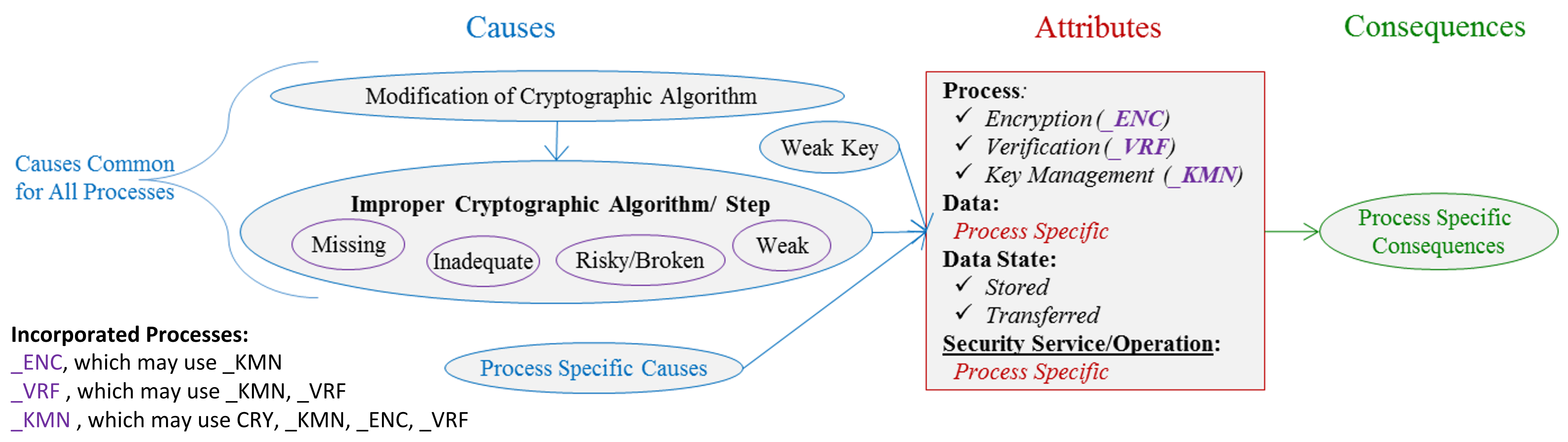
The new Cryptographic Store/Transfer (CST) Class from Bugs Framework (BF)

Irena Bojanova, NIST; Paul Black, NIST; Yaacov Yesha, NIST, UMBC

This is the BF of the new Cryptographic Store/Transfer (CRY–ST) fault class. It shows causes, attributes, and consequences of CST faults.
CST incorporates Encryption (_ENC), Verification (_VRF), and Key Management (_KMN).

Cryptographic Store/Transfer (CST): The software does not properly manage keys, or encrypt/decrypt or verify data for secure store/transfer.


