IPMX / NMOS Security Overview

Alain Bouchard, ing

v0.1

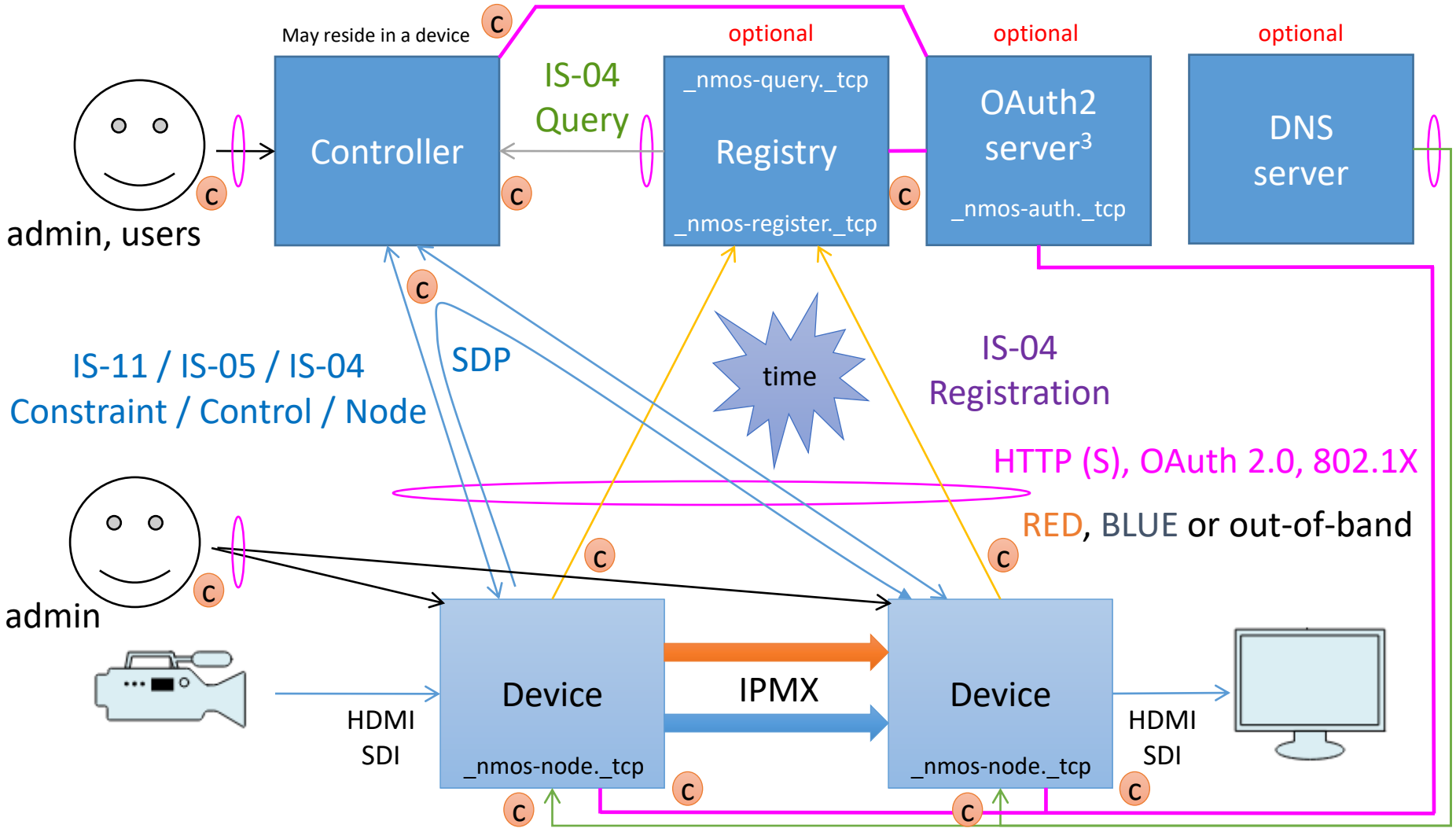
IPMX / NMOS Security

- Scope
  - This presentation is limited to users and sub-system interactions within a single administrative domain. It specifically covers NMOS system interactions under the administrative control of a single domain. Any interactions between systems within this domain and systems managed by another independent administrative domain are out of scope.

Reference Documents

- NIST Special Publication (SP) 800-52
  - "Guidelines for the Selection, Configuration, and Use of TLS“
- NIST Special Publication (SP) 800-57
  - “Recommendation for Key Management”
- Matrox: NMOS With Privacy Encryption
  - “Describes how VSF_TR-10-13 is implemented in NMOS”
- Matrox: NMOS With Node Reservation
  - “Describes how Node Reservation is implemented in NMOS”
- Matrox: NMOS With OAuth2.0
  - “Describes how OAuth2.0 authorizations are used in NMOS”

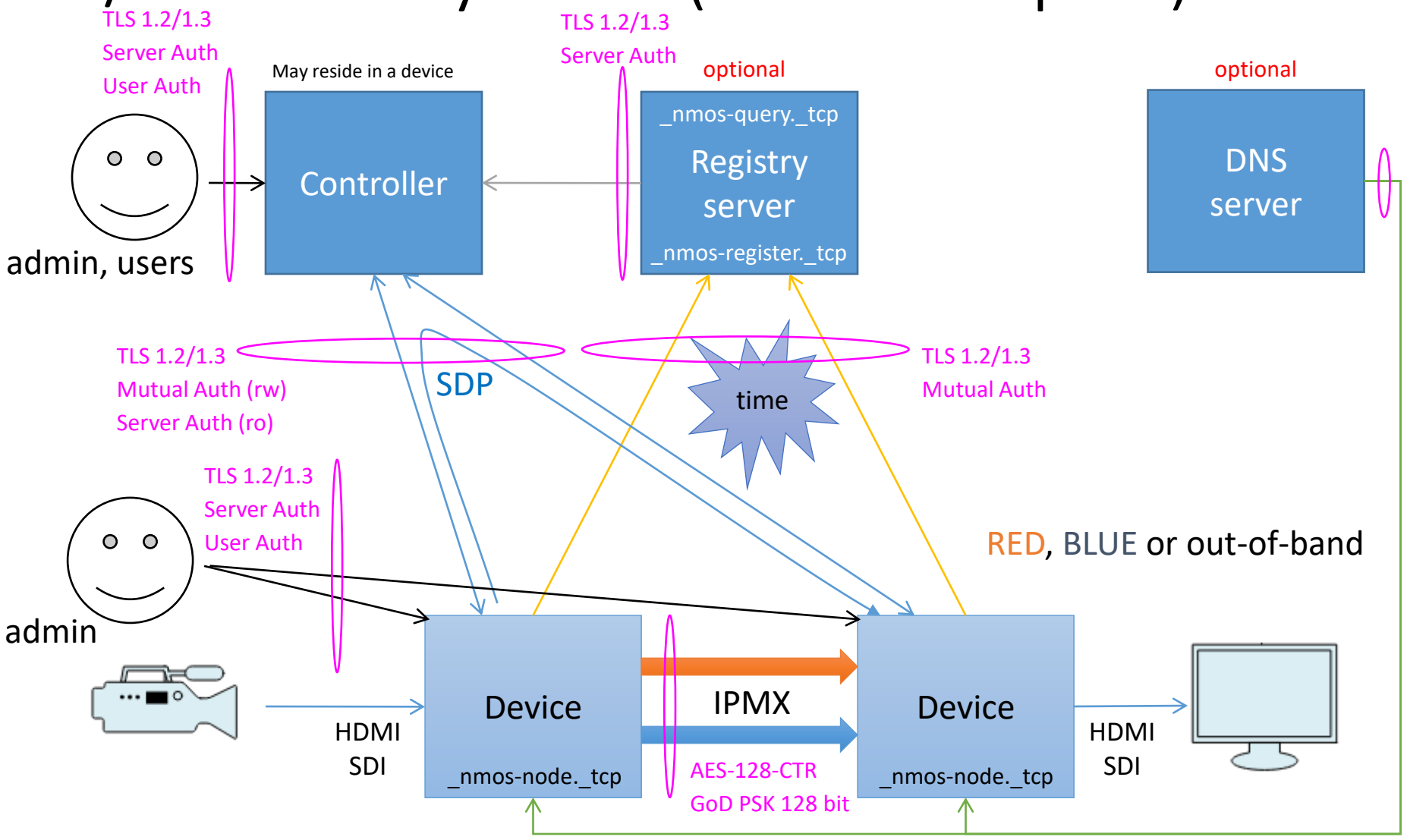
IPMX / NMOS System



IPMX to IPMX devices is also possible

DNS-SD (DNS or mDNS)

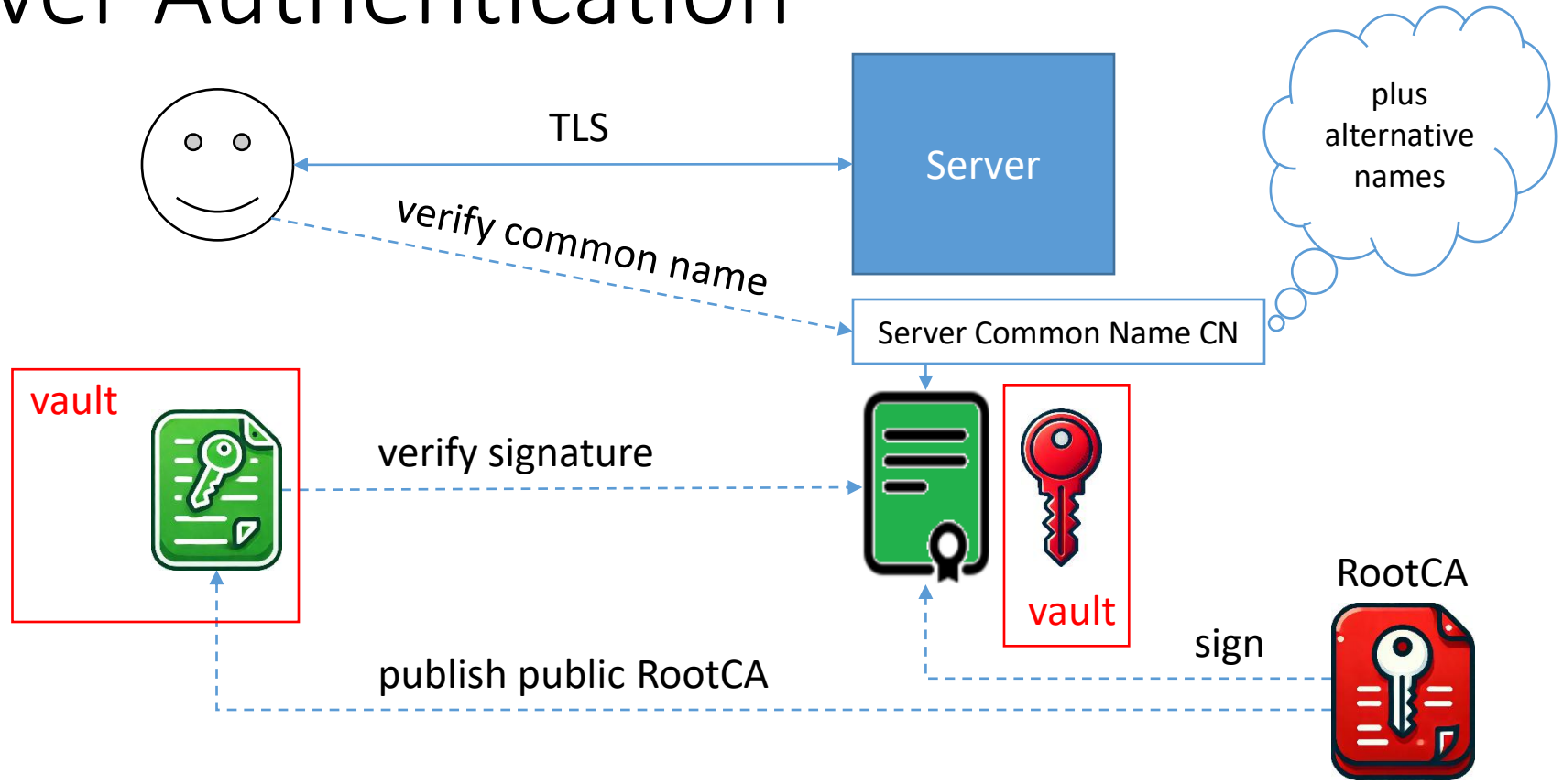
IPMX / NMOS System (normal open)



