NMOS **A**dvanced **S**treaming **A**rchitecture

USB and more ...

Alain Bouchard, ing

v0.3

Public GitHub Repository

- https://github.com/alabou/NMOS-MatroxOnly
  - README.md

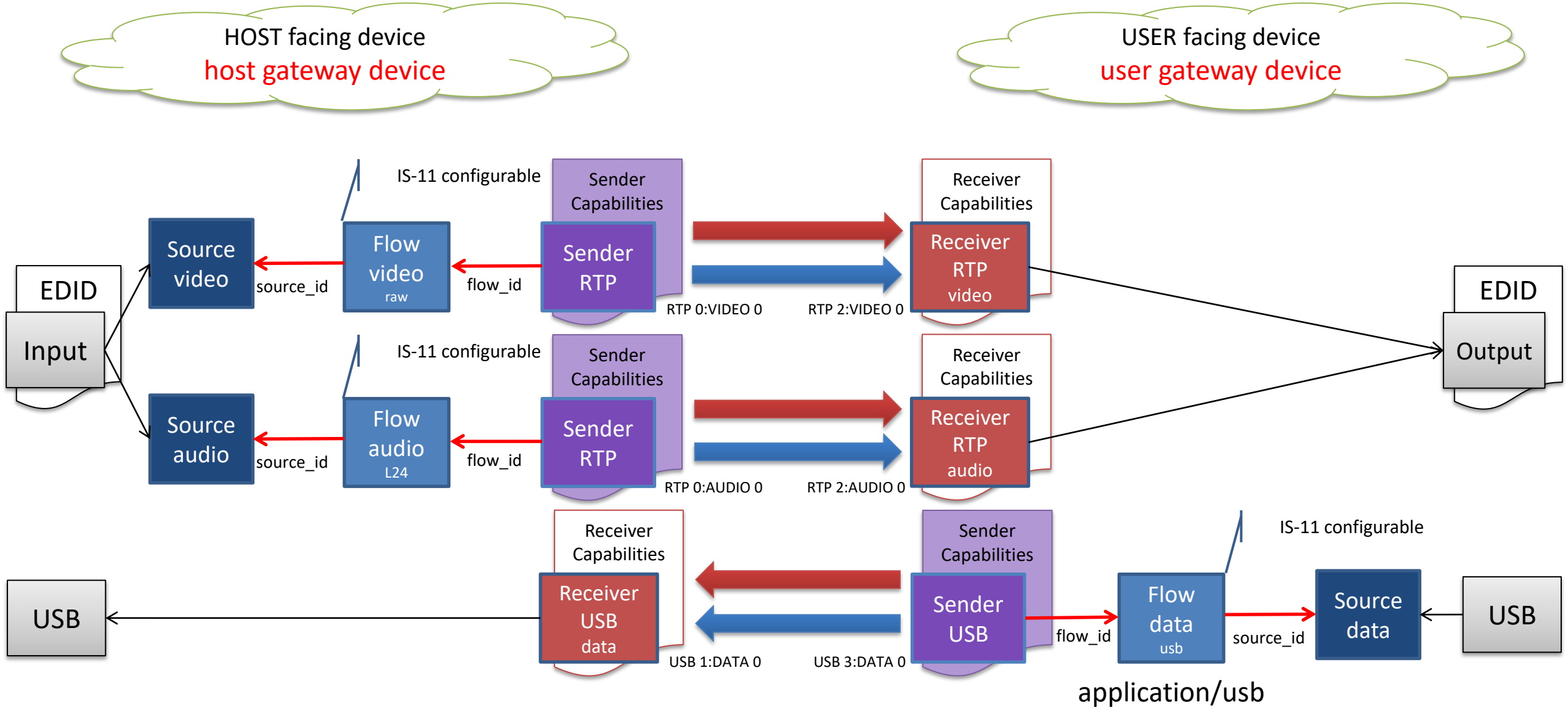
  - NMOS With USB.md
  - NMOS With IPMX.md
  - NMOS With Privacy Encryption.md
  - NMOS With Node Reservation.md

IPMX/USB Transport

- Technical Recommendation VSF_TR-10-14, IPMX USB
  - USB **2.0**: Universal Serial Bus Specification Revision 2.0

- Transport over TCP/IP
  - Bidirectional
  - Redundancy
  - Encrypted/Authenticated: VSF_TR-10-13
  - SDP Transport File

Audio, Video and Data Streams



Common USB devices

Device Type	USB Class Name	Class Code
Keyboard / Mouse	Human Interface Device (HID)	3
Flash Drive	Mass Storage	8
Printer	Printer	7
Audio Device	Audio	1
Webcam	Video	14
Network Adapter	Communications and CDC Control	2
Camera	Still Image	6
Smart Card Reader	Smart Card	13