Causes

Attributes

Consequences

Causes Common for All Processes

Modification of Cryptographic Algorithm

Weak Key

Improper Cryptographic Algorithm/ Step

Missing

Inadequate

Risky/Broken

Weak

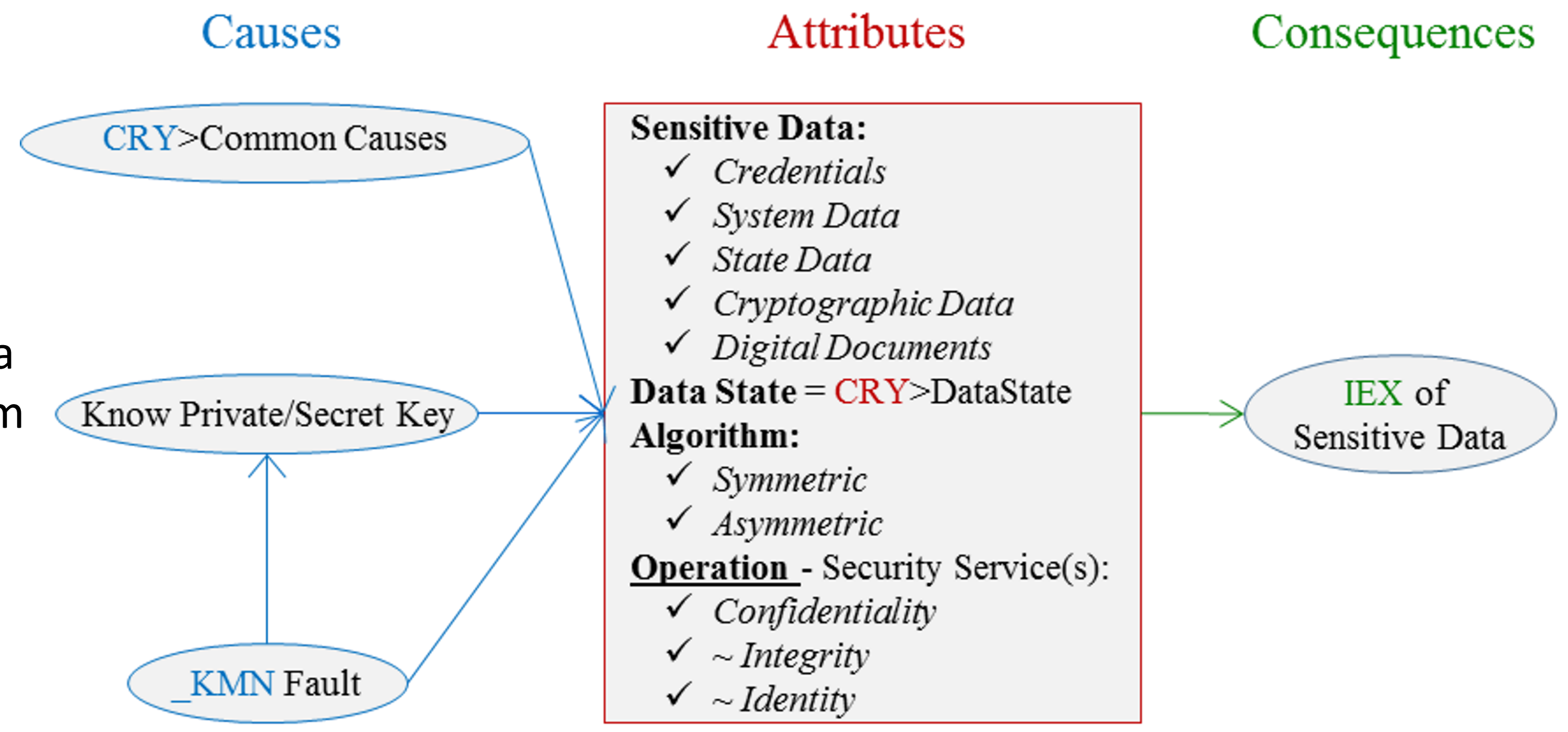
Process Specific Causes

Process:
✓ *Encryption (_ENC)*
✓ *Verification (_VRF)*
✓ *Key Management (_KMN)*
Data:
Process Specific
Data State:
✓ *Stored*
✓ *Transferred*
Security Service/Operation:
Process Specific

Process Specific Consequences

Incorporated Processes:
_ENC, which may use _KMN
_VRF , which may use _KMN, _VRF
_KMN , which may use CRY, _KMN, _ENC, _VRF

_ENC: The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).