IPMX to IPMX devices is also possible

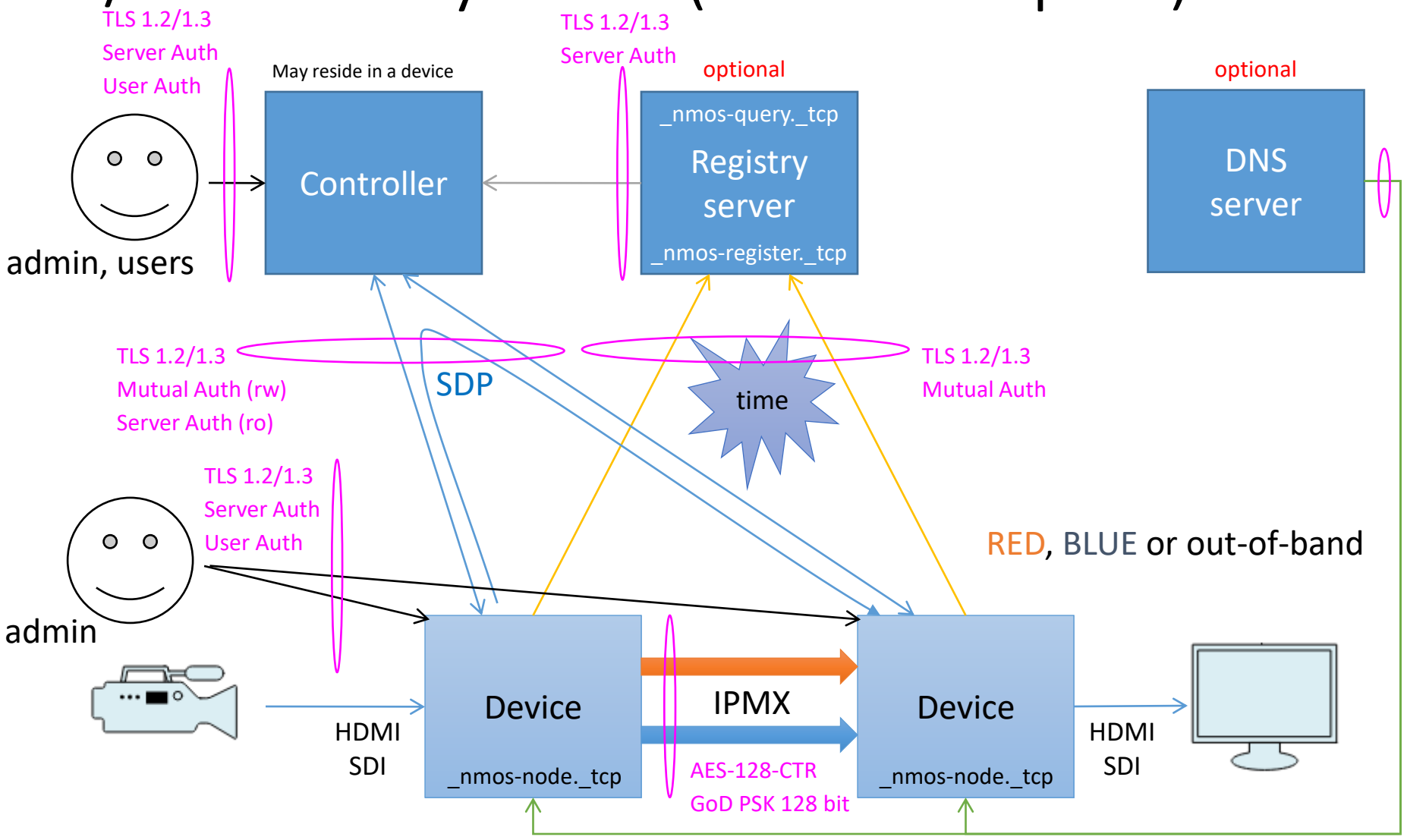
DNS-SD (DNS or mDNS)

TLS Server Authentication



Self-signed certificates SHALL NOT be used.

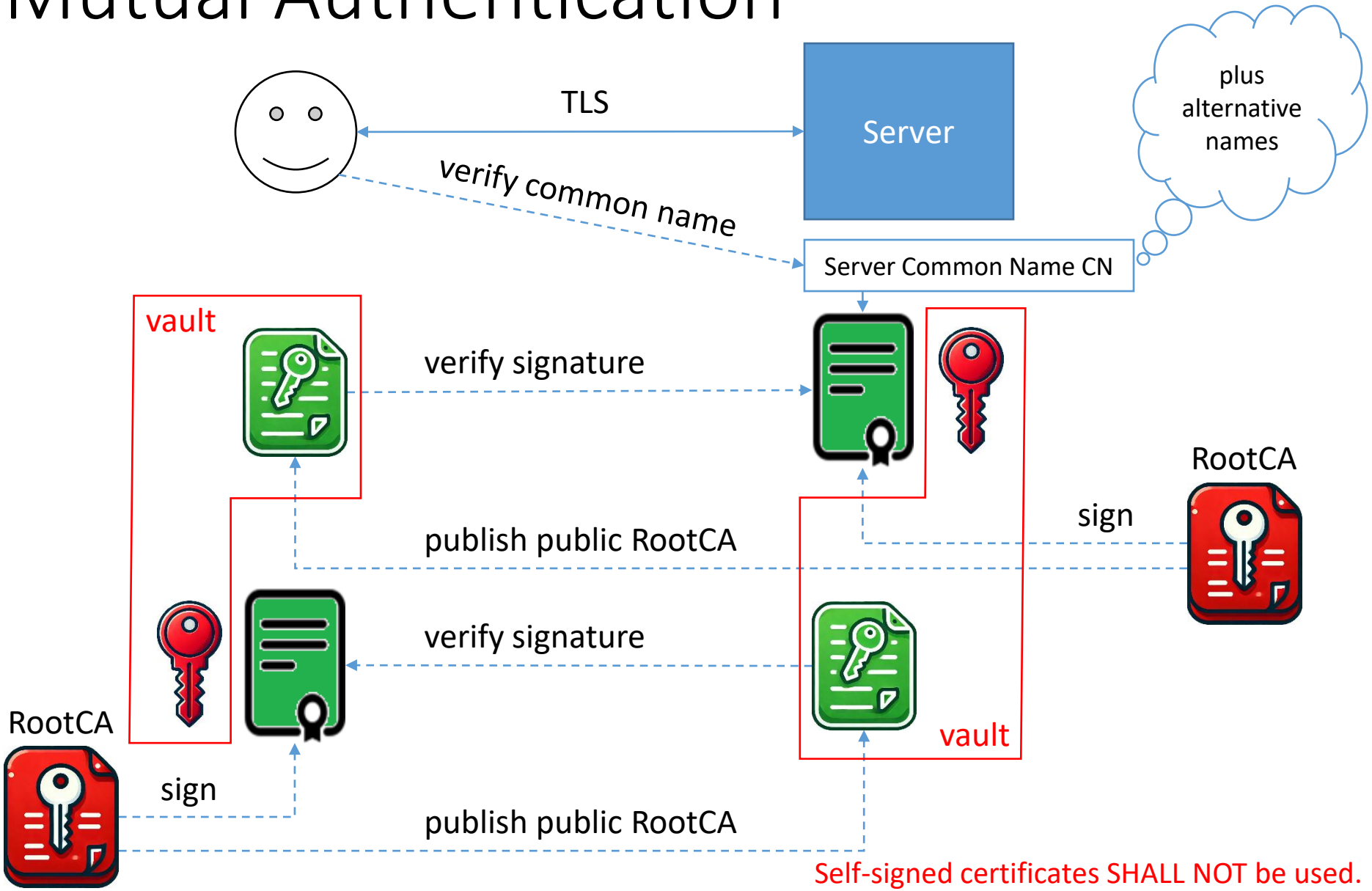
IPMX / NMOS System (normal open)



IPMX to IPMX devices is also possible

DNS-SD (DNS or mDNS)

TLS Mutual Authentication



Self-signed certificates SHALL NOT be used.

Client Accesses

- Assumptions:
  - The service discovery, name resolution and IP address provisioning is performed in a secure way through device configuration, DHCP, mDNS or DNS-SD, using technologies such as DoT (DNS over TLS), DoH (DNS over HTTPS) or DNSSEC.
  - The Controller have adequate support for certificates revocation verification for their client accesses to the devices and sub-systems interfaces.
  - Devices have limited support for certificates revocation verification for their client accesses to the devices and sub-systems interfaces, through a CRL (certificate revocation list) safely uploaded to the devices by an administrator through the device configuration interface.
  - Admin browser and tools have adequate support for certificates revocation verification for their client accesses to the device configuration and the controller user interfaces.
  - Users browser have adequate support for certificates revocation verification for their client accesses to the controller user interface.

Client Authentication

- Assumptions:
  - Devices have limited support for certificates revocation verification for their clients authentication (mutual authentication) from the Configuration and NMOS interfaces, through a CRL (certificate revocation list) safely uploaded to the devices by an administrator through the Device Configuration interface.
  - The Controller have adequate support for certificates revocation verification for their clients authentication (mutual authentication) from the User interface.
  - The Registry have limited support for certificates revocation verification for their clients authentication (mutual authentication) from the query, websocket and registration interfaces.

Time

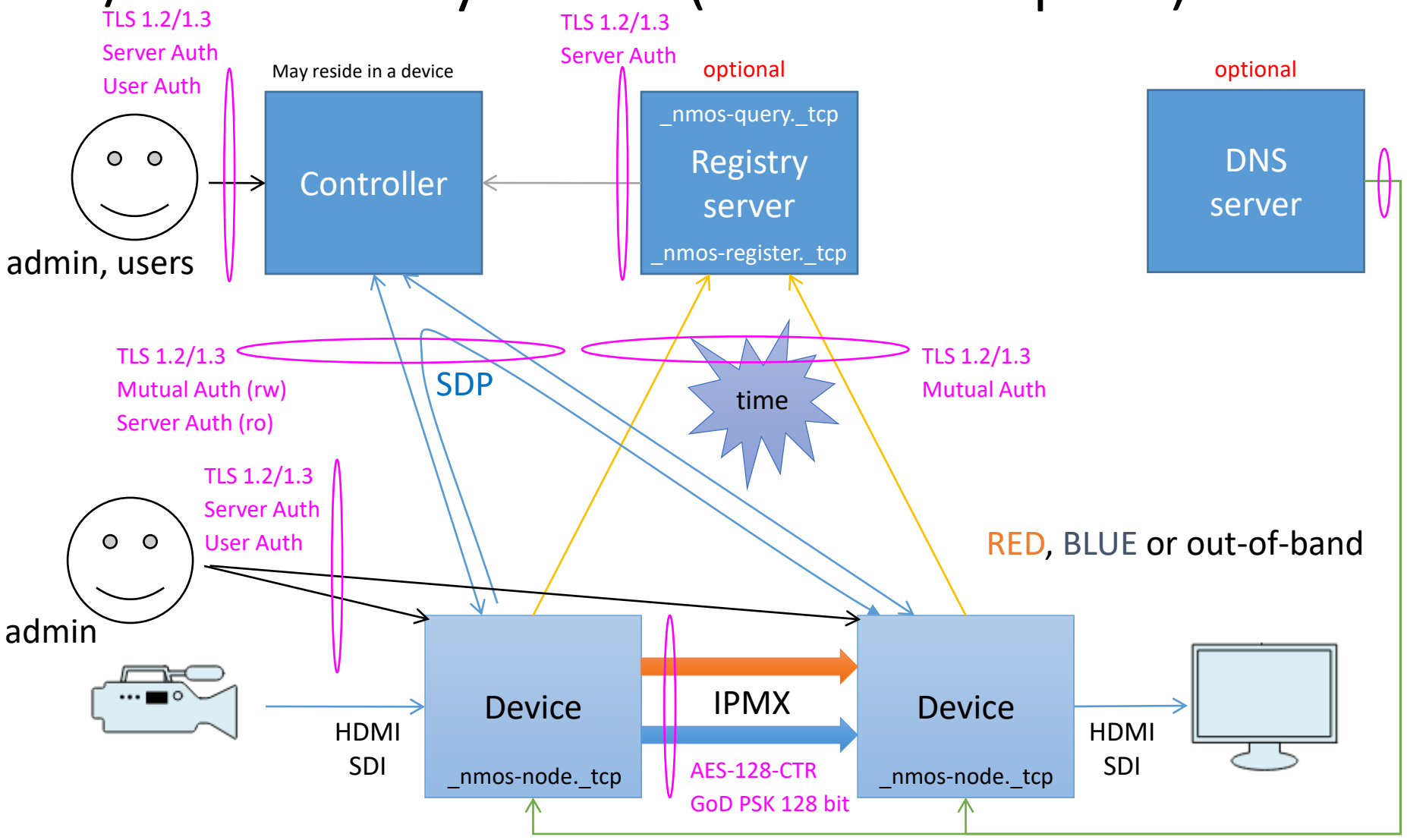
- An important security aspect of an NMOS system is the NTP / PTP time reference provided by time servers.
  - Secure protocols like Network Time Security (NTS) which is based on TLS could be used but may be challenging with PTP
  - Implementation may use an alternate secure NTP time reference to validate that the current NTP / PTP time is within a few seconds of the secure time.
  - Secure time is crucial for the validation of public certificate and bearer token activation/expiration date/time.
  - Securing the time is out of the scope of the current presentation.