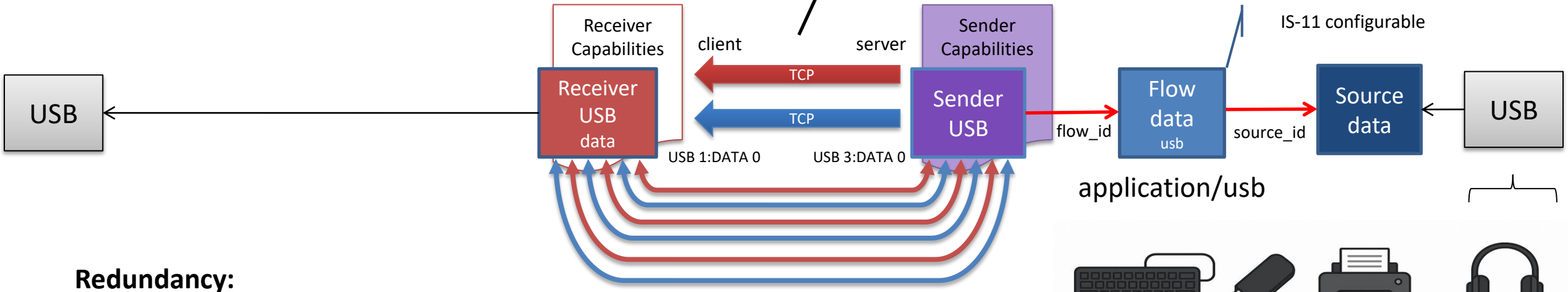
usb_class parameter

Data Stream => bidirectional sub-streams

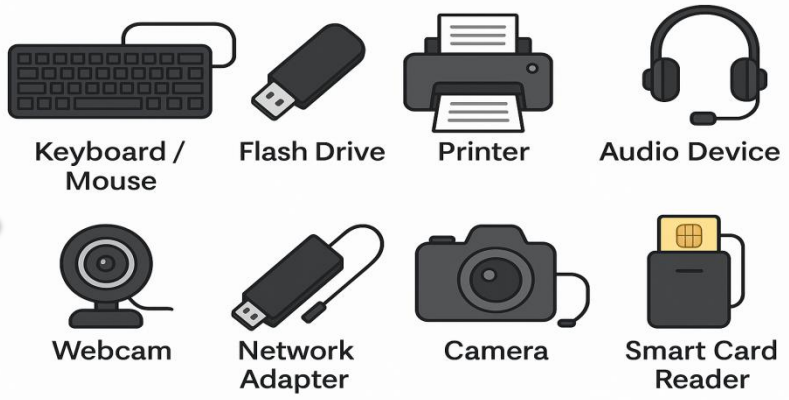
USER facing device
user gateway device

HOST facing device
host gateway device

Controller sees only one TCP data stream



Per USB device bidirectional sub-streams



dynamic devices

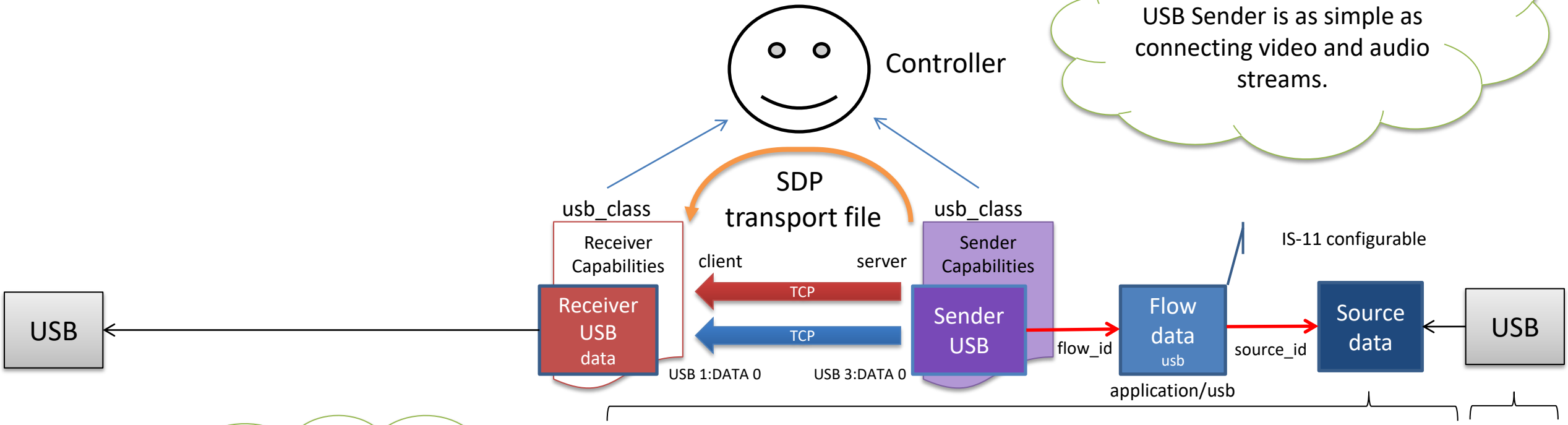
Redundancy:

Audio and Video uses ST 2022-7
=> red-blue redundant interfaces.