Causes

Attributes

Consequences

CRY>Common Causes

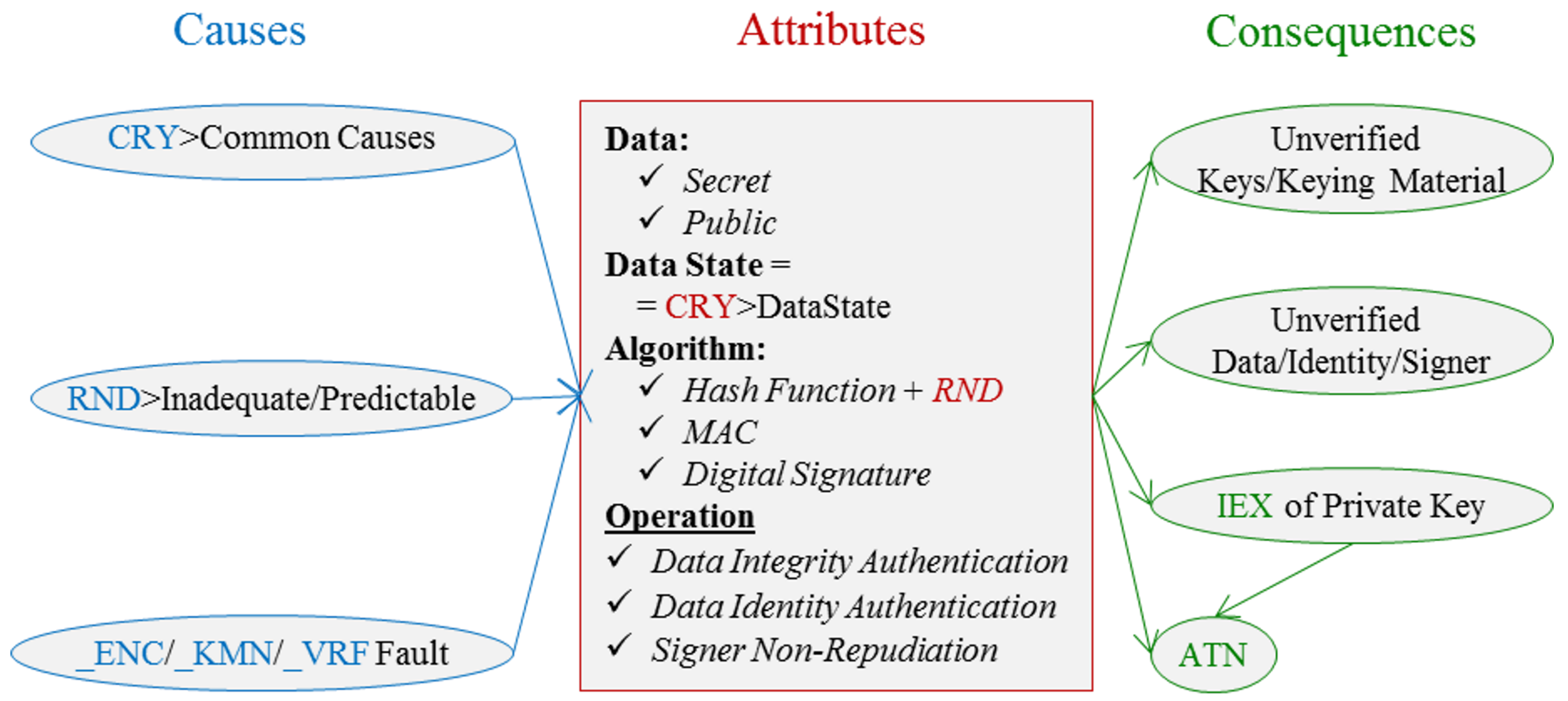
Know Private/Secret Key

_KMN Fault

Sensitive Data:
✓ *Credentials*
✓ *System Data*
✓ *State Data*
✓ *Cryptographic Data*
✓ *Digital Documents*
Data State = CRY>DataState
Algorithm:
✓ *Symmetric*
✓ *Asymmetric*
Operation - Security Service(s):
✓ *Confidentiality*
✓ *~ Integrity*
✓ *~ Identity*

IEX of Sensitive Data

_VRF: The software does not properly sign message, check and prove origin, or assure message is not altered.


Causes

Attributes

Consequences

CRY>Common Causes

RND>Inadequate/Predictable

_ENC/_KMN/_VRF Fault

Data:
✓ *Secret*
✓ *Public*
Data State =
= CRY>DataState
Algorithm:
✓ *Hash Function + RND*
✓ *MAC*
✓ *Digital Signature*
Operation
✓ *Data Integrity Authentication*
✓ *Data Identity Authentication*
✓ *Signer Non-Repudiation*