802.1x

- Access to the network by devices and sub-systems may optionally be secured by 802.1x
  - EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)
    - Public Key Certificate-based approach
    - Mutual authentication
      - client (supplicant) – server (authenticator)

  - Securing the network access is out of the scope of the current presentation.

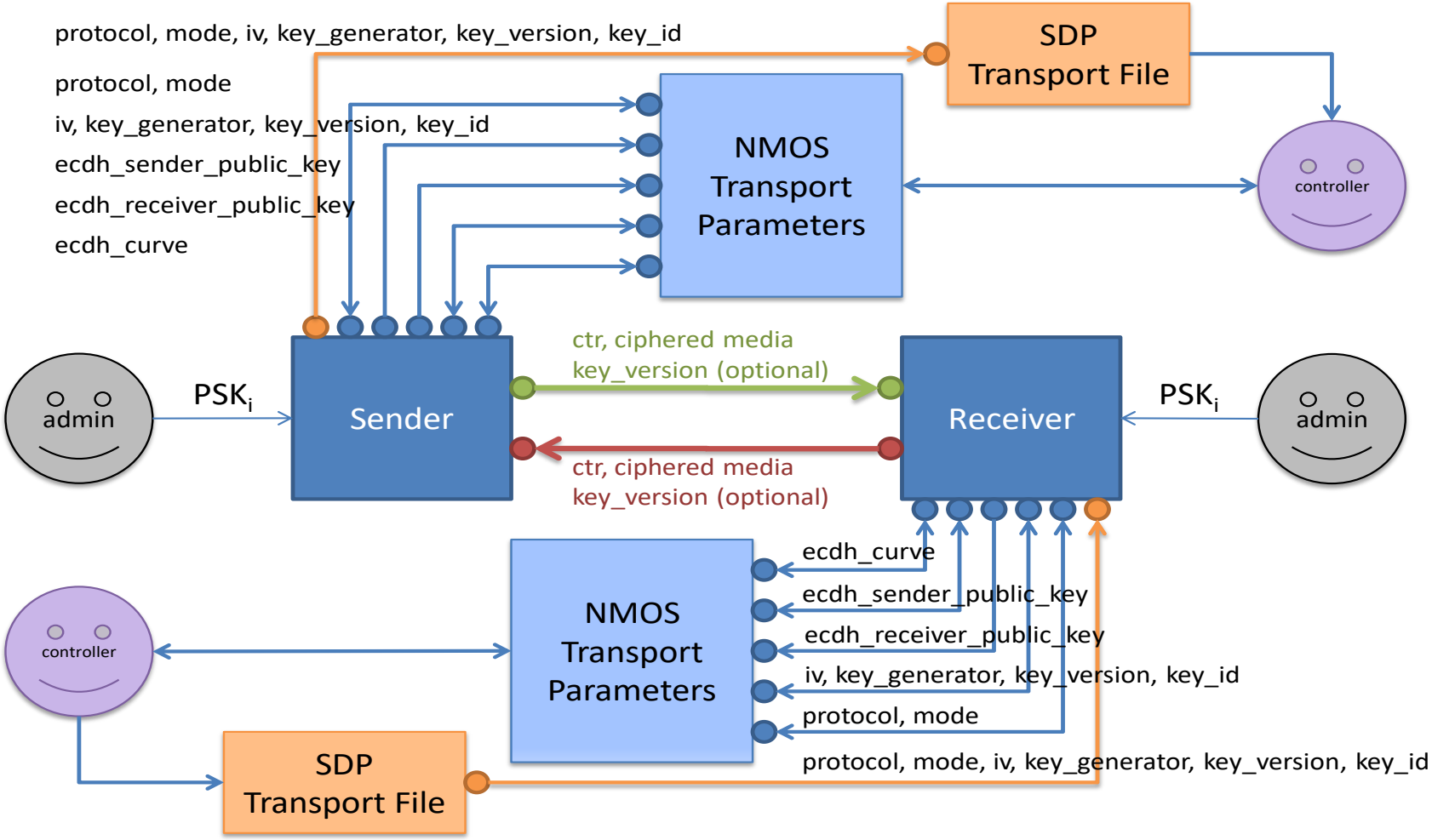
IPMX / NMOS System (normal open)



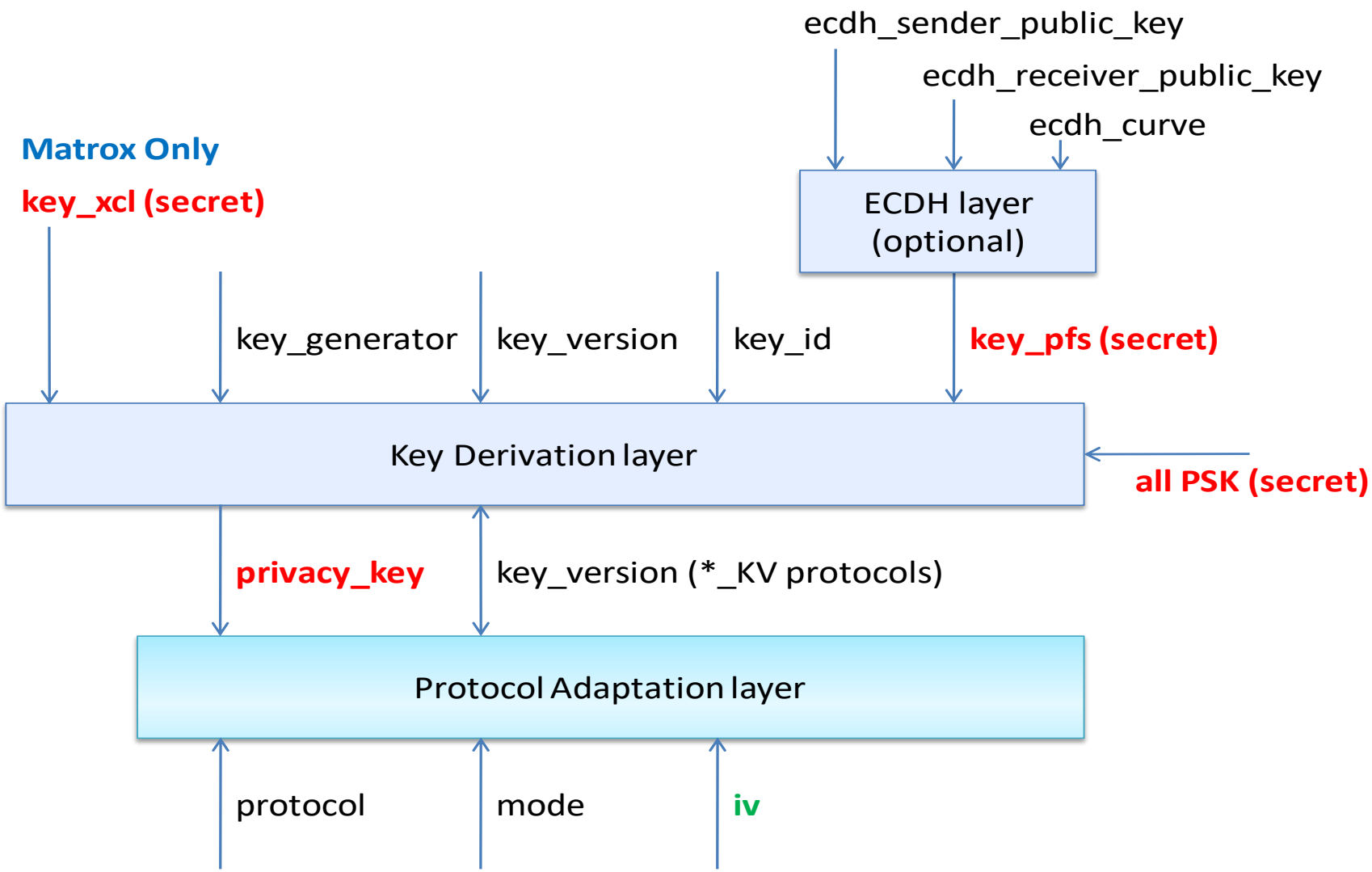
IPMX to IPMX devices is also possible

DNS-SD (DNS or mDNS)

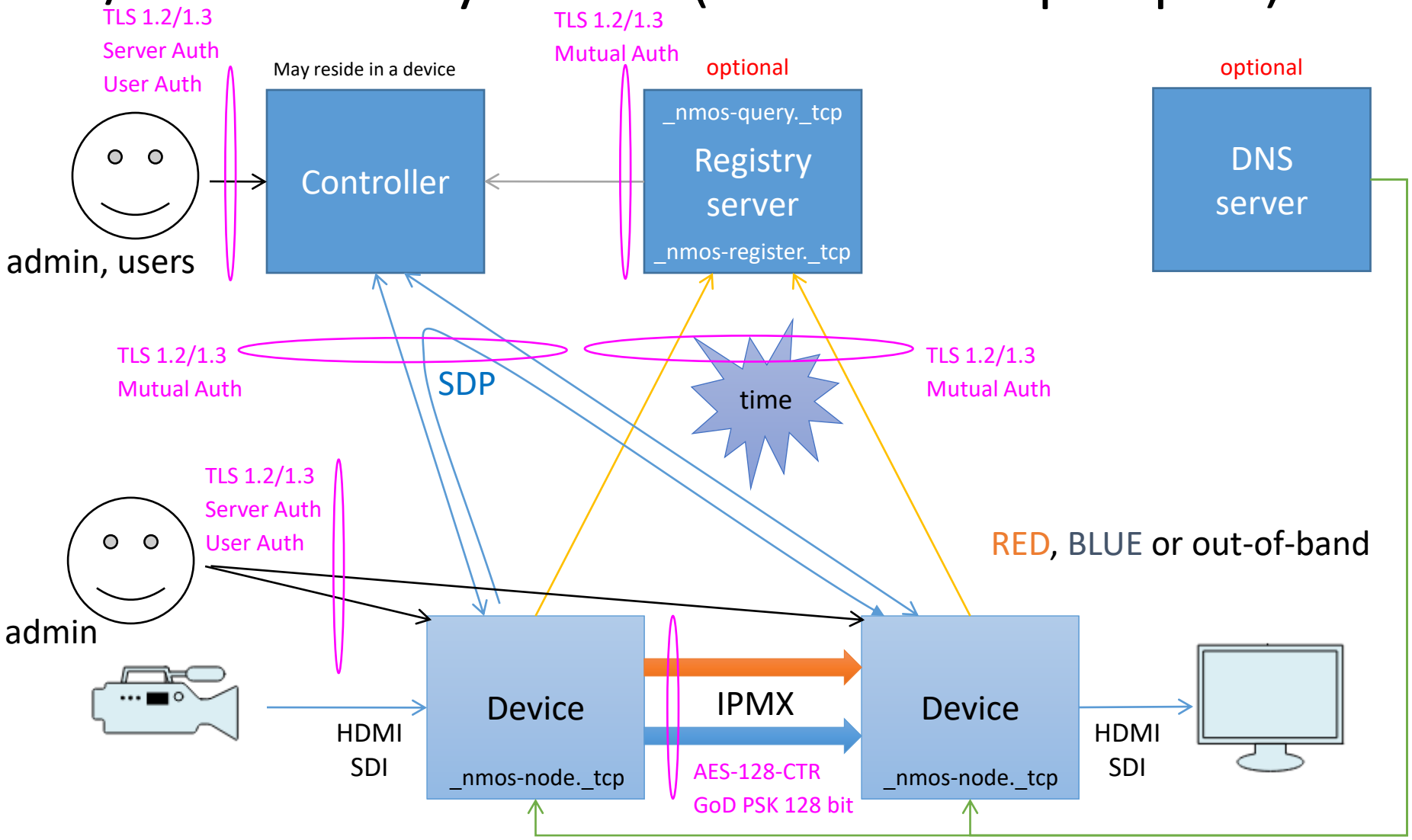
PEP Architecture



PEP Key Derivation



IPMX / NMOS System (normal opaque)



