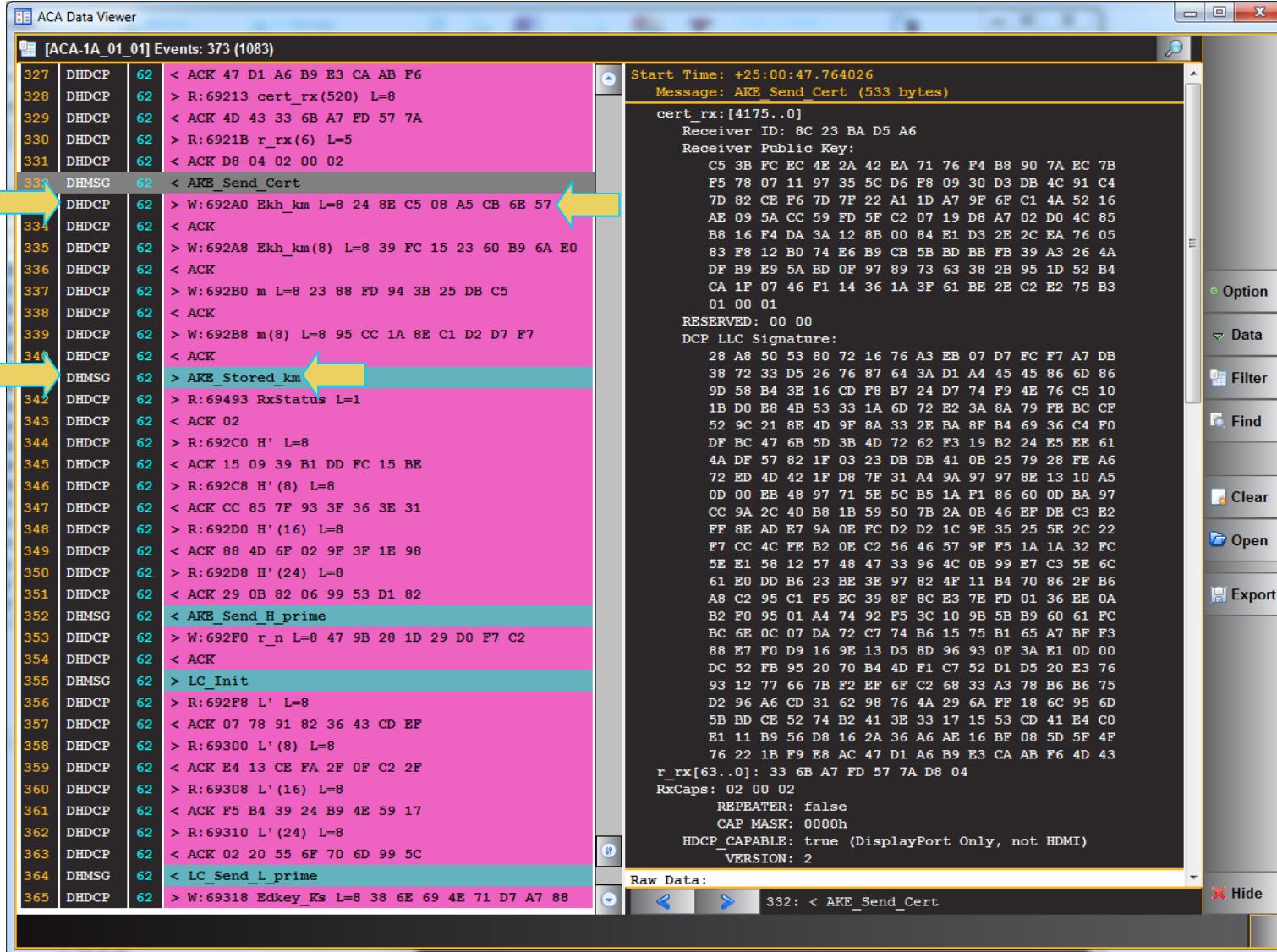
- ◆ Example shows details of test 1A-06 where there is a failure.
- ◆ The point of failure is identified. In this case, after disconnection cycle, encryption pulse was enabled following a connection cycle. The Transmitter should have terminated the encryption and re-initiated authentication.

