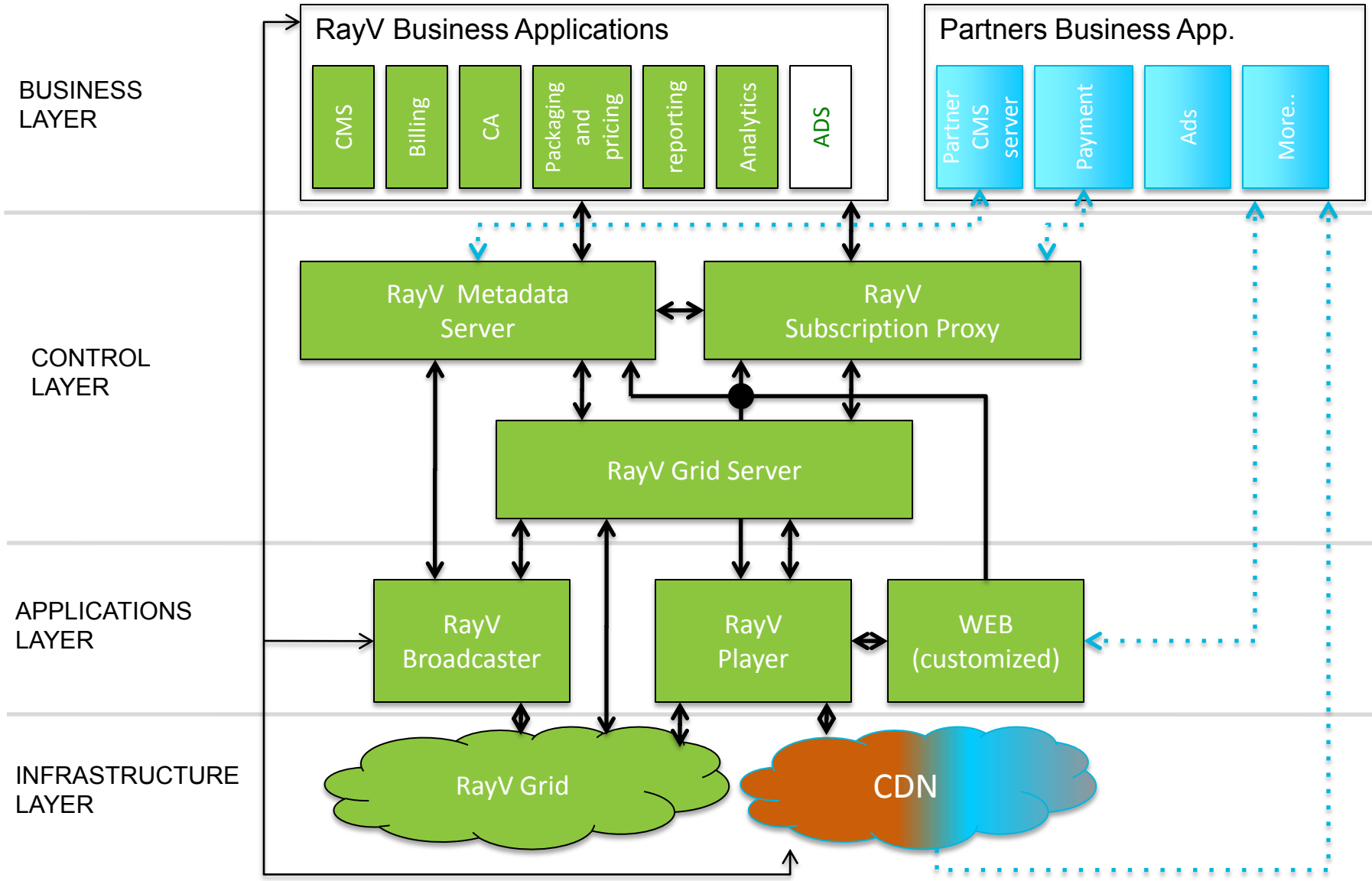
Technical – Security

List

- RayV security General strengths
  - Built on standards
  - Types of attacks
  - General strength of platform security
- Infrastructure and NOC
  - Architecture
  - NOC security facts
- Conditional access and web
  - Subscription server/proxy
- Grid server Security
- Admin sites (internal and to customers)
- RayV TVDN: architecture and concepts