IPMX to IPMX devices is also possible

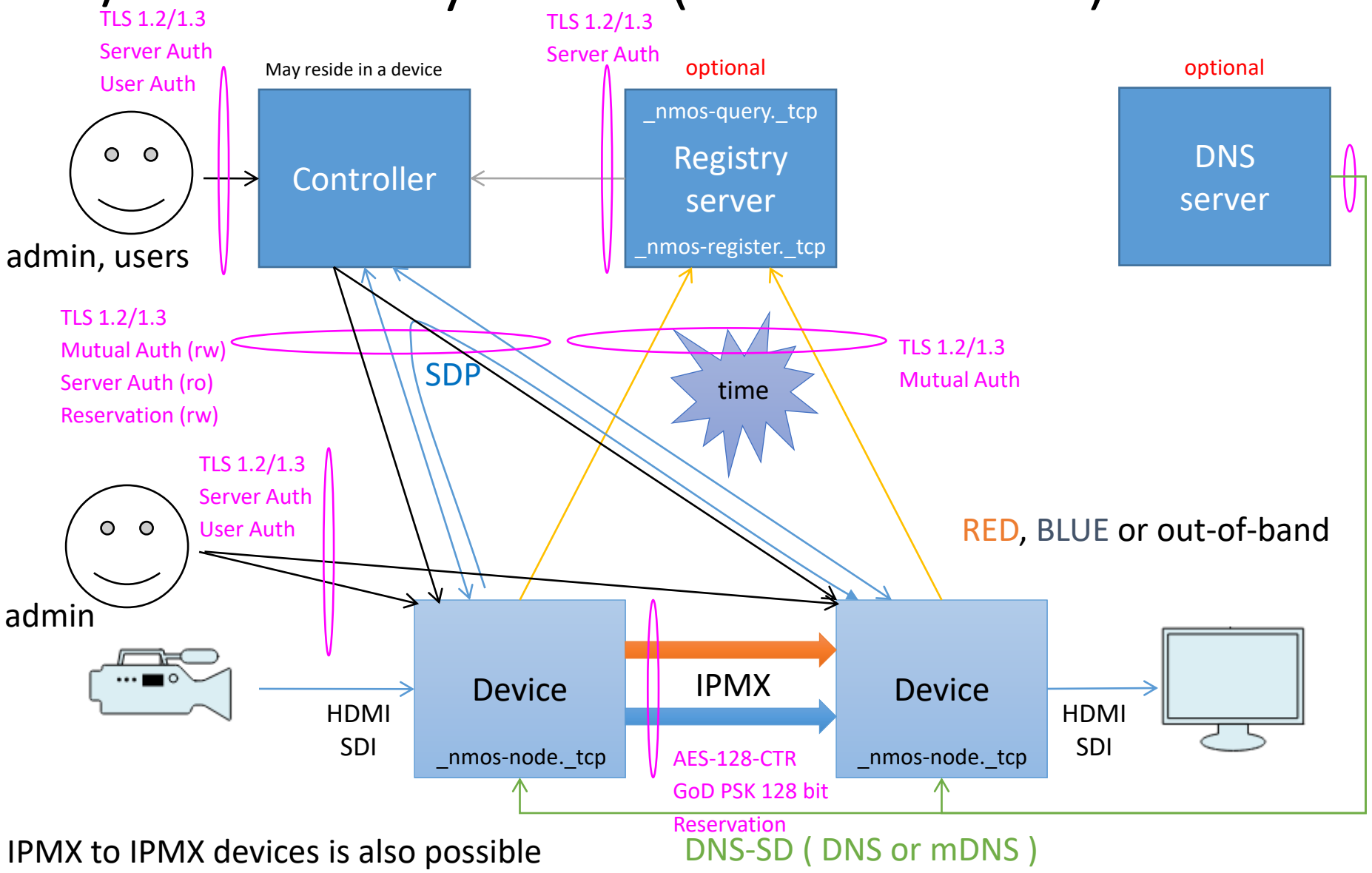
DNS-SD (DNS or mDNS)

IPMX / NMOS System (reservation)

- Matrox NMOS Exclusive Node Reservation API (urn:x-matrox:service:exclusive/v1.0)
  - Add key material in PEP (key_xcl)
  - Add authorizations to the device's NMOS API
    - Use either or both Exclusive or/and OAuth2 bearer tokens
- Scenario
  - A controller generate a random 128 bit exclusive key and acquire the exclusive use of a number of devices.
    - Only the controller owning the devices can operate them
    - Only the devices sharing the same exclusive secret key can share / access the content.

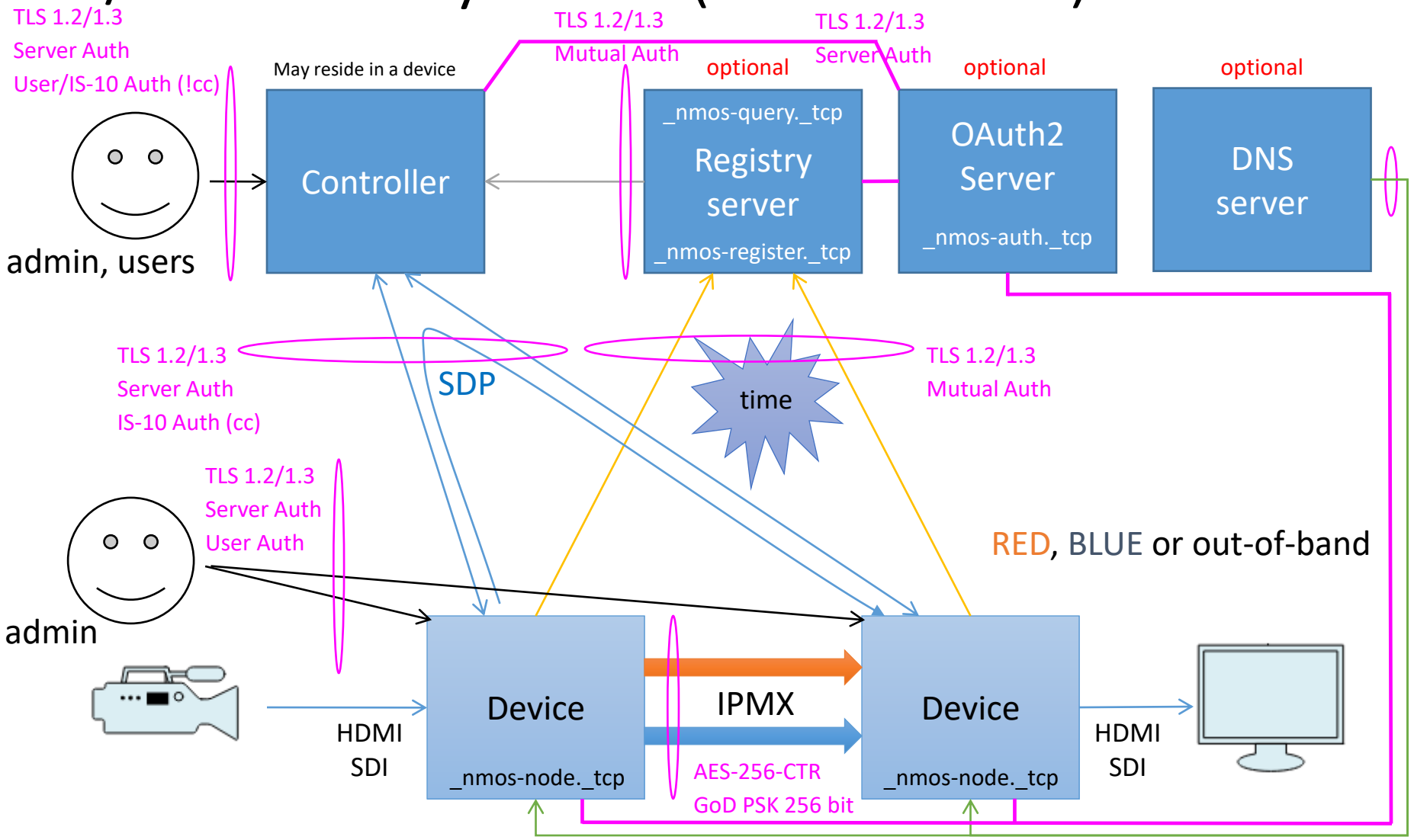
Matrox Only

IPMX / NMOS System (reservation)



IPMX to IPMX devices is also possible

IPMX / NMOS System (enhanced)



IPMX to IPMX devices is also possible

DNS-SD (DNS or mDNS)

Device IS-10 / OAuth2 Authorizations


```
bearer token claims {
        “iss”: “https://oauth2.matrox.com/v1.0“,
        “scope”: ”node connection streamcompatibility”,
        “sub”: ”nmosController-12345”
        “aud”: [“*”],
        “client_id”: ”nmosController-12345”,
        “exp”: 1.720537916e+09,
        “x-nmos-node”: {
                “read”:[“*”], “write”:[“*”] },
        “x-nmos-connection”: {
                “read”:[“*”], “write”:[“*”] },
        “x-nmos-streamcompatibility”: {
                “read”:[“*”], “write”:[“*”]] }
}
```


client_credentials grant
“sub” matching “client_id”

OAuth2 server may explicitly indicate the “grant_type” used to obtain the token

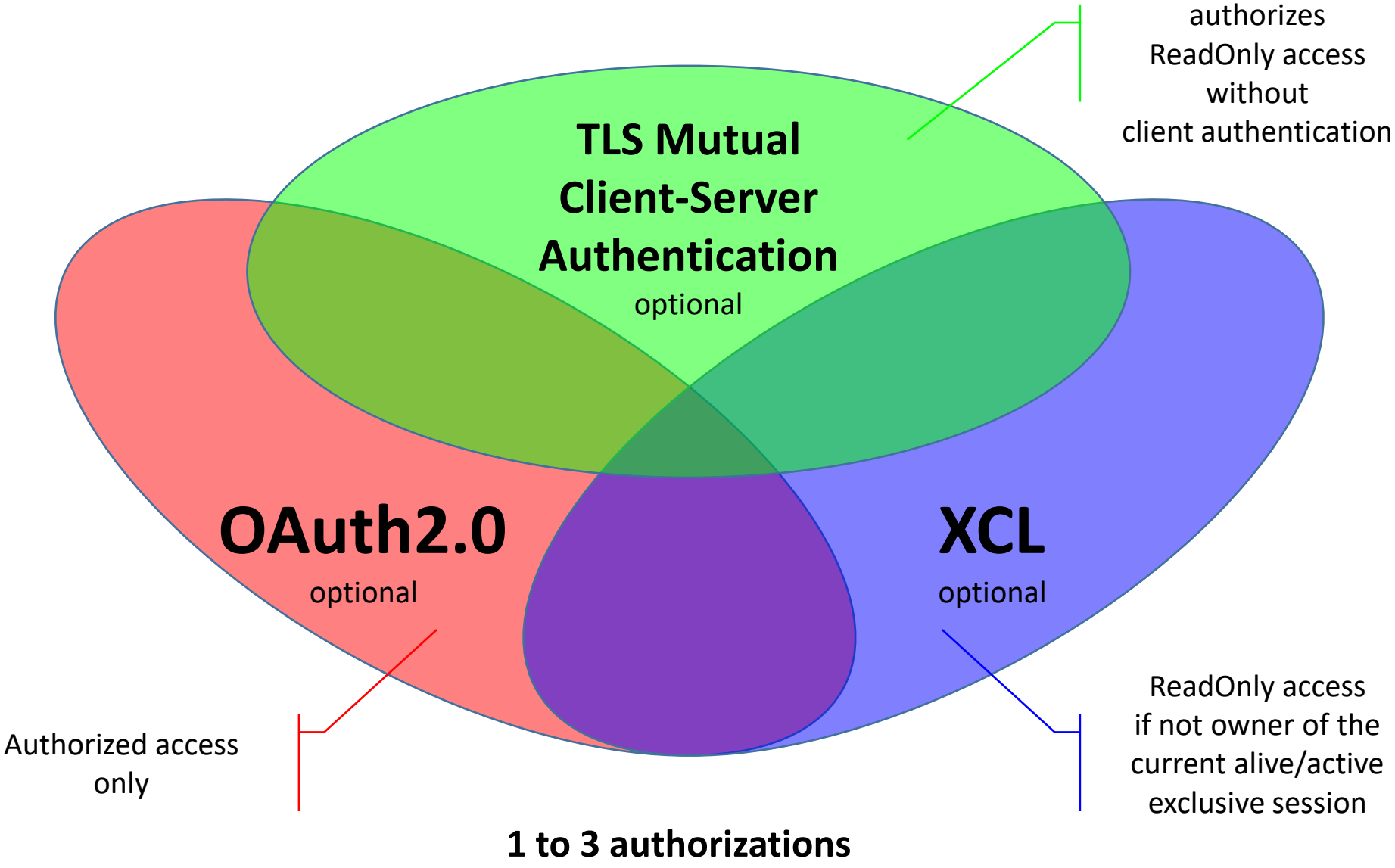
Device IS-10 / OAuth2 Authorizations

```
bearer token claims {
    “iss”: “https://oauth2.matrox.com/v1.0”,
    “scope”: ”offline node connection streamcompatibility”,
    “sub”: ”user@matrox.com”
    “aud”: [“MTXCIP-CC91629”, “MTXCIP-CC91699”],
    “client_id”: "nmosController-54321”,
    “exp”:1.720538859e+09,
    “x-nmos-node”: {
        “read”:[“*”], “write”:[“*”] },
    “x-nmos-connection”: {
        “read”:[“*”], “write”:[“*”] },
    “x-nmos-streamcompatibility”: {
        “read”:[“*”], “write”:[“*”] },
}
```