1A-07: Regular Procedure: Receiver sends REAUTH REQ after Ks	Pass
1A-08: Irregular Procedure: Rx certificate not received.	Pass
1A-09: Irregular Procedure: Verify Receiver Certificate	Pass
1A-11: Irregular Procedure: Invalid H'	Pass
1A-12: Irregular Procedure: Pairing Failure	Pass
1A-13: Irregular Procedure: Locality Failure	Pass
1B-01: Regular Procedure: With Repeater	Pass
1B-02: Irregular Procedure: Timeout of Receiver ID list	Pass
1B-03: Irregular Procedure: Verify V'	Pass
1B-04: Irregular Procedure: MAX DEVS EXCEEDED	Pass
1B-05: Irregular Procedure: MAX CASCADE EXCEEDED	Pass
1B-06: Irregular Procedure: Incorrect seq num V	Pass

1A-01: Regular Procedure: With previously connected Receiver (With stored Km)

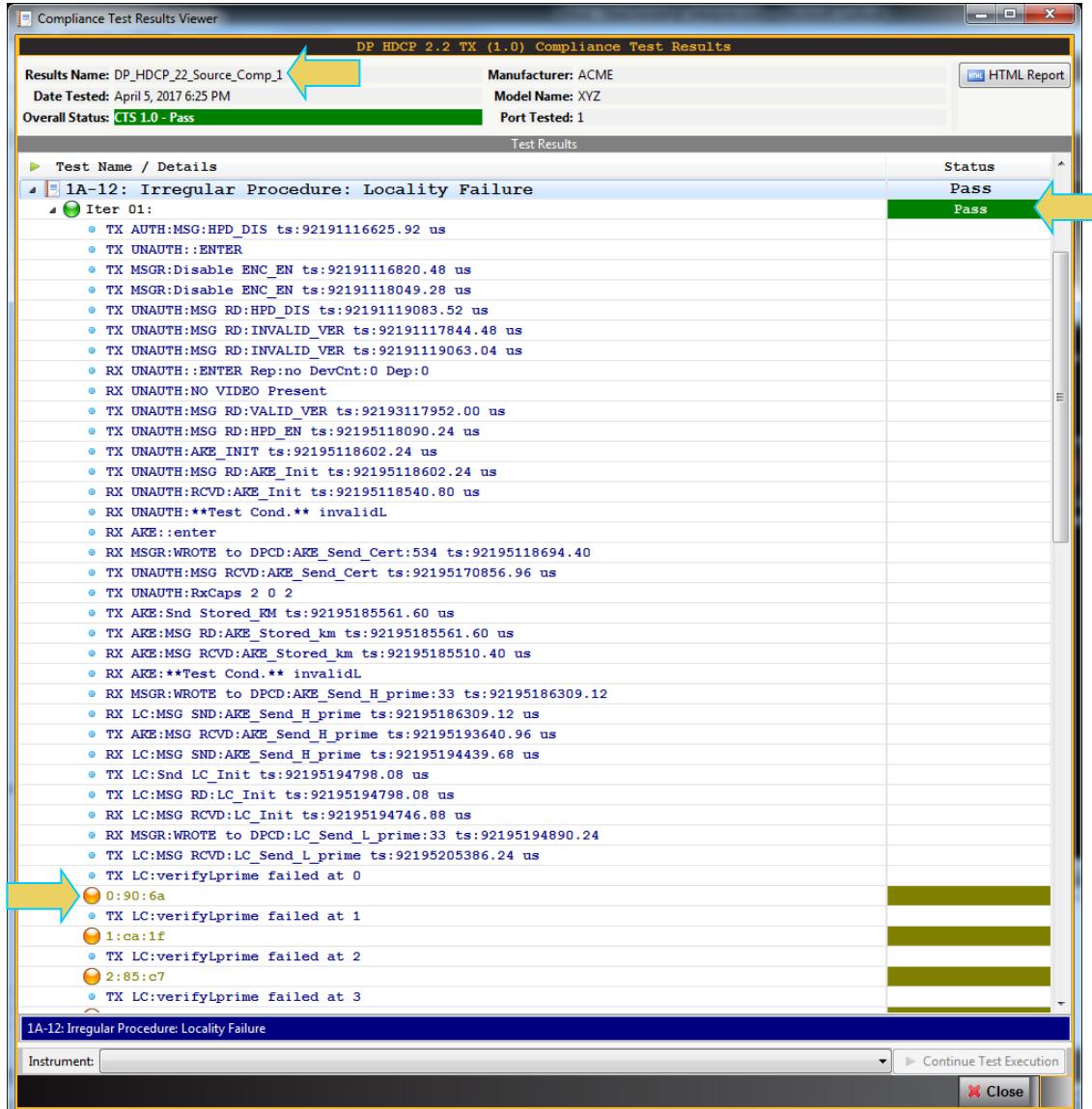
Instrument: My980 [10.30.196.32] Continue Test Execution Close