TVDN Layers – unified solution



General strengths of platform

1. Complete platform from billing to network where all security layers are addressed.
2. **RayV is PCI compliant (McAfee)**.
3. HTTPS is used for account/billing password creation. HTTPS is used between PC devices and Grid control servers
4. Geo-targeting is used to authorize only viewers from specific countries/carriers/offices and every other attribute that may be deduced from the viewer's IP.
5. URL allowance is used to allow watching the content only on specific web pages. This is done in order to protect content from being distributed not in authorized sites.
6. No storage is kept on any kind of user device
7. Authentication is session-oriented and the client's signature is only valid for the duration of the current session.
8. Encrypted tokens are used for authorization of the peers in the network among themselves for non-repudiation.
9. Session key between viewer and server to exchange all control protocol.

Types of attacks

Spoofing:

HTTPS User authentication prevents such attacks (one stealing another identity)

Denial-of-service attacks:

HTTPS and Cryptographic hash values used in all RayV protocols prevent such attacks.

Man-in-the-middle attacks:

HTTPS and Messages authentication and integrity prevents against such attacks when the man in the middle is between, say, hostile routers.

Replay attacks:

HTTPS and Use of sequence numbers prevents such attacks.

Connection hijacking:

HTTPS and Use of authentication/integrity and secured EID (End point identification) for each signaling message prevents such attacks.

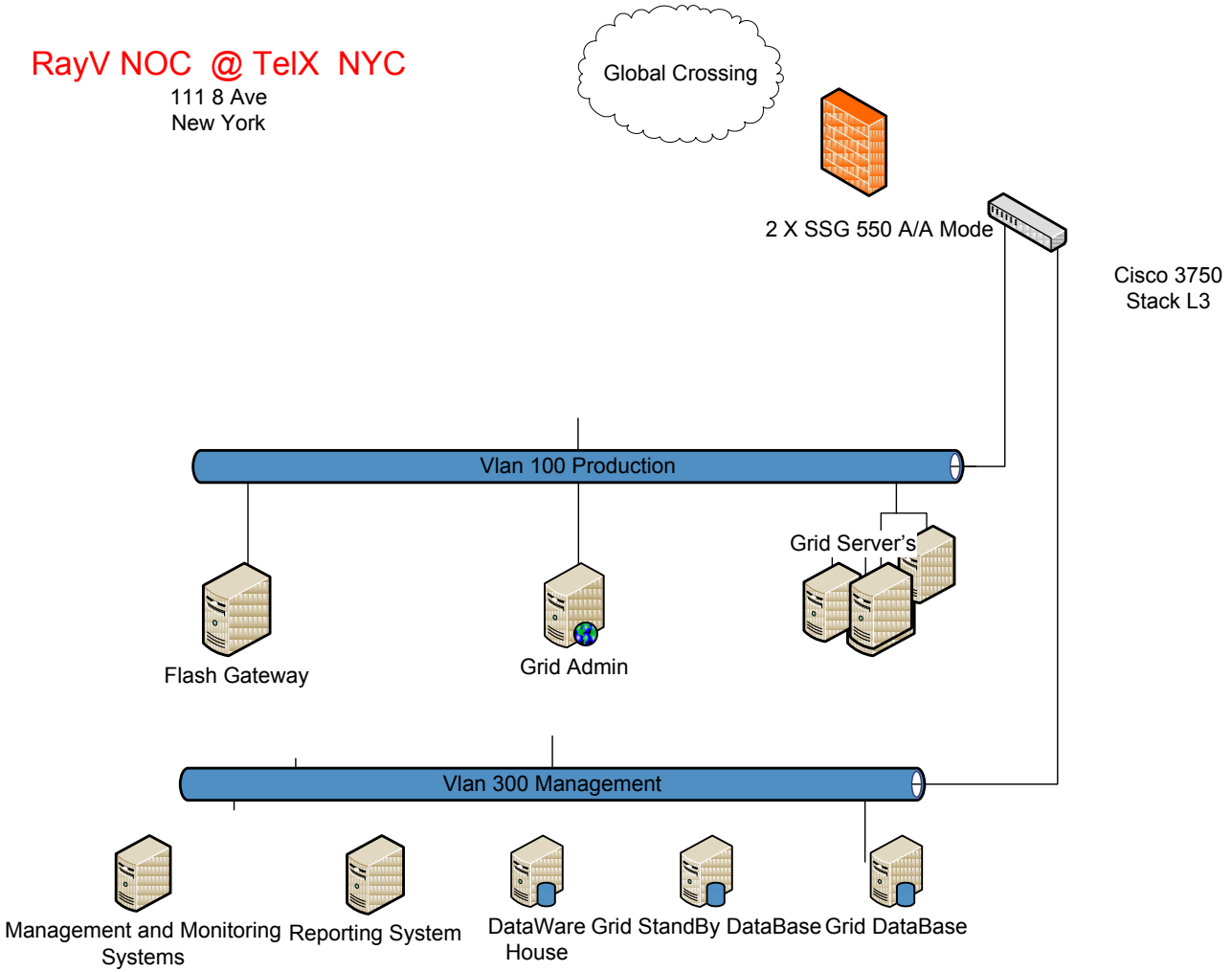
Eavesdropping of media stream:

Eavesdropping is countered by encryption and use of secret keys in the media itself.

Non repudiation:

Non-repudiation is countered by having data from the peers contributing the stream.

Infrastructure – NOC security



Infrastructure – NOC security points

Network Operation Center Security
•RayV NOC is in TelX NYC - Physical access to the NOC is restricted to only few RayV employees.
•Hosting facility is NOT shared with any other company.
•No wireless network is available in the NOC.
•DMZ is implemented to limit inbound and outbound traffic for the cardholder environment.
•All console administrative access is encrypted using VPN.
•Security policies address all PCI DSS requirements.
•Access to sensitive information is restricted to business use only, and protected.
•All sensitive information (login/password) is stored protected.

Software in NOC
•All system components and software have the latest vendor supplied security patches installed.
•During installation RayV never uses the vendor-supplied defaults for system passwords.
•Anti-virus software is always used regularly also on all employee-owned computers

Firewalls and routers
•Firewall configuration to protect all types of data. Cisco 3750 L3 is used.
•RayV maintains a formal process for approving and testing all changes to the firewall and router.
•Stateful inspection (dynamic packet filtering) is implemented and only established connections are allowed.

From development to production in NOC
•RayV has a separated development/test environment from Production environment.
•Test data accounts are removed before production systems become active.
•Production data is not used for testing or development.