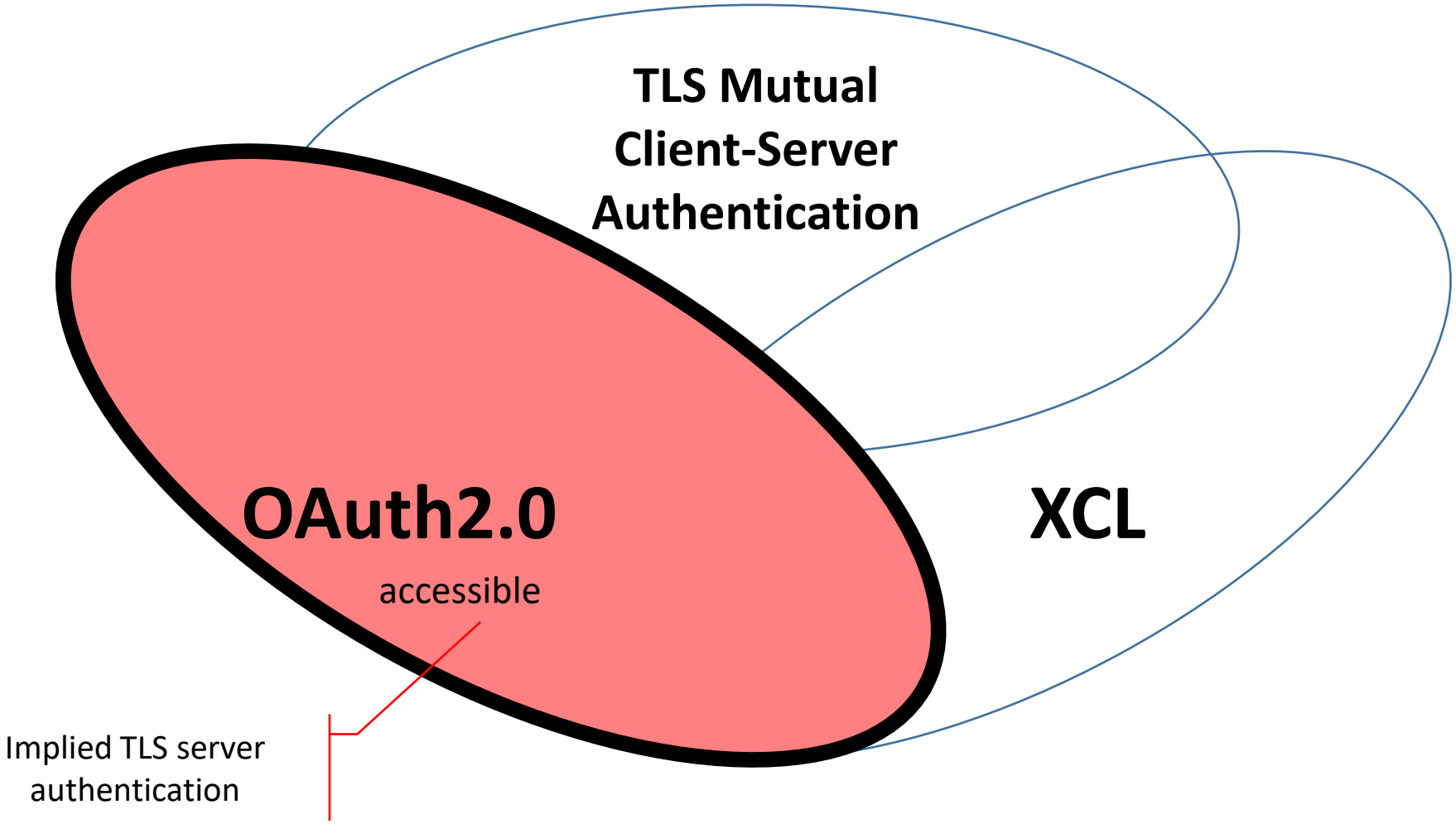
authorisation_code grant
“sub” !matching “client_id”