HDCP Compliance Testing – HDCP Transactions (Example Test 1A-01)



- ◆ Example shows details of HDCP transactions occurring over the HDCP 2.2 source compliance test for 1A-01 test.
- ◆ Details of selected transaction shown in Details panel.
- ◆ Note the related AKE DHDCP messages are consolidated in the DPMMSG transactions.

HDCP 2.2 Compliance Test – Test Results Viewer (Example Test 1A-12)



- ◆ Example shows details of test 1A-12 which passes.
- ◆ Test 1A-12 is an irregular test where the Test Equipment (980 DP/HDMI Protocol Analyzer) responds with an invalid L-Prime value.
- ◆ The details are useful for pinpointing the root cause in the event of a failure.

HDCP 2.2 Compliance Test – Transmitter 1B Test Series (with Repeater)

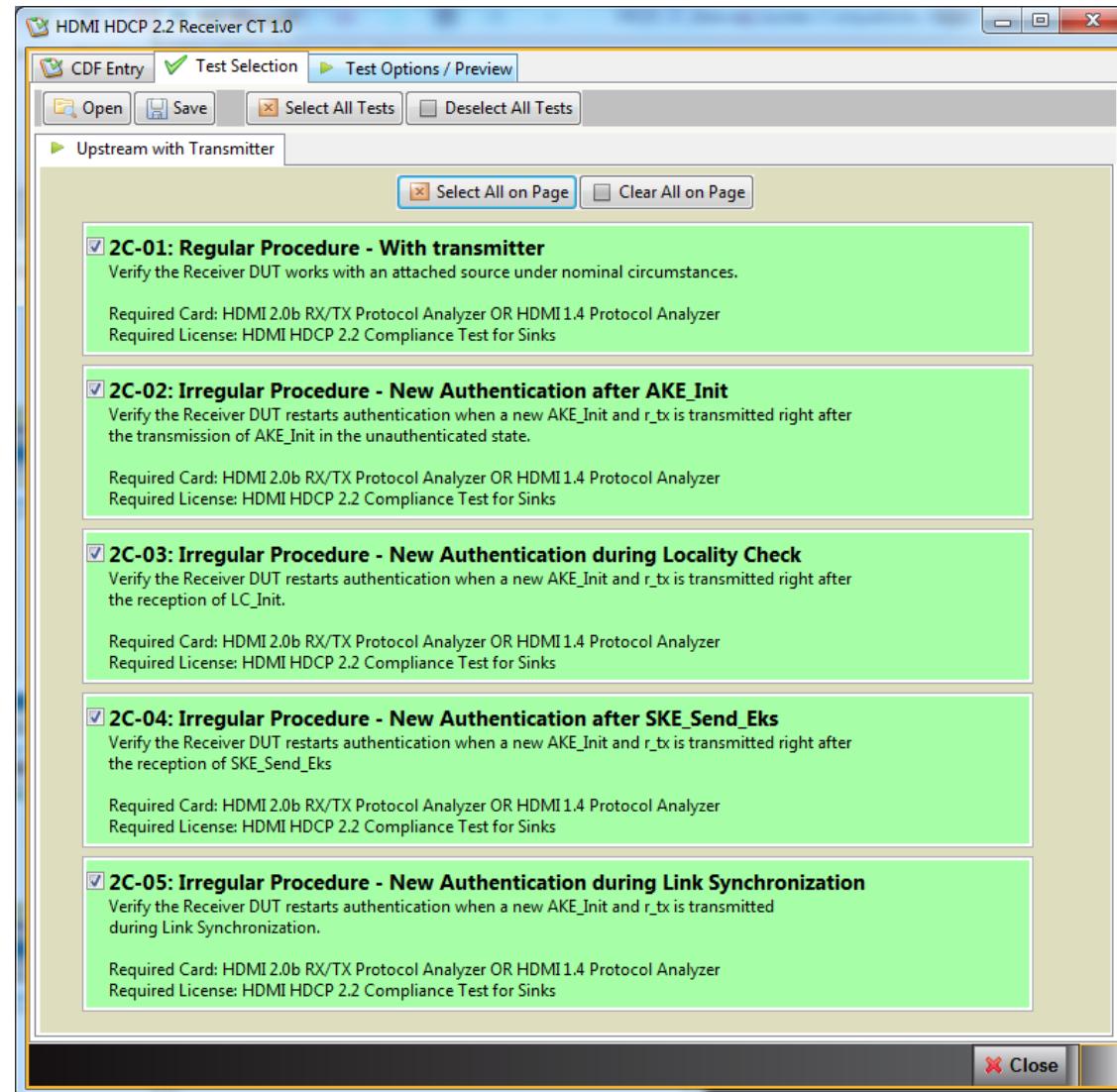
Test Selection window (Left):