➔ USB uses MPTCP over the red-blue redundant interfaces

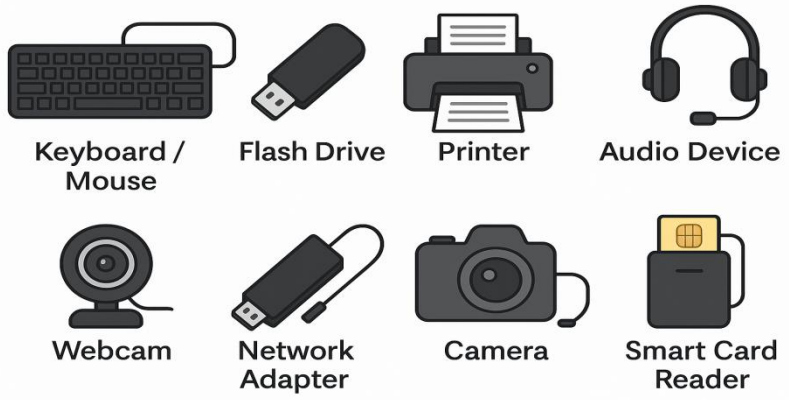
Data Stream => compatibility and connection

Connecting a Receiver to a USB Sender is as simple as connecting video and audio streams.



Source's attribute **usb_devices** may provide the list of USB devices that are active within the USB data stream.

```
usb_device {
    ipmx_bus_id: [64]integer
    class: []integer // Class Code
    vendor: integer
    product: integer
    serial: string
}
```



based on the organization's security policies

SDP Transport File

```
v=0
o=- 1730740959 1730740959 IN IP4 10.0.59.30
s=Device [MTX05079] – USB data stream 0
t=0 0
m=application 27502 TCP usb
c=IN IP4 10.0.59.30
a=ts-refclk:ptp=IEEE1588-2008:39-A7-94-FF-FE-07-CB-D0:00
a=mediaclk:direct=0
a=privacy:protocol=USB_KV; mode=AES-128-CTR_CMAC-64-AAD;
        iv=e06d9bcdb3eb4e5e; key_generator=3318ce76a8858bee4176030390185dd8;
        key_version=e2cb4299; key_id=0001020304050607
a=setup:passive
```

Data Stream => usb_class capabilities and restrictions

Receiver may be configured through a vendor specific mechanism to only support keyboard and mouse.

Controller

Sender may be configured through a vendor specific mechanism to only allow keyboard and mouse.

usb_class

usb_class

Receiver Capabilities

client

server

Sender Capabilities

IS-11 configurable

USB

Receiver USB data

TCP

TCP

Sender USB

flow_id

Flow data usb

source_id

Source data

USB

USB 1:DATA 0

USB 3:DATA 0

application/usb

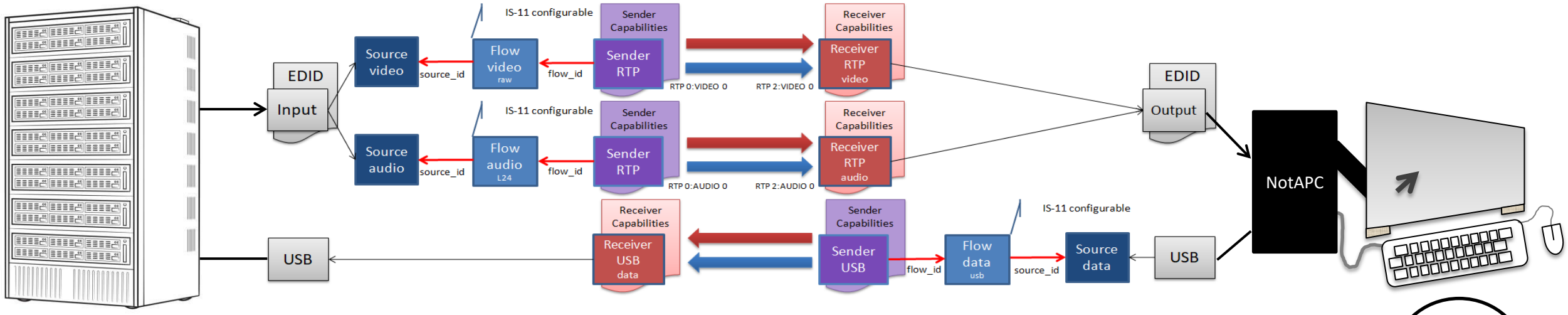
IS-11 active constraints to usb_class restrict the use of some classes of USB devices

based on organization's security policies

Audio, Video and Data Streams

HOST facing device
host gateway device

USER facing device
user gateway device



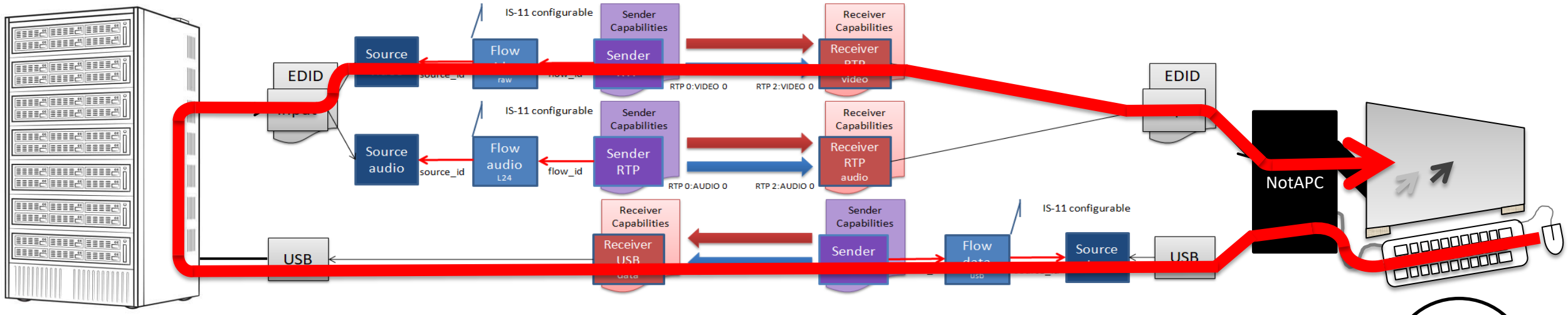
Enterprise Computer Room

User

USB to Video Latency => Mouse to Display

HOST facing device
host gateway device

USER facing device
user gateway device



Enterprise Computer Room

User

Security and USB data integrity

IPMX Privacy Encryption Protocol (PEP)