Conditional Access and web

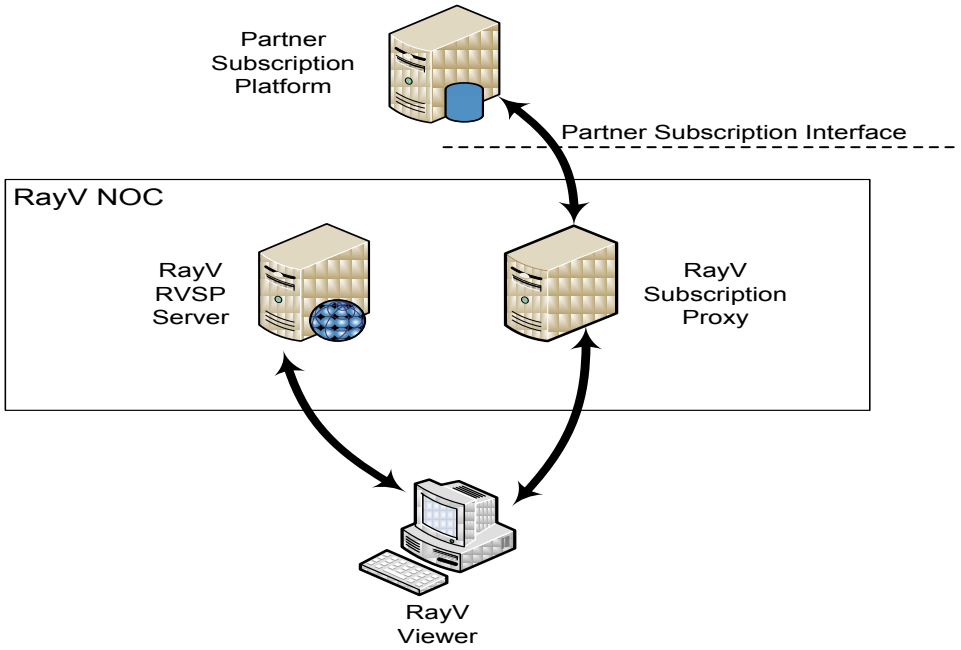
Subscription server security guidelines

•Only one primary function is implemented per server.
•All unnecessary functionalities have been removed. This includes: scripts, drivers, features, sub-systems, file systems, and unnecessary web servers
•Disk-encryption is used and logical access is managed independently of native operating system access control mechanisms. Decryption keys are independent of user accounts.
•All web applications are developed based on secure coding guidelines.

Card data protection

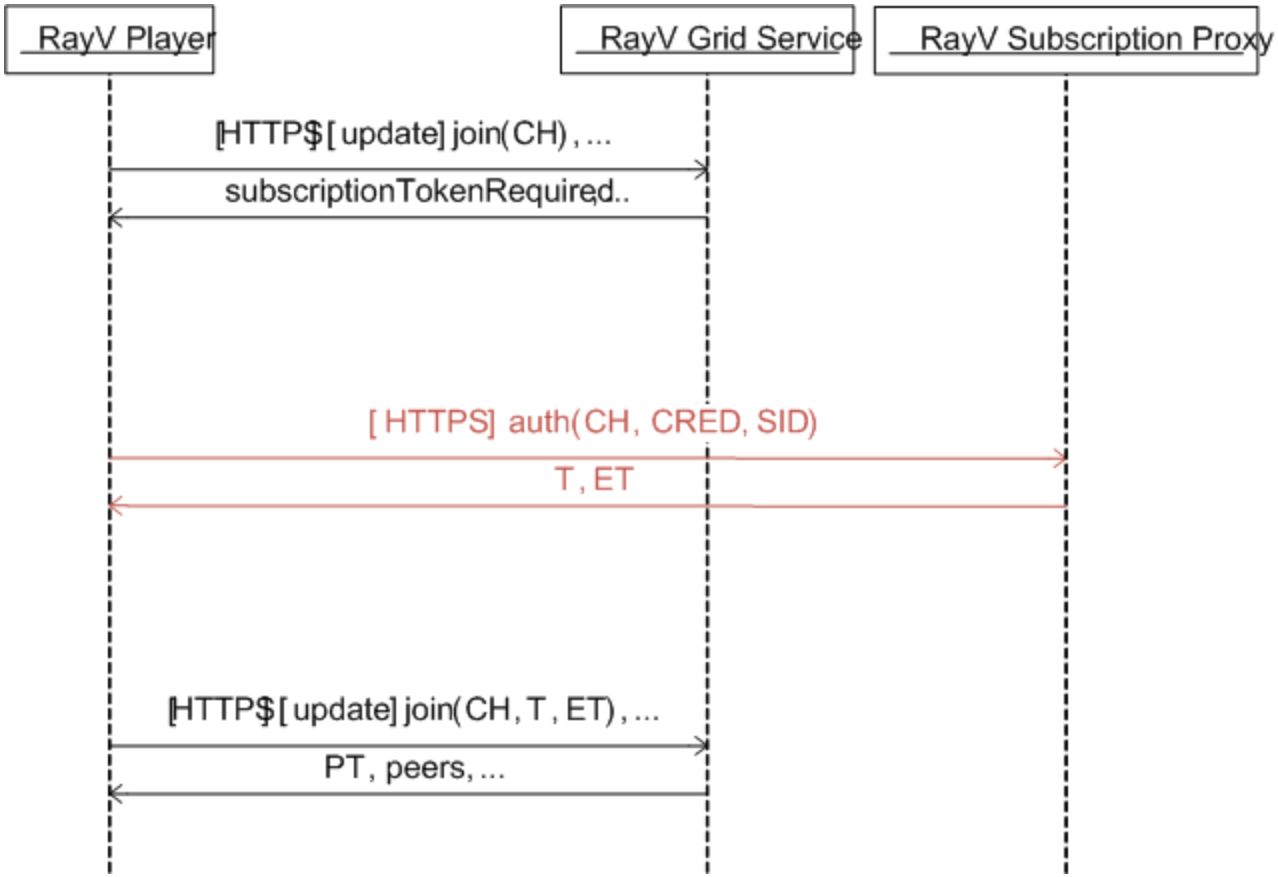
•RayV never stores the cardholder sensitive data.
•The cardholder data that is saved, is stored protected.
•Transmission of cardholder data is always encrypted when sent across open, public networks.
•Card number / primary account number (PAN) is not stored but we do keep the Mask (last four digits)
•Card validation code or value (three digits or four digits number) is not stored.
•PIN (personal identification number) is not stored.
•Pan is hashed and never kept clear.
•Strong cryptography and security protocols, such as SSL/TLS are used to safeguard sensitive cardholder data during transmission over open public networks.