OAuth2 server may explicitly indicate the “grant_type” used to obtain the token

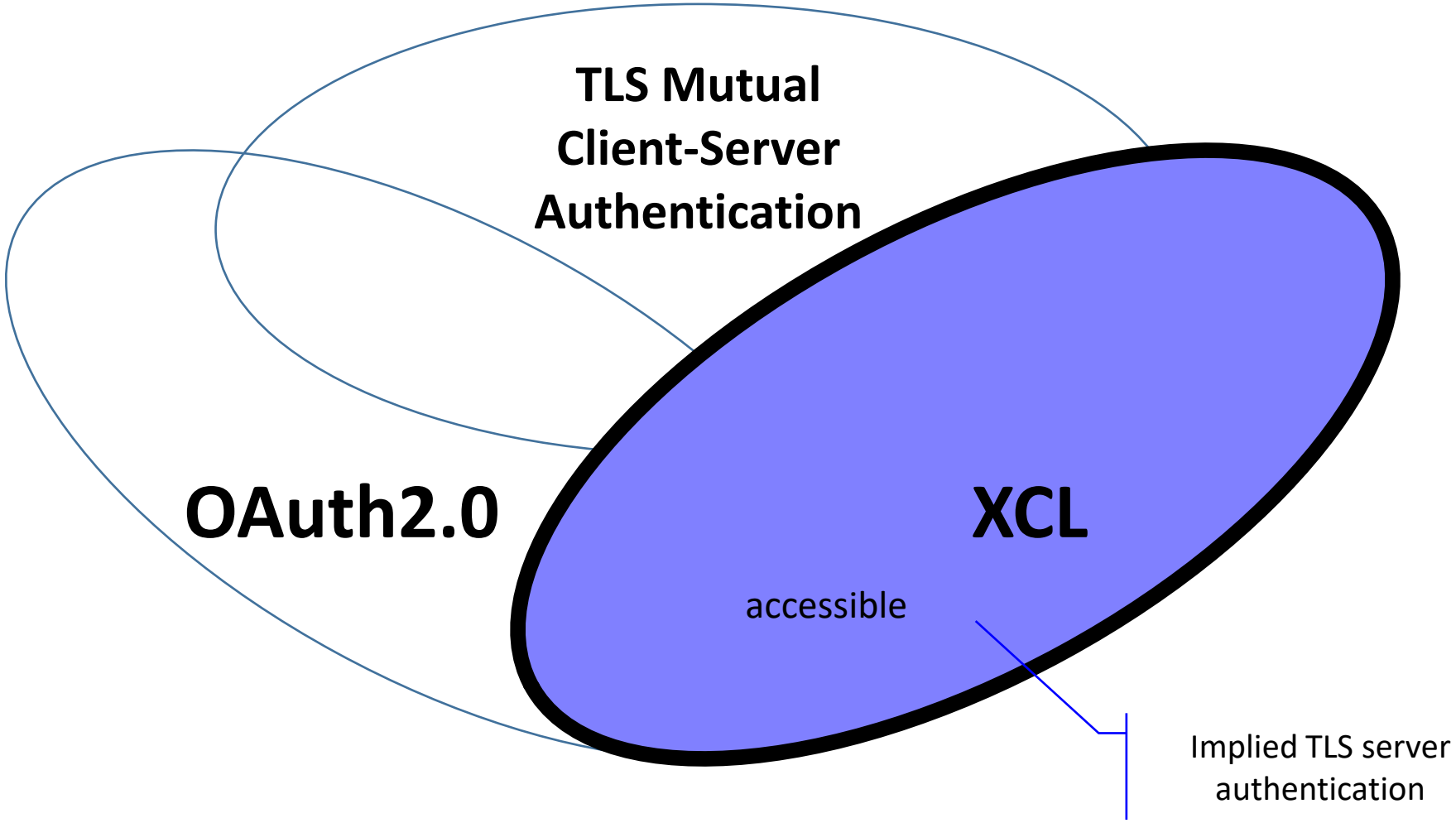
NMOS Node Security



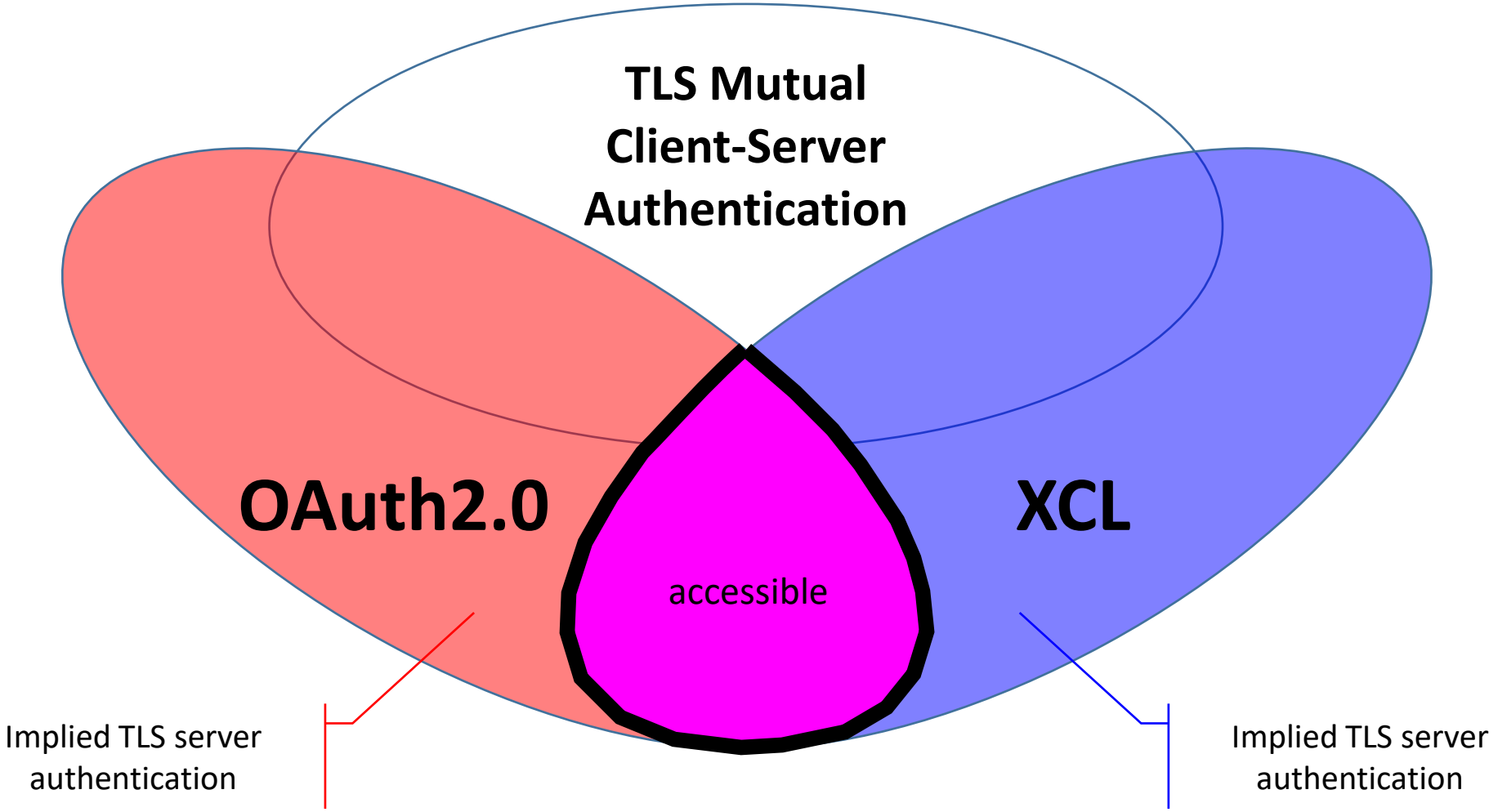
NMOS Node Security



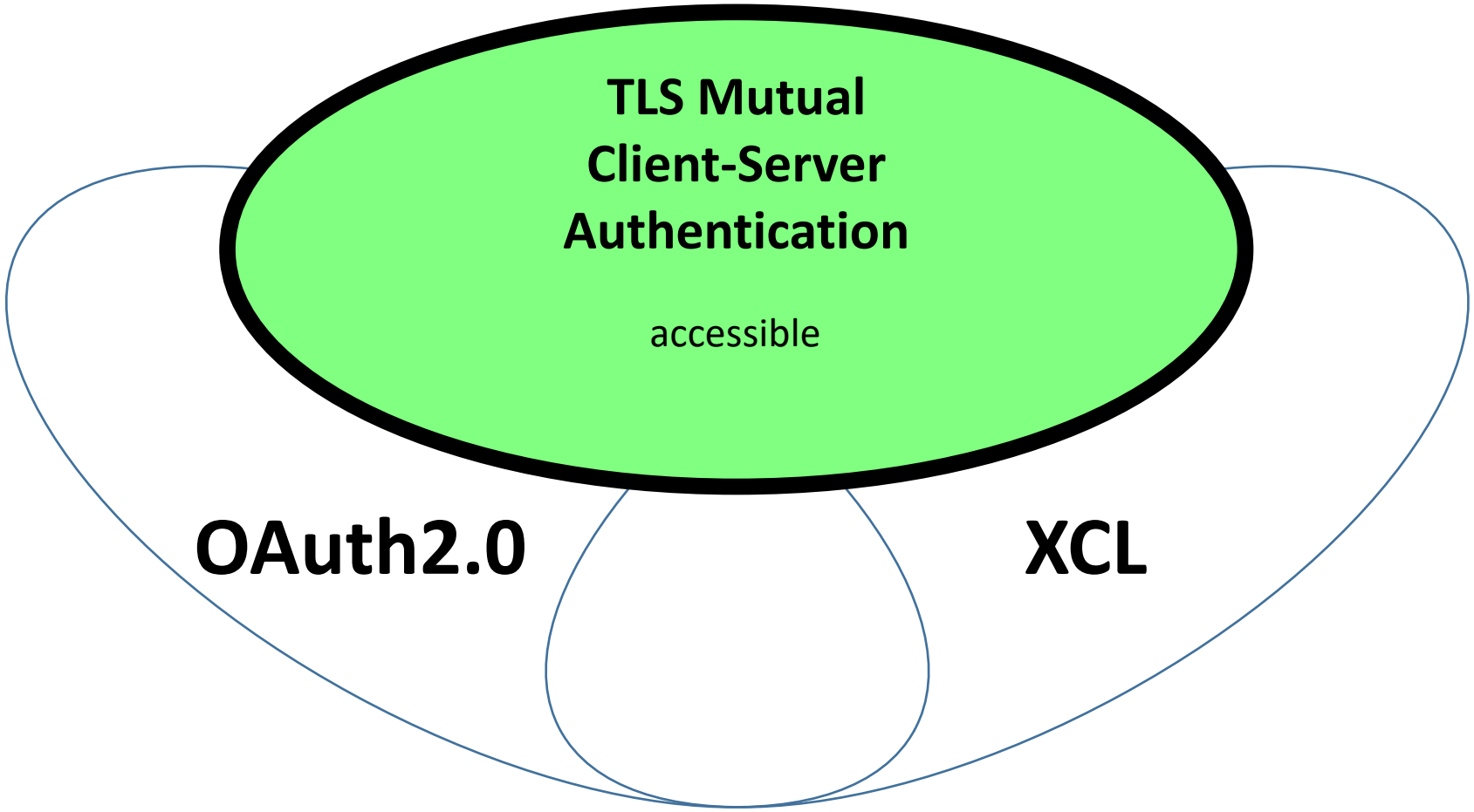
NMOS Node Security



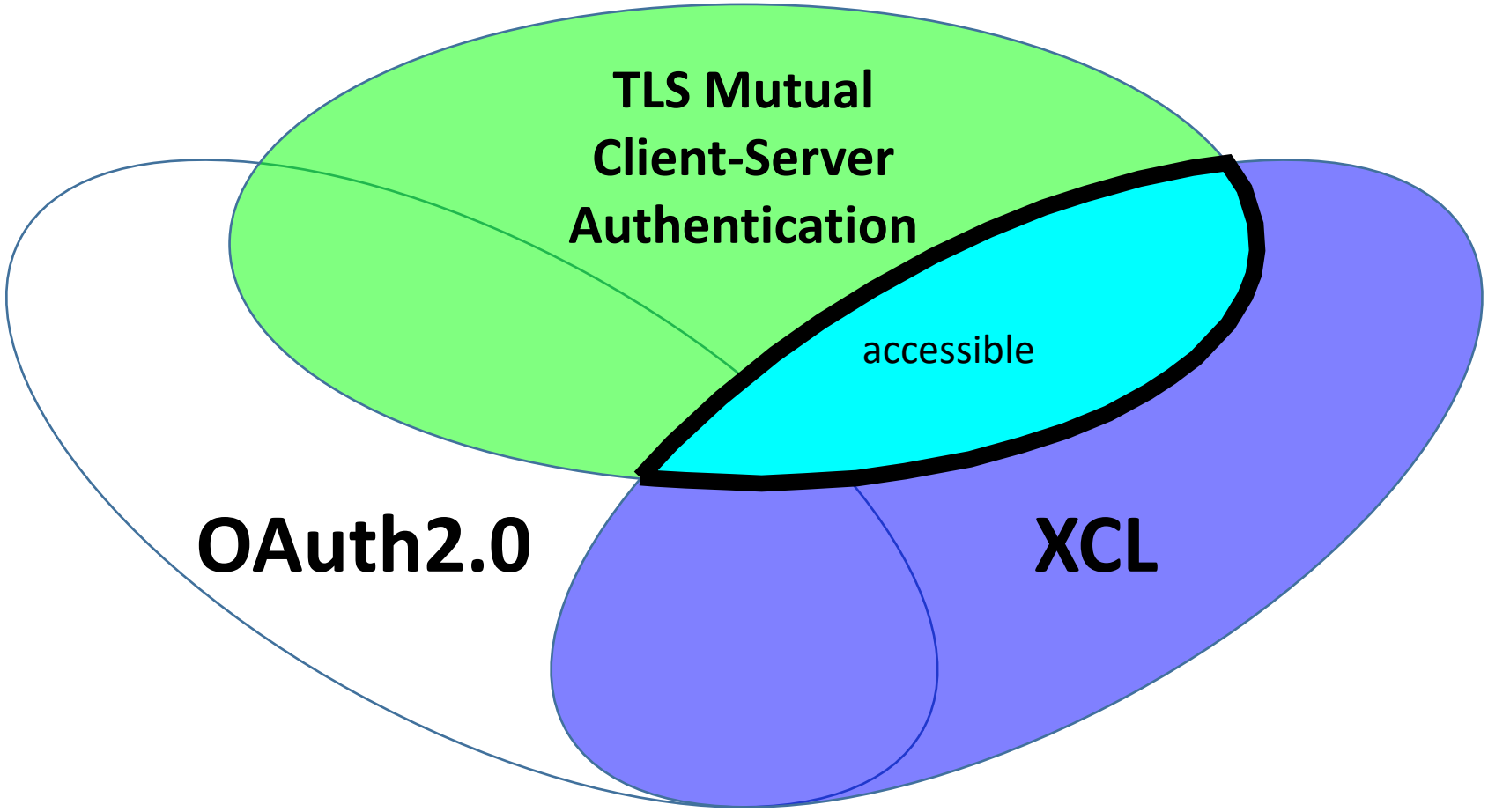
NMOS Node Security



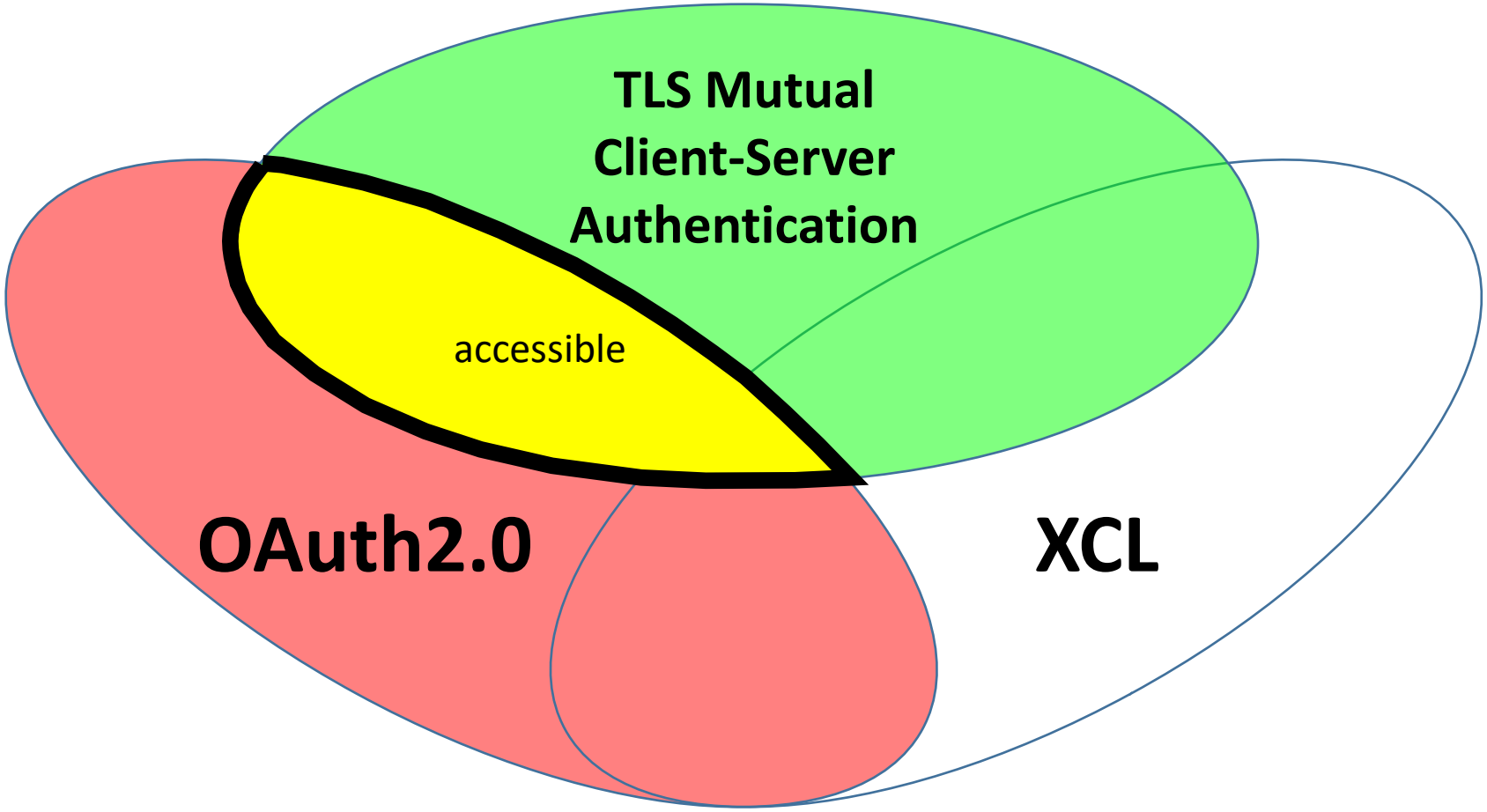