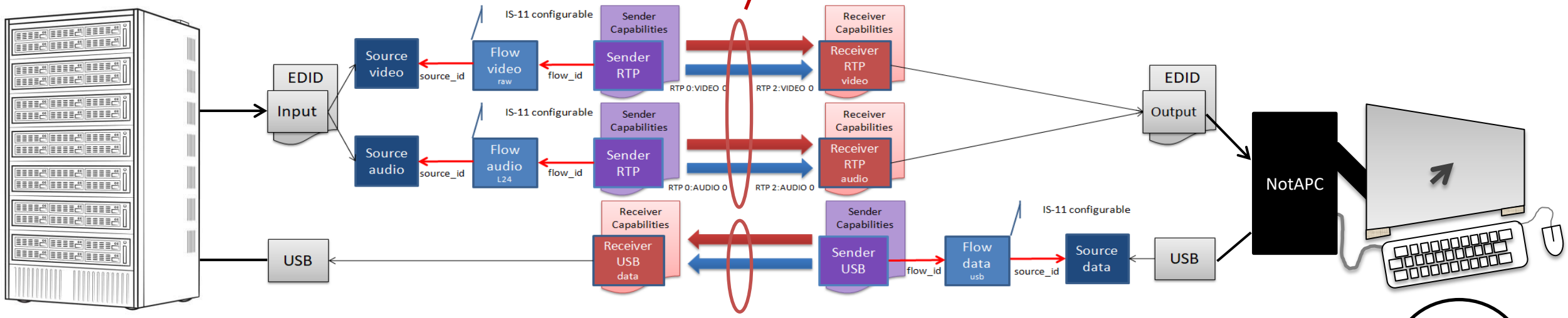
RTP (Required), **RTP_KV**

- **AES-128-CTR (Required)**
- AES-256-CTR
- ECDH_AES-128-CTR
- ECDH_AES-256 .. and many more

USB_KV

- **AES-128-CTR_CMAC-64-AAD (Required)**
- AES-256-CTR_CMAC-64-AAD
- ECDH_AES-128-CTR_CMAC-64-AAD
- ECDH_AES-256- CTR_CMAC-64-AAD

Audio/Video Privacy Encryption parameters are under the control of the **host** facing device.