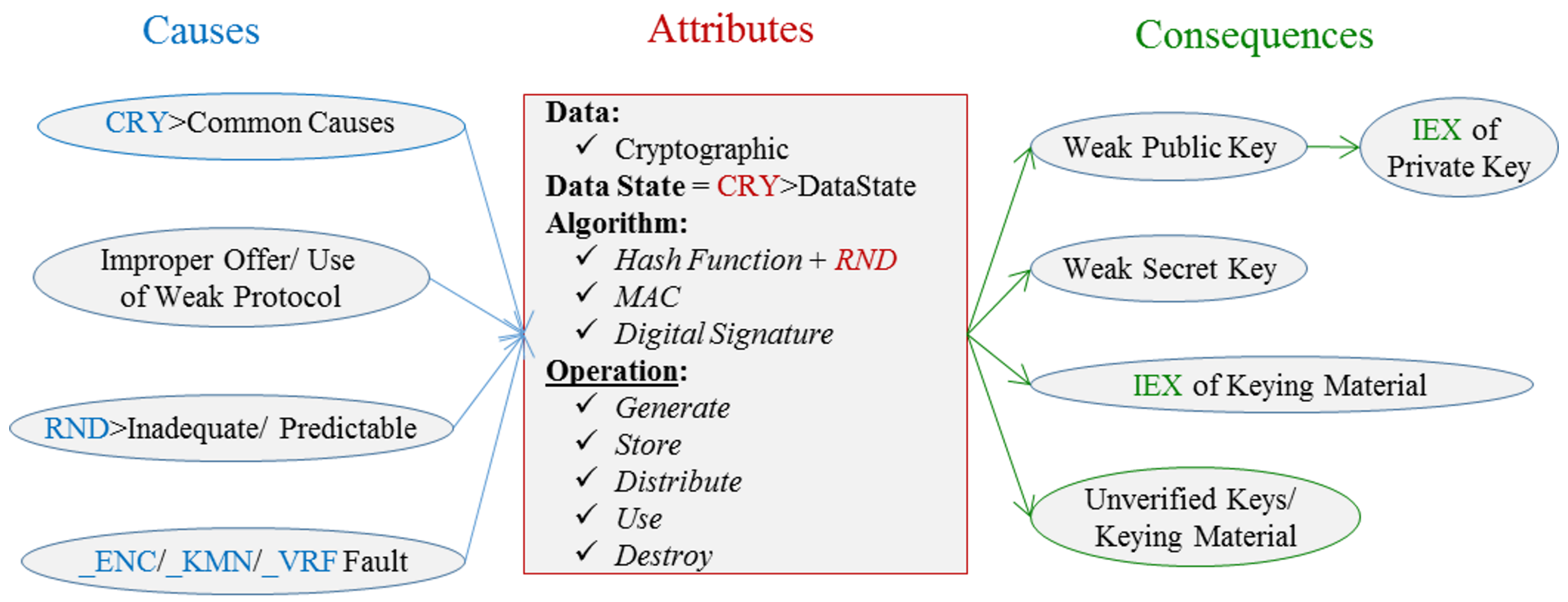
Unverified Keys/Keying Material

Unverified Data/Identity/Signer

IEX of Private Key

ATN

_KMN: The software does not properly generate, store, distribute, use, or destroy cryptographic keys (keying material).


Causes

Attributes

Consequences

CRY>Common Causes

Improper Offer/ Use of Weak Protocol

RND>Inadequate/ Predictable

_ENC/_KMN/_VRF Fault

Data:
✓ Cryptographic
Data State = CRY>DataState
Algorithm:
✓ *Hash Function + RND*
✓ *MAC*
✓ *Digital Signature*
Operation:
✓ *Generate*
✓ *Store*
✓ *Distribute*
✓ *Use*
✓ *Destroy*

Weak Public Key

IEX of Private Key

Weak Secret Key

IEX of Keying Material

Unverified Keys/ Keying Material

Examples

CVE-2015-0204, 1637, 1067 (FREAK)
→ _KMN & _ENC CRY:

Inner _KMN CRY leads to inner _ENC CRY, which leads to outer _ENC CRY.

Inner _KMN CRY:
Client-accepted improper offer of weak protocol (SSL with Export RSA)
from MITM-tricked server, which generates 512-bit RSA key-pair
that is transferred over network,
leads to IEX of sensitive data (private key*).

Inner _ENC CRY:
Known private key
for asymmetric encryption (RSA)
for transferred sensitive data (Pre-Master Secret**),
allows confidentiality failure and decryption,
which leads to IEX of other sensitive data (Master Secret***).

Outer _ENC CRY:
Known secret key (Master Secret)
for symmetric encryption
of transferred sensitive data (passwords, credit cards, etc.).
allows confidentiality failure and decryption,
which leads to IEX of that data.

CVE-2002-1946
→ _ENC CRY:
Use of weak algorithm
for symmetric encryption
(specifically, one-to-one mapping)
for stored in registry sensitive data (passwords)
allows confidentiality failure and decryption ,
which leads to and IEX of that data.

CVE 2001-1585
→ _VRF CRY:
Missing cryptographic step
in public key authentication
(specifically, challenge-response verification
of private key using digital signature)
allows client identity authentication failure,
which leads to ATN.