NMOS Node Security



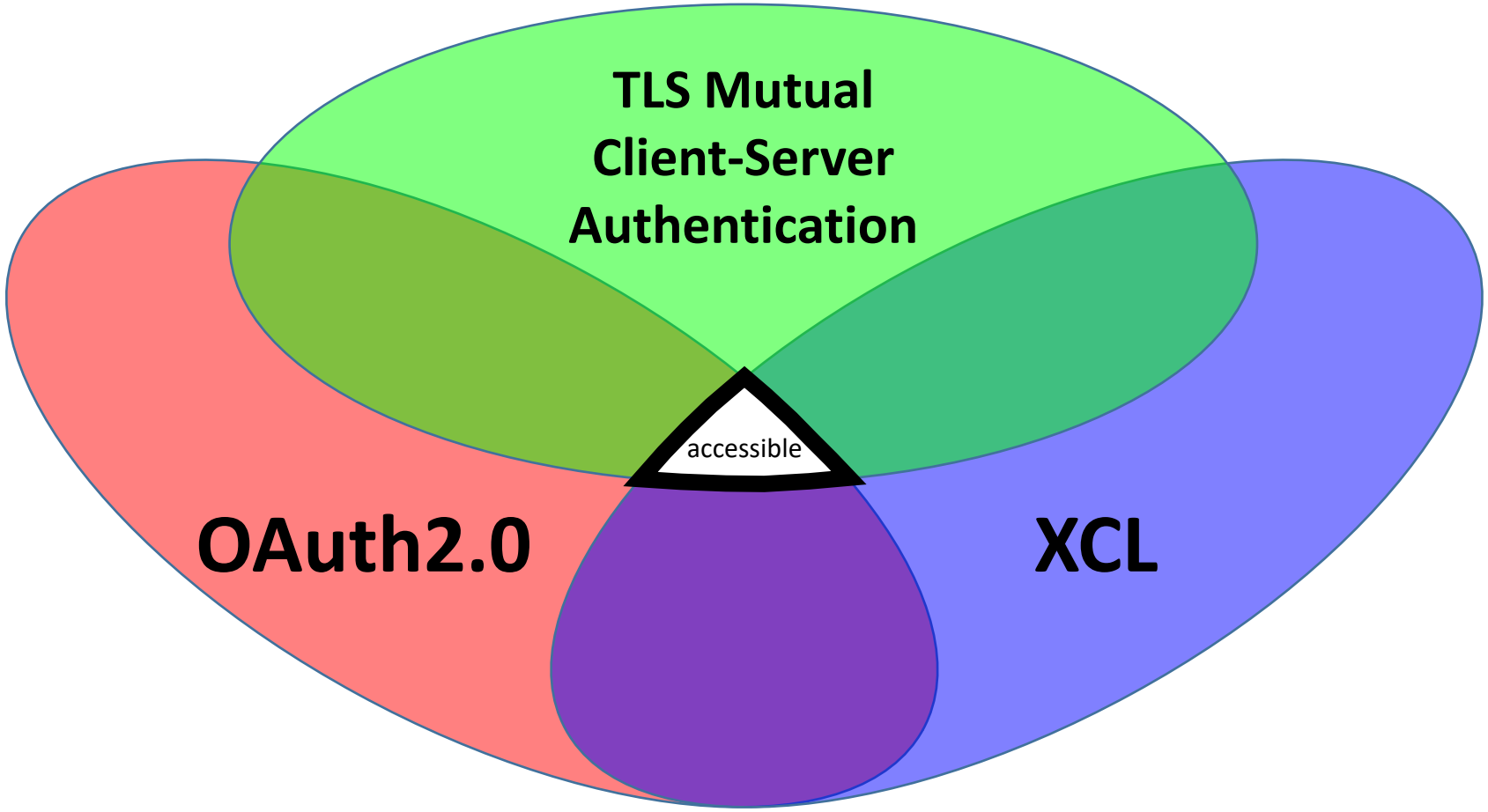
NMOS Node Security



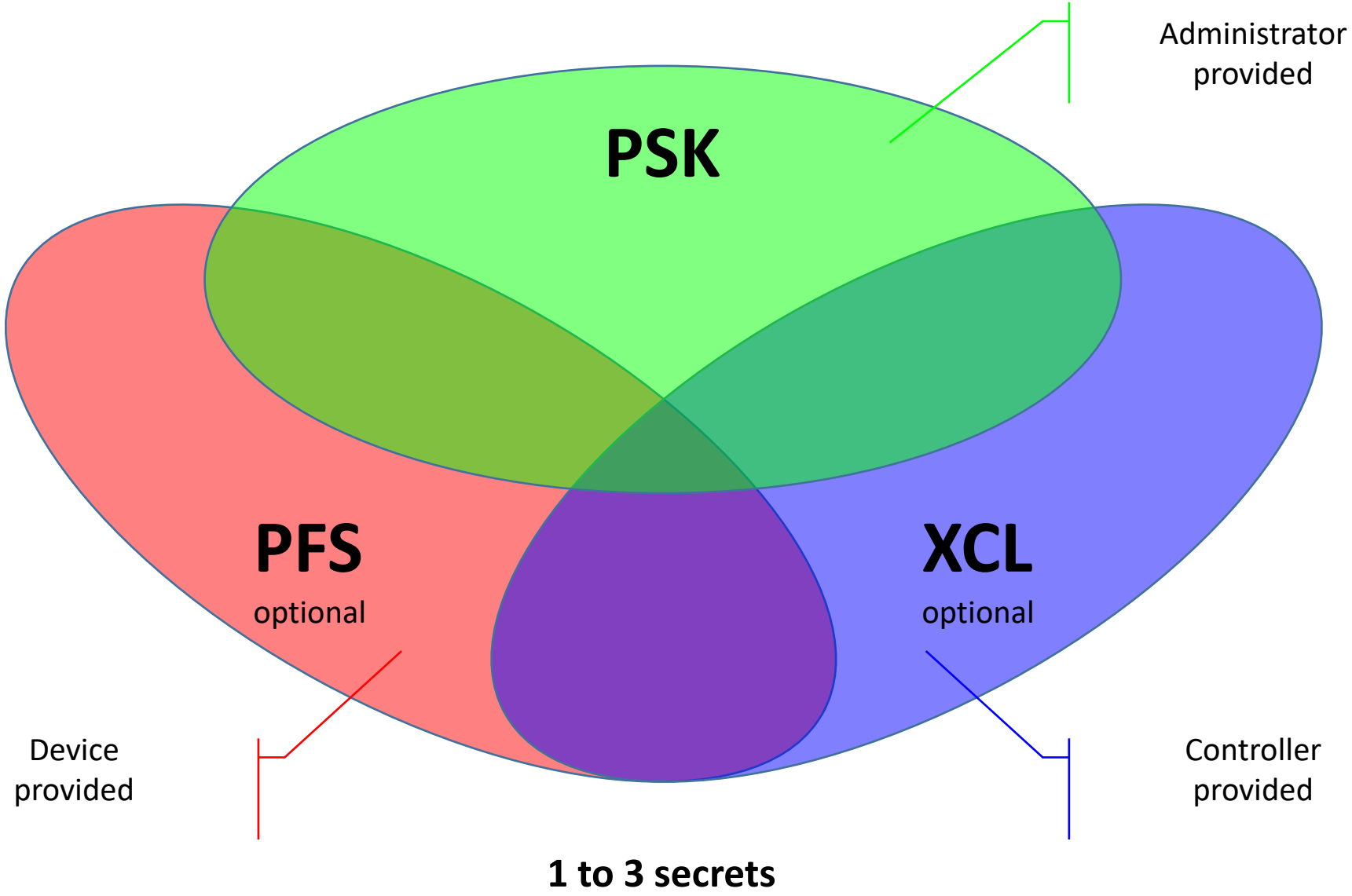
NMOS Node Security



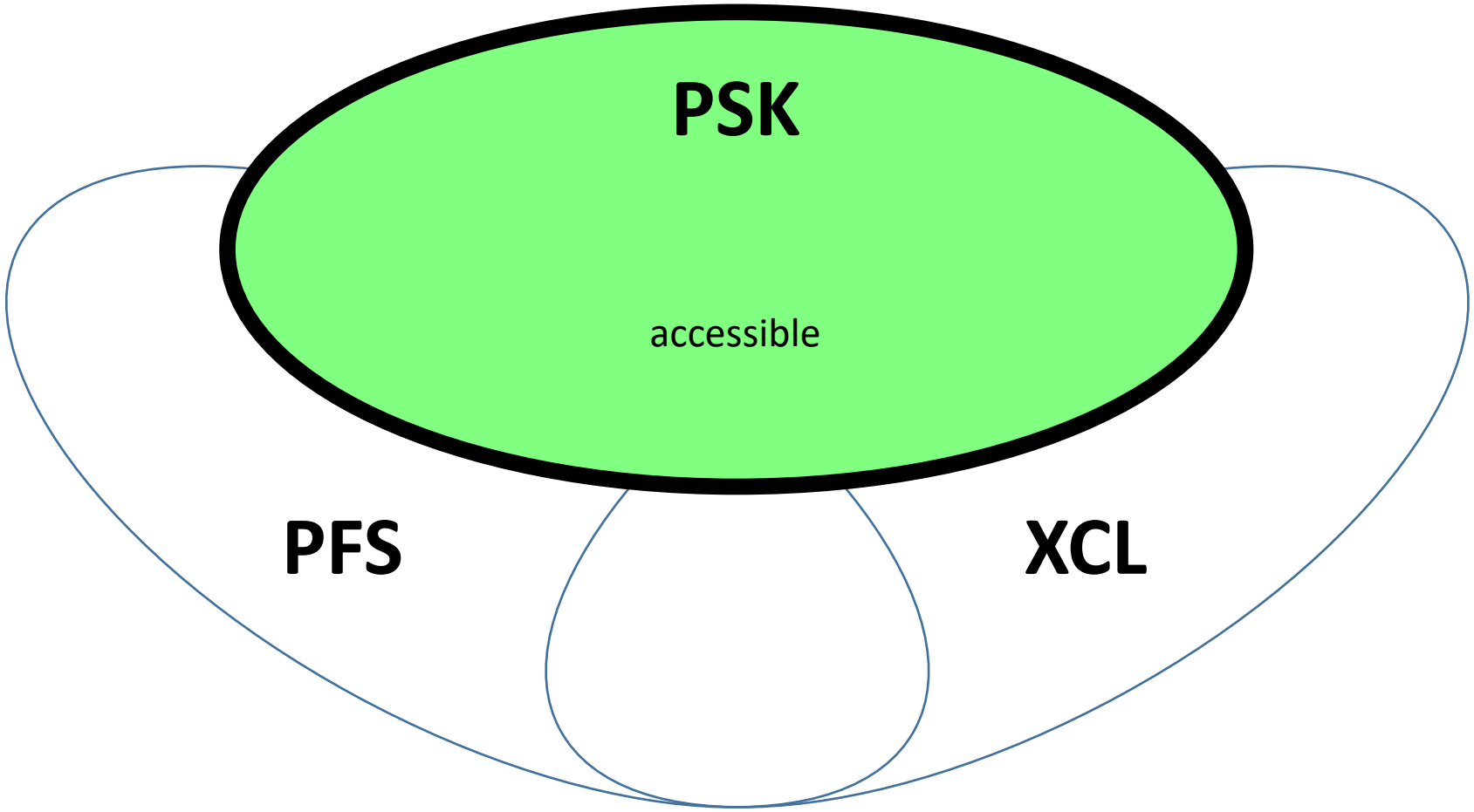
NMOS Node Security



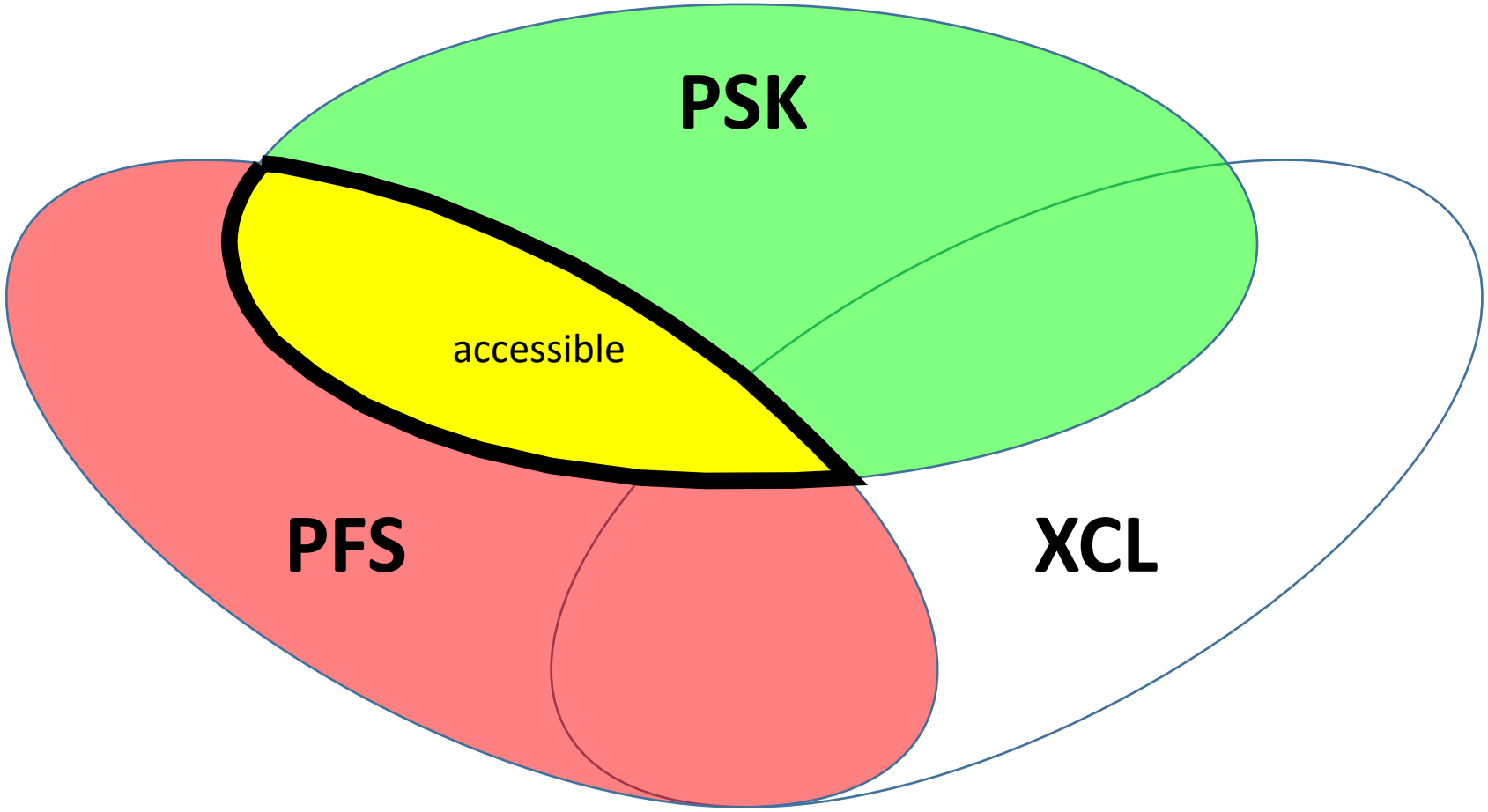
PEP Streaming Security



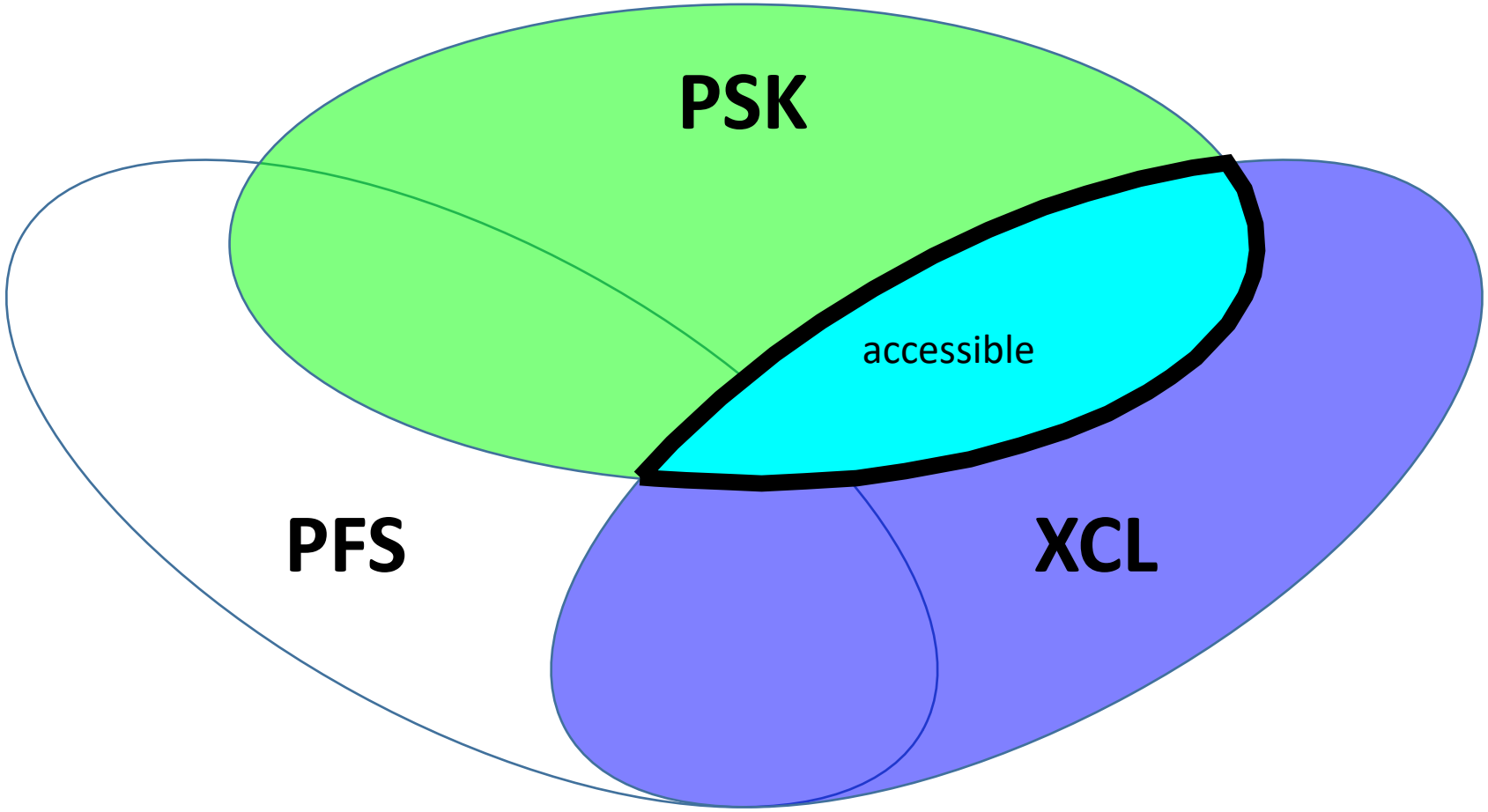
PEP Streaming Security