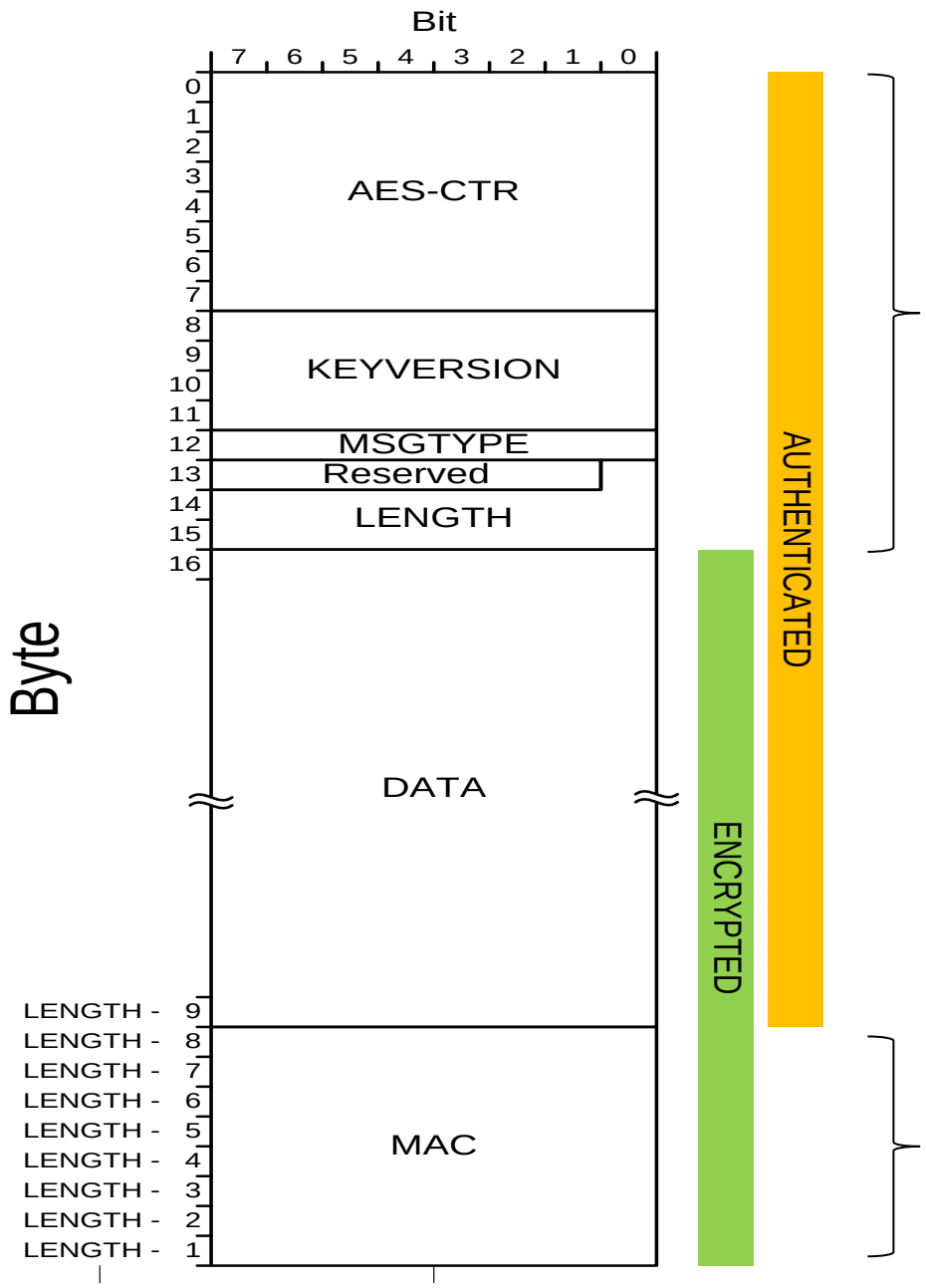
Enterprise Computer Room

USB Privacy Encryption parameters are under the control of the **user** facing device.

User

PEP Transport Parameters

Transport Parameter Name	Type	SDP Name	Sender	Receiver
ext_privacy_protocol	string	protocol	**r/w**	**r/w**
ext_privacy_mode	string	mode	**r/w**	**r/w**
ext_privacy_iv	string	iv	**read-only**	**r/w**
ext_privacy_key_generator	string	key_generator	**read-only**	**r/w**
ext_privacy_key_version	string	key_version	**read-only**	**r/w**
ext_privacy_key_id	string	key_id	**read-only**	**r/w**
ext_privacy_ecdh_sender_public_key	string	-	**read-only**	**r/w**
ext_privacy_ecdh_receiver_public_key	string	**-**	**r/w**	**read-only**
ext_privacy_ecdh_curve	string	**-**	**r/w**	**r/w**