- 1B-01: Regular Procedure: With Repeater**
Verify the Source DUT works with a repeater attached under normal circumstances.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-02: Irregular Procedure: Timeout of Receiver ID list**
Verify the Source DUT considers it a failure of authentication if the downstream repeater does not respond with RepeaterAuth_Send_ReceiverID_List prior to expiration of watchdog timer.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-03: Irregular Procedure: Verify V'**
Verify the Source DUT considers it a failure of authentication if the repeater provides a value for V' that does not match V.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-04: Irregular Procedure: MAX_DEVS_EXCEEDED**
Verify the Source DUT considers it a failure of authentication if the repeater sets the MAX_DEVS_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-05: Irregular Procedure: MAX CASCADE EXCEEDED**
Verify the Source DUT considers it a failure of authentication if the repeater sets the MAX CASCADE_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

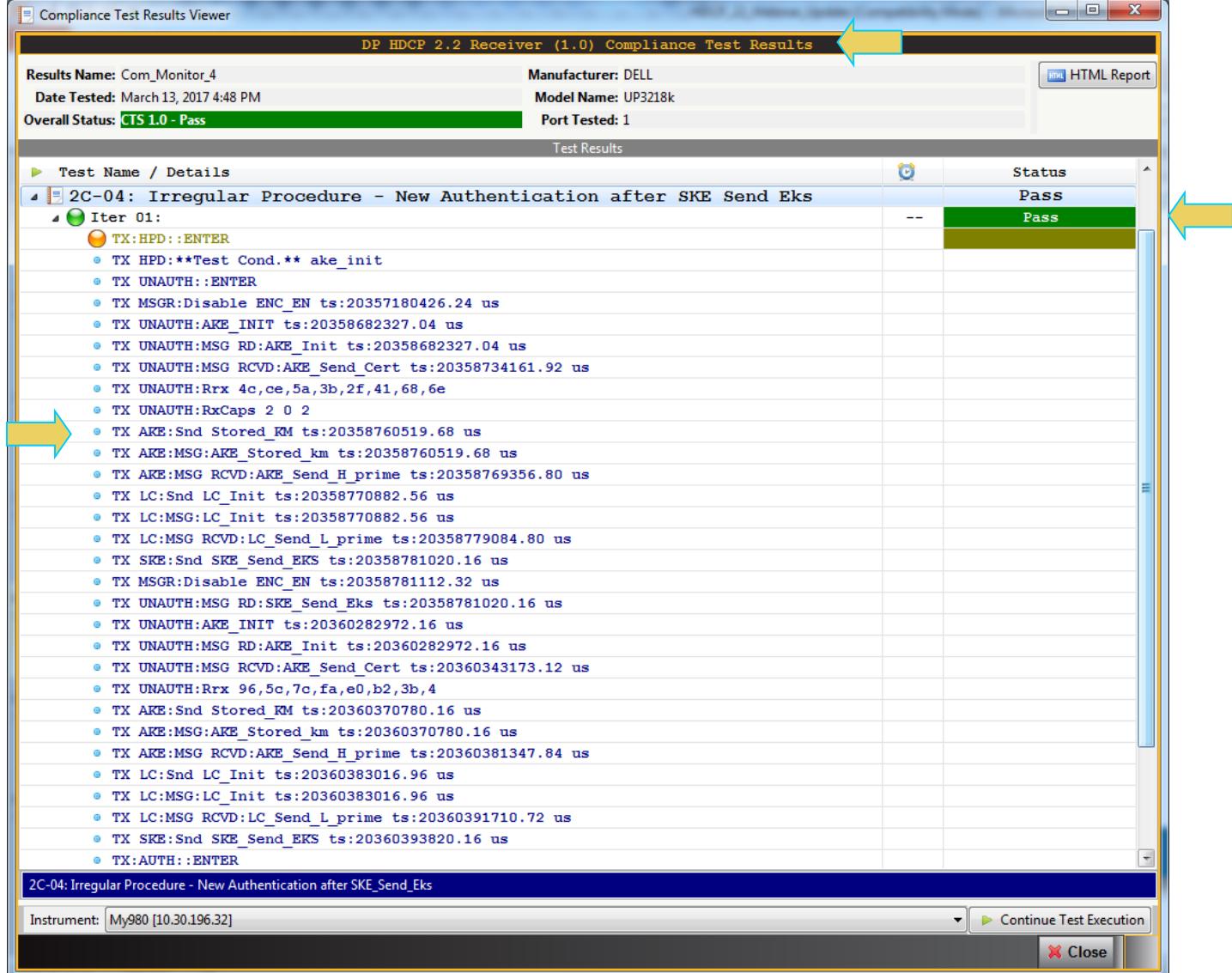
Test Selection window (Right):