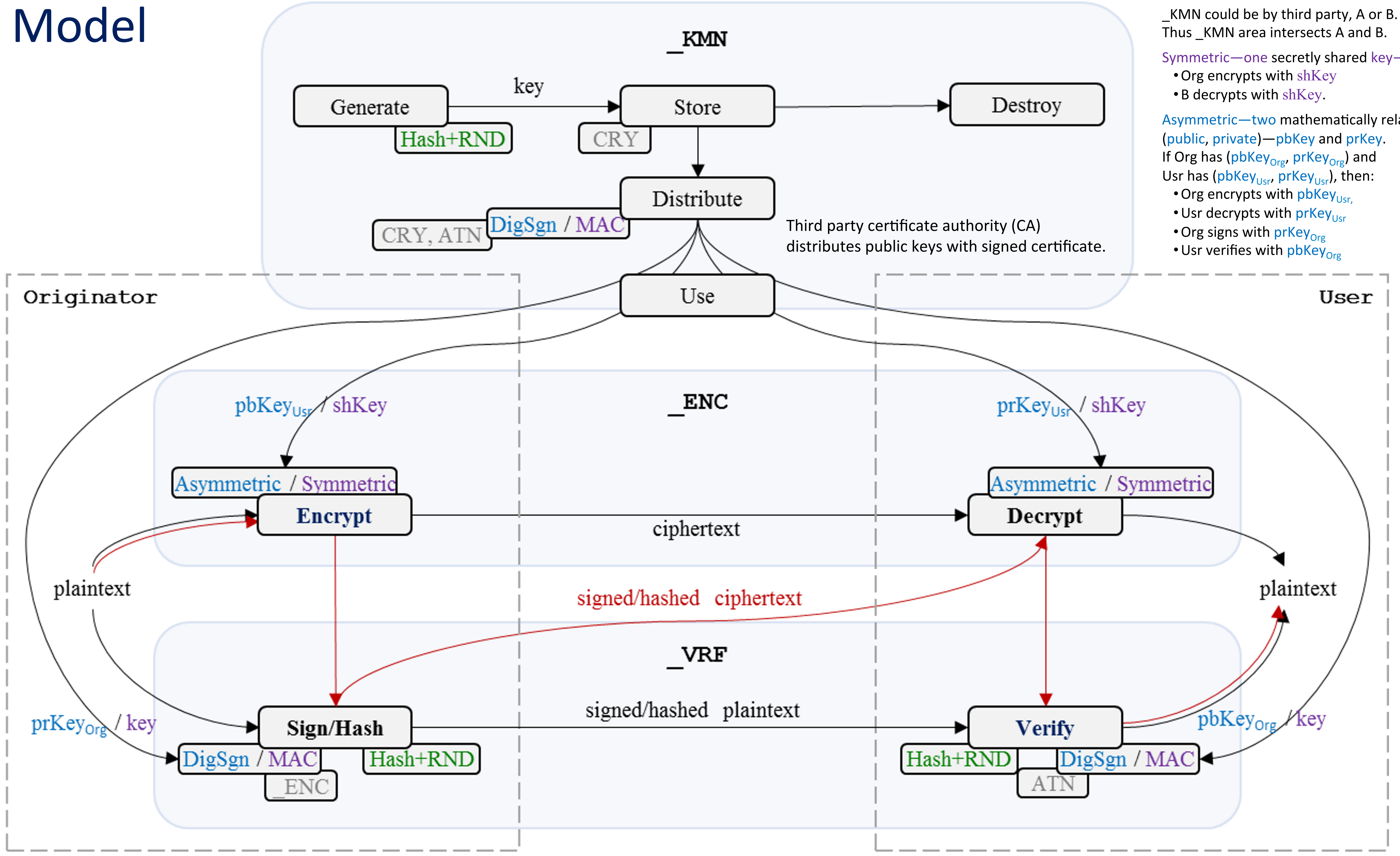
Inner CRYs only set up the secret key. Outer CRY is the actual general data transmission.

* It is computationally feasible for MITM to obtain the private key by factoring the public key for a 512-bit RSA key-pair.

** Knowing the private key MITM can obtain the Pre-Master Secret by message decryption."

*** Knowing Pre-Master Secret, MITM can generate Master Secret (Shared Secret Key)

Model



Third party certificate authority (CA) distributes public keys with signed certificate.

_KMN could be by third party, A or B.
Thus _KMN area intersects A and B.

Symmetric—one secretly shared key—shKey:
- Org encrypts with shKey
- B decrypts with shKey.

Asymmetric—two mathematically related keys (public, private)—pbKey and prKey.
If Org has (pbKey$_{Org}$, prKey$_{Org}$) and Usr has (pbKey$_{Usr}$, prKey$_{Usr}$), then:
- Org encrypts with pbKey$_{Usr,}$
- Usr decrypts with prKey$_{Usr}$
- Org signs with prKey$_{Org}$
- Usr verifies with pbKey$_{Org}$