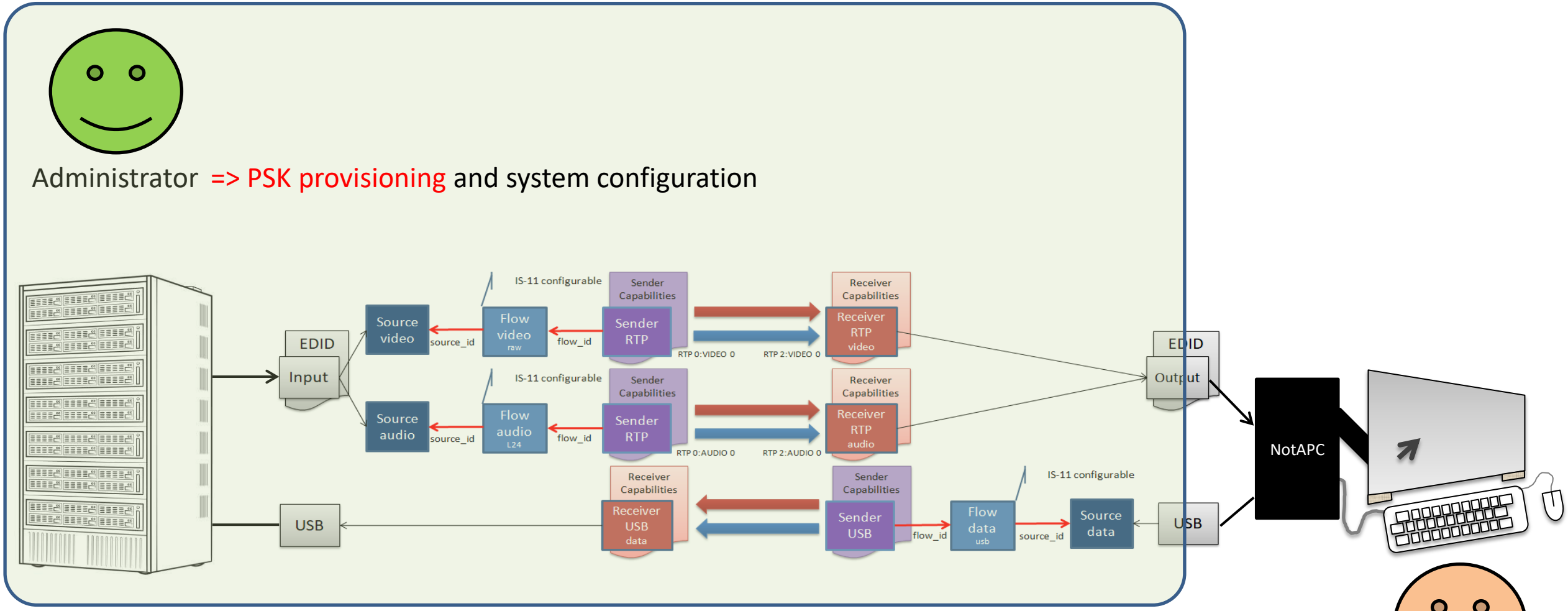


AAD: Additional Authenticated Data

Data that is not part of the payload

MAC is encrypted: mac-then-encrypt

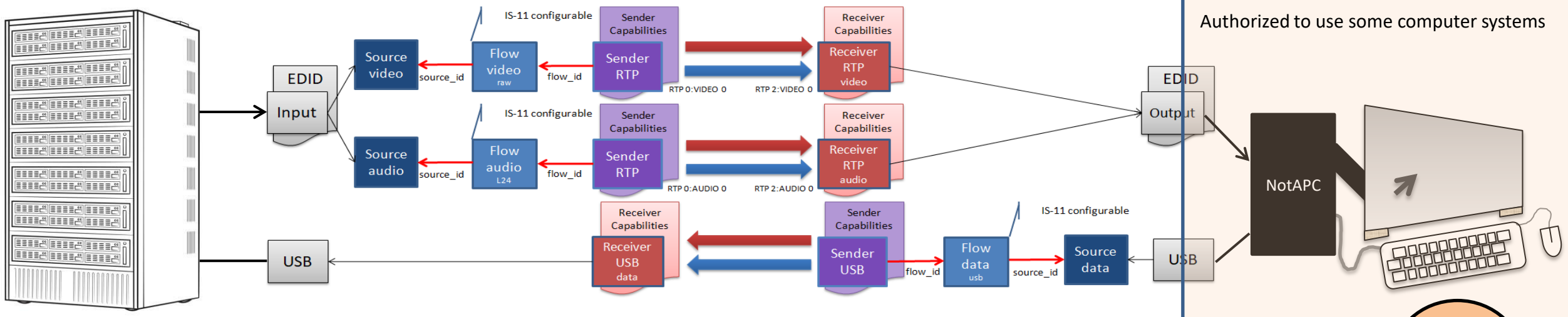
Roles and Actors in the ecosystem: Administrator