- 1B-06: Irregular Procedure: Incorrect seq_num_V**
Verify the Source DUT considers it a failure of authentication if the repeater provides a non-zero value in seq_num_V in the first RepeaterAuth_Send_ReceiverID_List message after AKE_Init.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-07: Regular Procedure: Re-authentication on HDCP_HPD**
Verify the Source DUT initiates re-authentication when a HDCP_HPD is received from the downstream repeater.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-08: Regular Procedure: Re-authentication on REAUTH_REQ**
Verify the Source DUT initiates re-authentication when a REAUTH_REQ is received from the downstream repeater.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-09: Irregular Procedure: Rollover of seq_num_V**
Verify the Source DUT initiates re-authentication when a rollover of seq_num_V is detected from the downstream repeater.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources
- 1B-10: Irregular Procedure: Failure of Content Stream Management**
Verify the Source DUT re-attempts Content Stream Management following a failure of Content Stream Management.
Required Card: HDMI 2.0b RX/TX Protocol Analyzer OR HDMI 1.4 Protocol Analyzer
Required License: HDMI HDCP 2.2 Compliance Test for Sources

HDCP 2.2 Compliance Test – Receiver 2C Test Series



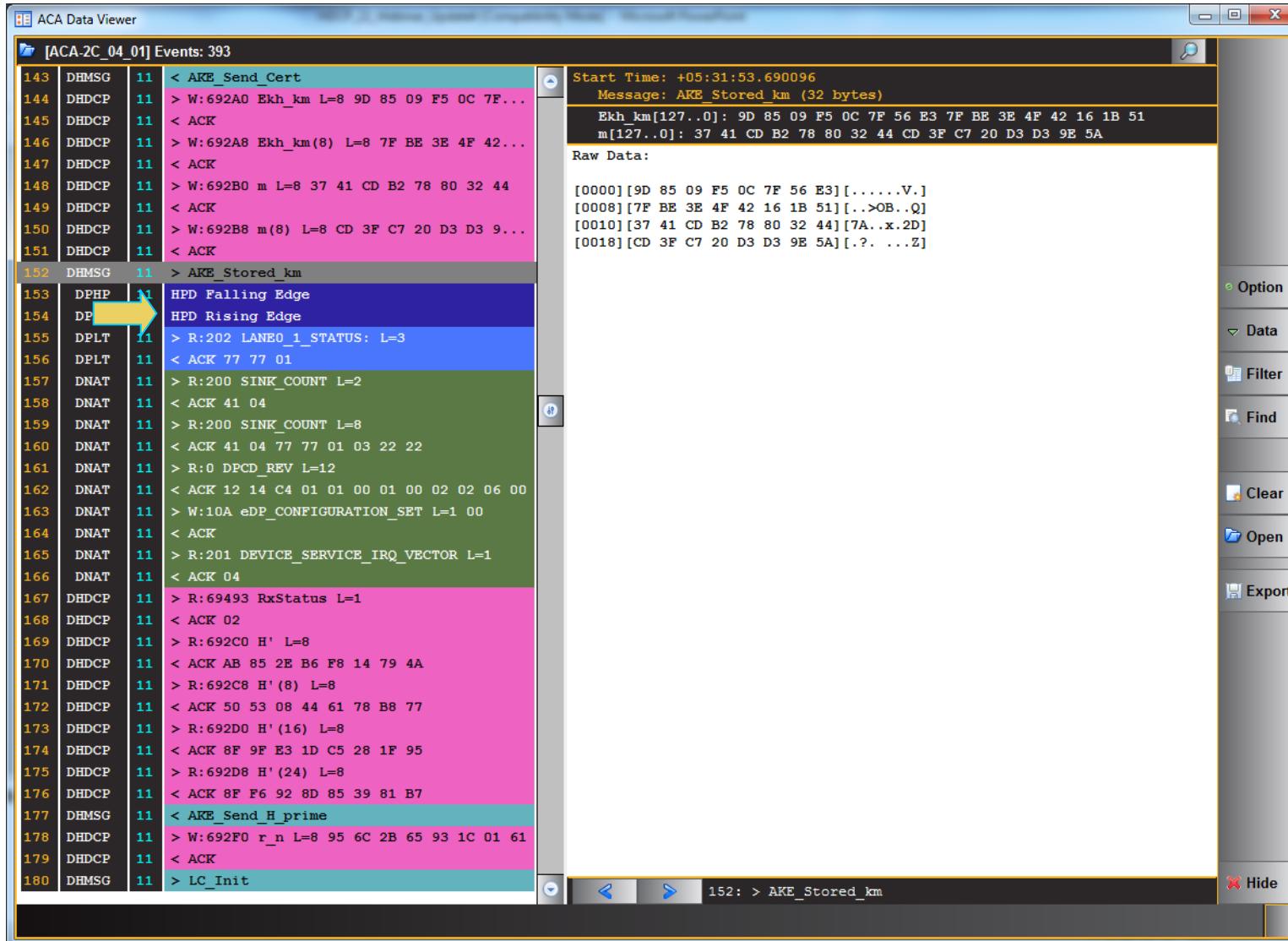
HDCP 2.2 Compliance Test – Test Results Viewer (Example Test 2C-04)



- ◆ Example shows details of test 2C-04 which passes.
- ◆ Test 2C-04 is an irregular test where the Test Equipment (980 DP/HDMI Protocol Analyzer) is emulating a source that initiates re-authentication during Session Key (Ks) exchange.

Note: You can also view the ACA transactions to confirm a failure (which we have seen in this webinar already).

HDCP 2.2 Compliance Test – View ACA of Test Results (Example Test 2C-04)