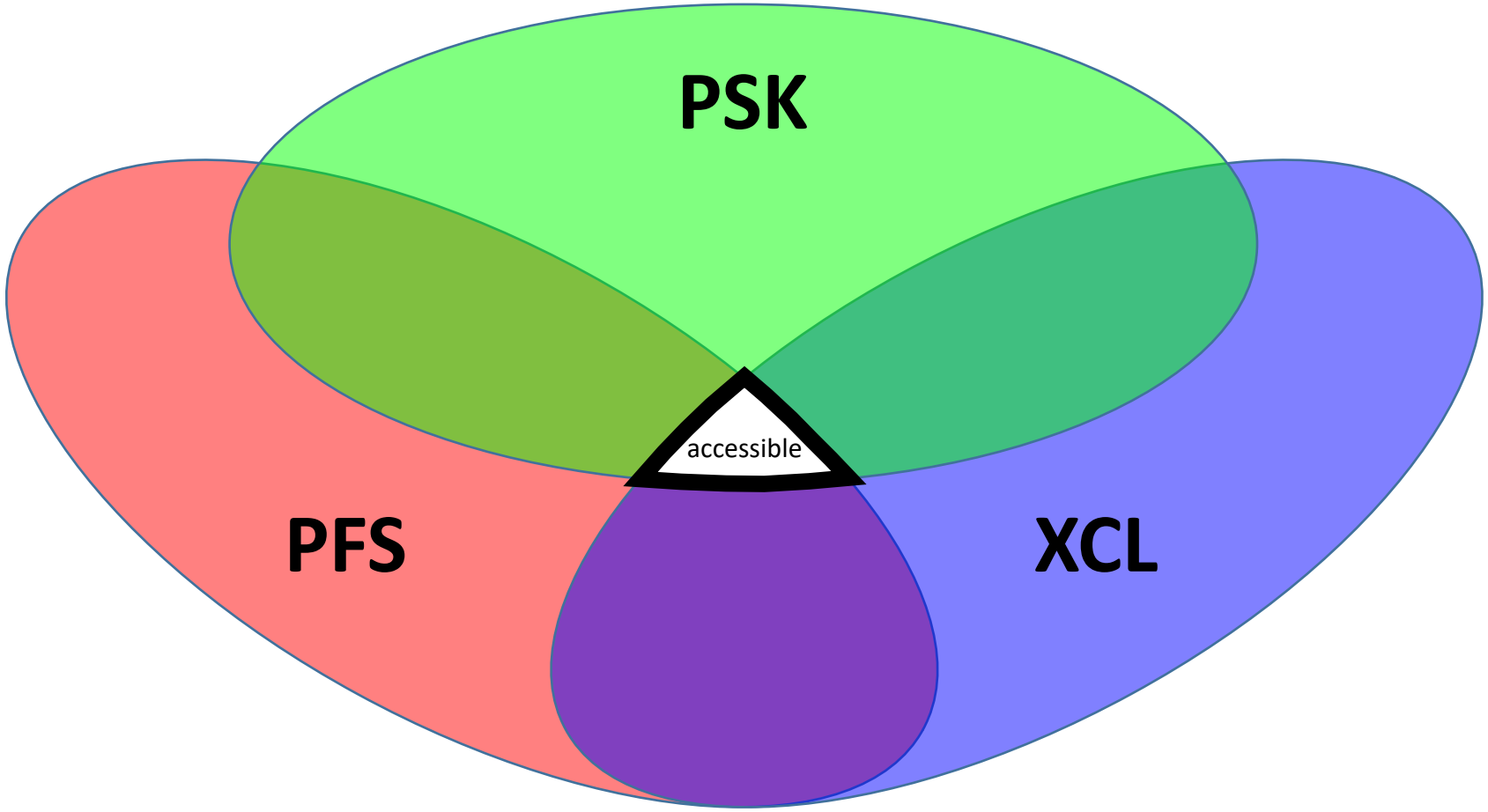
PEP Streaming Security



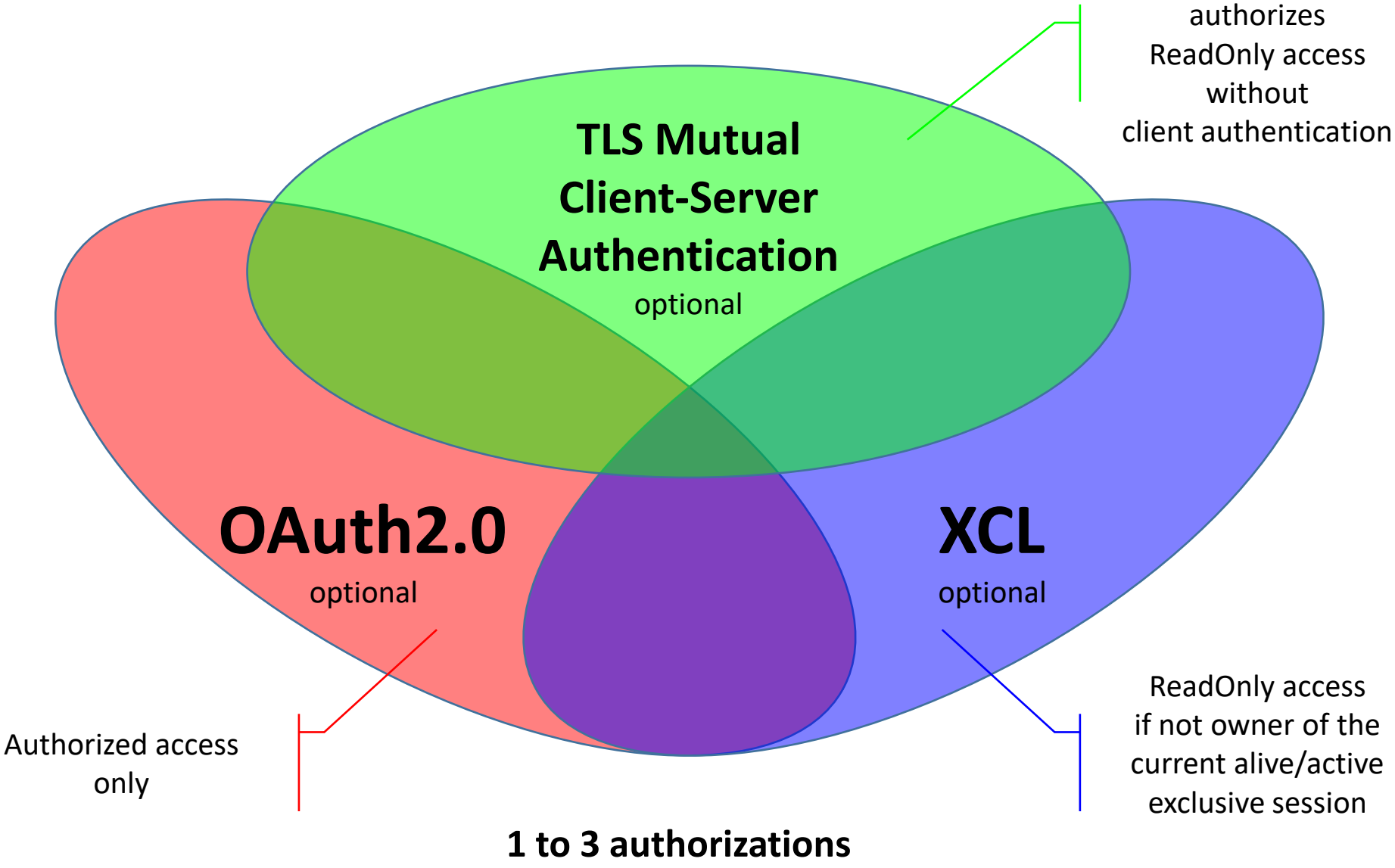
PEP Streaming Security



PEP Streaming Security



NMOS Node Security



- This concludes our tutorial on the security aspects of IPMX NMOS Systems.
- If you have any questions, feel free to reach out at abouchar@matrox.com.
- Thank you for attending.