Enterprise Computer Room

User

Roles and Actors in the ecosystem: User



Owns USB devices
- files
- images, video, audio
- keyboard keystrokes

Owns sessions in computer systems
- graphics, text, sound
- files, controls

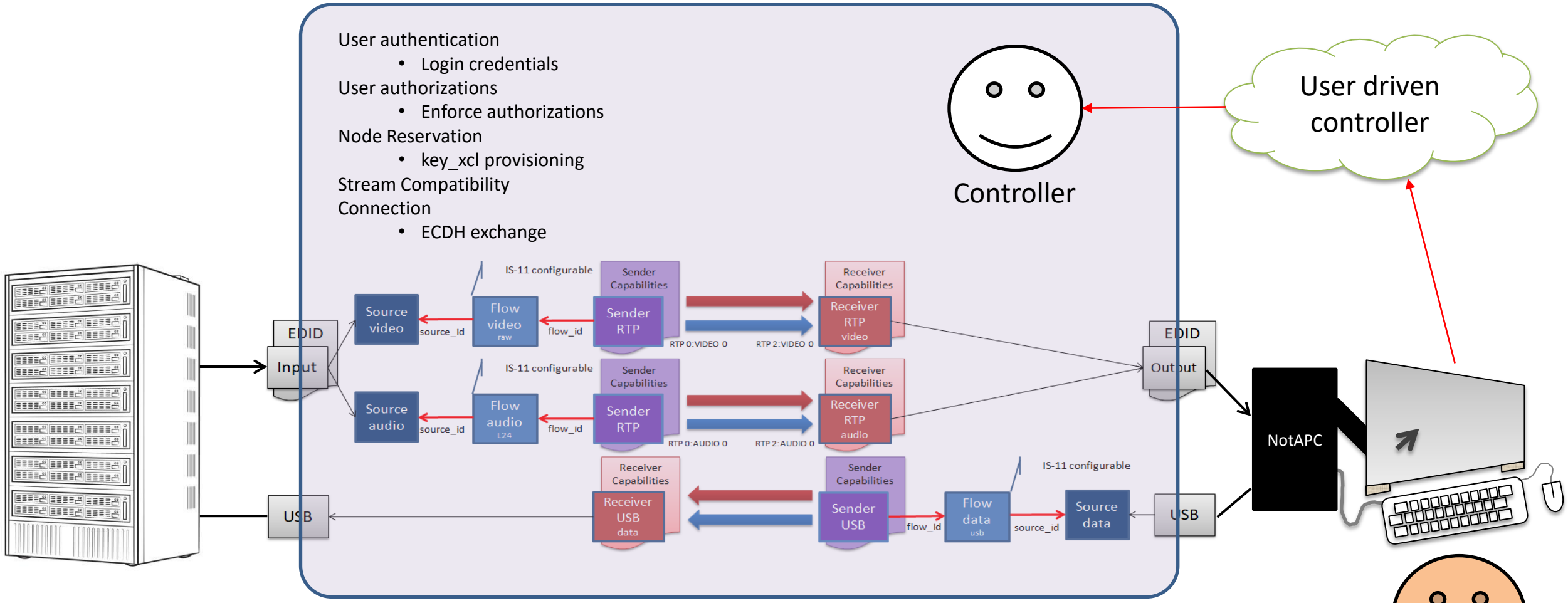
Authorized to use some devices

Authorized to use some computer systems

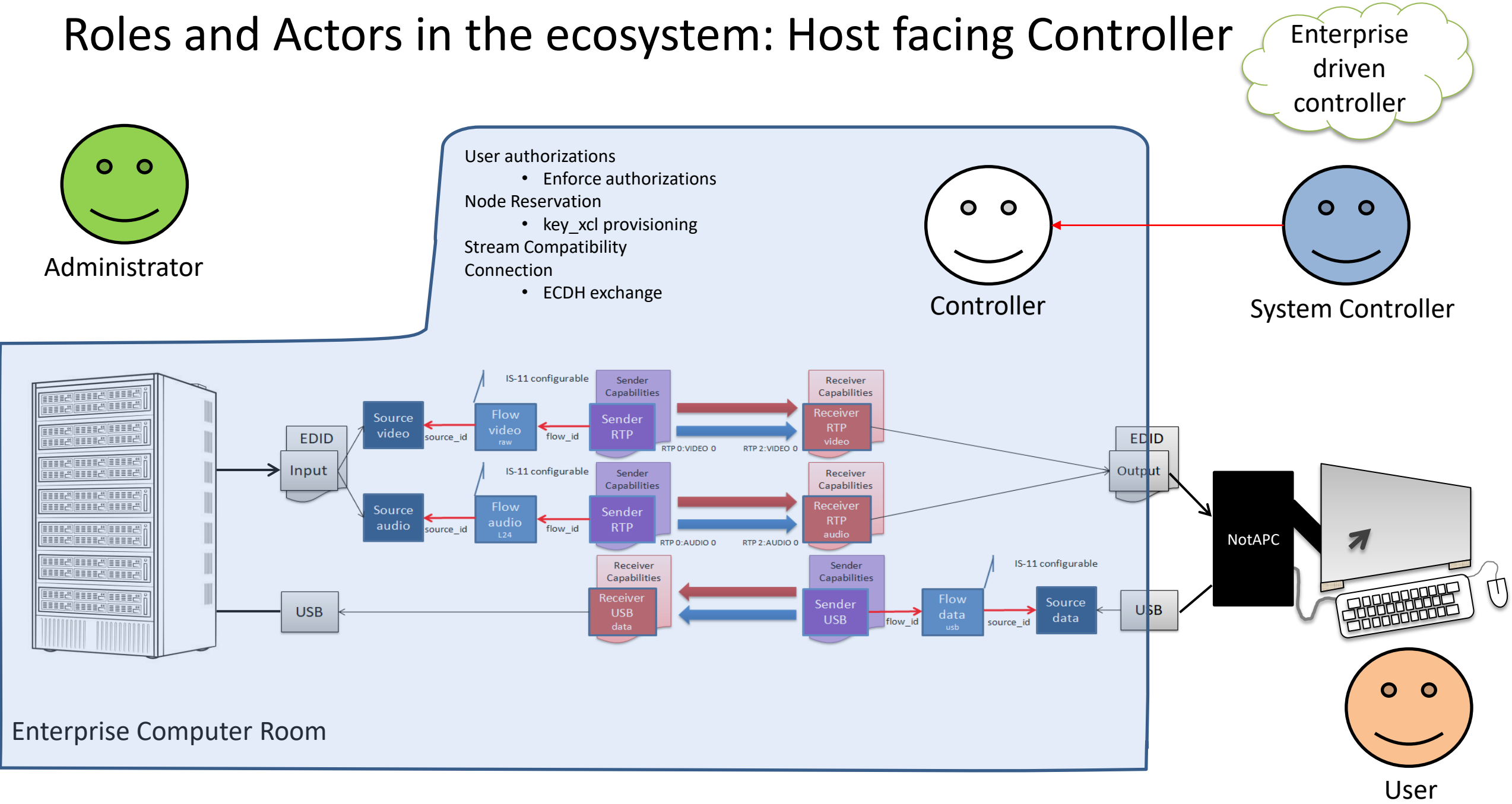
User

Enterprise Computer Room

Roles and Actors in the ecosystem: User facing Controller

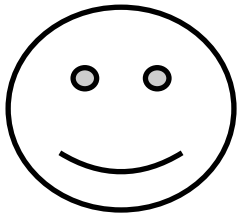


Roles and Actors in the ecosystem: Host facing Controller



Node Reservation

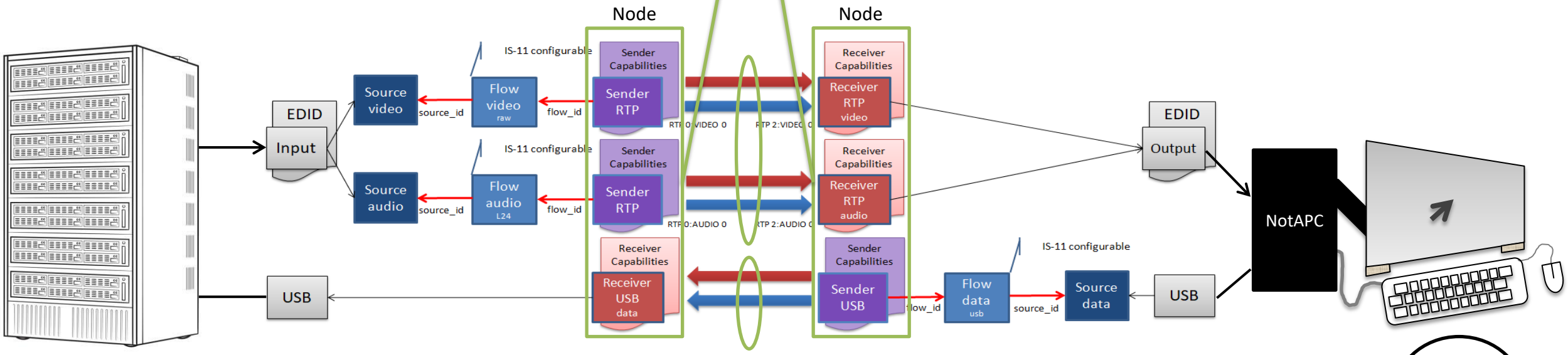
As long as the controller remains the owner
Of the nodes' exclusive session (keep alive),