- ◆ Example shows details of test 2C-04 which passes.
- ◆ Test 2C-04 is an irregular test where the Test Equipment (980 DP/HDMI Protocol Analyzer) is emulating a source that initiates re-authentication during Session Key (Ks) exchange.
- ◆ Here you see the disconnect occurring. Immediately following the disconnect the Transmitter reads the Receiver's DPCD registers.
- ◆ There is some residual activity of the previous authentication.

HDCP 2.2 Compliance Test – View ACA of Test Results (Example Test 2C-04)

The screenshot shows the ACA Data Viewer application interface. On the left, a list of events is displayed in a table format. The columns show the event number (e.g., 177, 199), the source (e.g., DHMSG, DHDPC), the type (e.g., < AKE_Send_H_prime, > AKE_Init), and the details of the message. A yellow arrow points to the row for event 201, which is highlighted in blue. On the right, a detailed view of event 201 is shown in a larger window. It includes fields for Start Time, Message, r_tx, TxCaps, and VERSION. Below this is a Raw Data section showing hex and ASCII representations of the message. A vertical toolbar on the right contains buttons for Option, Data, Filter, Find, Clear, Open, and Export. At the bottom, there are navigation buttons and a status bar indicating '201: > AKE_Init'.

◆ Here you see the re-initiation of authentication following the disconnect.

Thank you for attending
Questions?

Please take the brief
survey that follows.

Please contact me, Neal Kendall at:
neal.kendall@teledyne.com
If you have any questions.

- ◆ We will be announcing additional webinars on the following topics in the coming months; possible topics are:
 - ◆ HDMI 2.1 Protocols
 - ◆ DisplayPort 1.4 Protocols (e.g. DSC/FEC)
 - ◆ DisplayPort Multi-Stream Transport (MST)
 - ◆ Dynamic High Dynamic Range