no other device can control the Nodes,
or access the encrypted media streams.



Controller

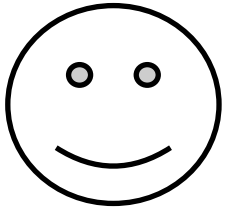
Controller authenticates devices using TLS server certificates.

Atomically ACQUIRE Nodes
=> exclusive session with key_xcl



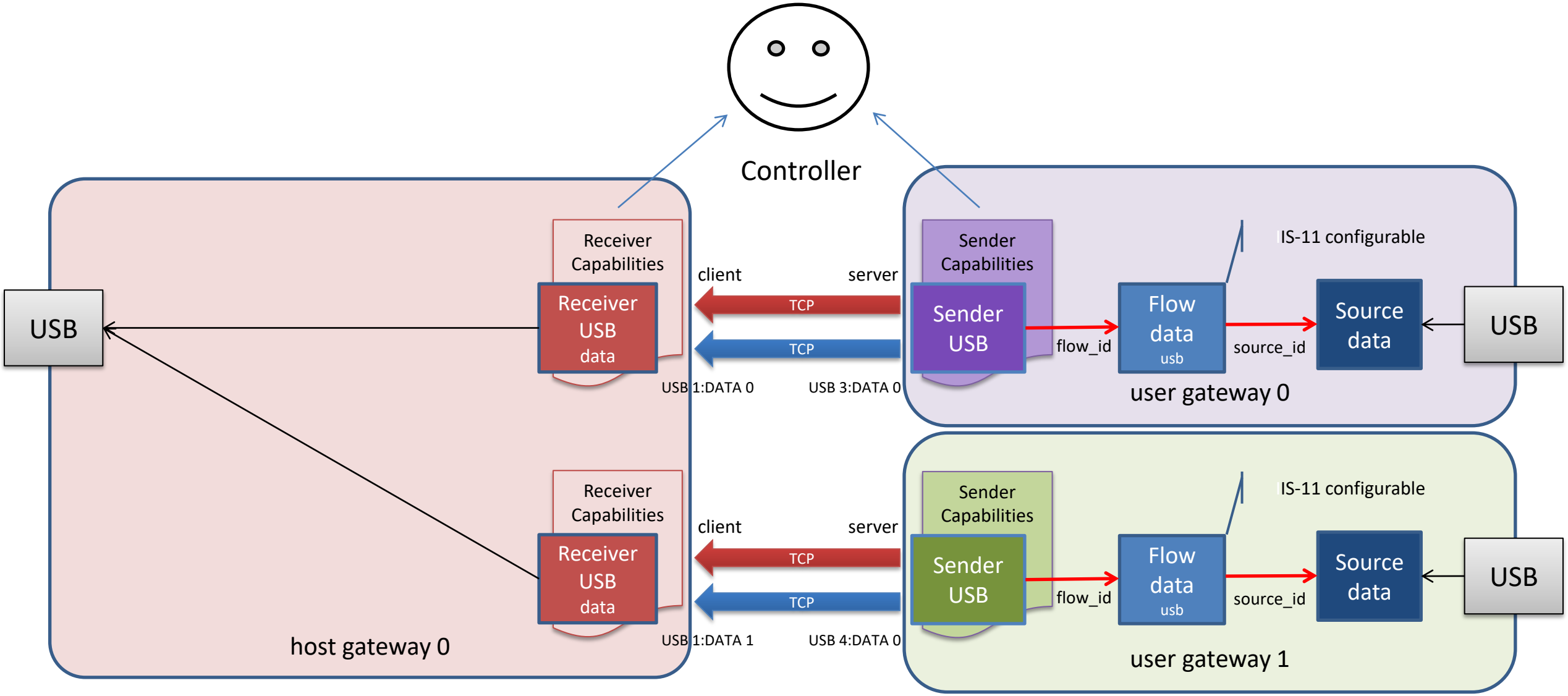
Enterprise Computer Room

Exclusive session's key_xcl added
to PEP key derivation function.



User

Data Stream => multiple Receivers for a USB connector



- This concludes our overview of NMOS with USB transport, a key feature of Matrox NMOS Advanced Streaming Architecture.
- If you have any questions, feel free to reach out at abouchar@matrox.com.
- Thank you for attending.