Conditional Access and web



- The client (browser) communication with the proxy server is done using HTTPS, with a 128 encryption key.
- Only the hash of the password is stored in the proxy.
- No credit card information is saved or stored.
- Between servers (RayV subscription proxy and PayPal servers) the communication is always and only SSL.
- The administration site created by RayV for the customers is always SSL with two passwords line protection.

Conditional Access and web – Flow



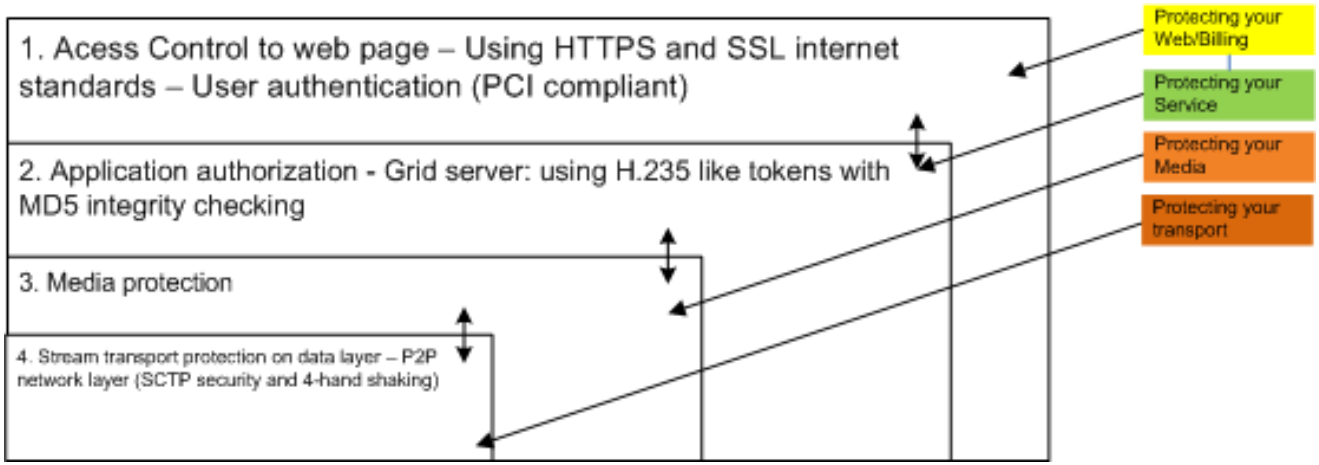
TVDN Security – built on standards

Distinguishing:
- VOD DRM – Data is saved, limitation on copy/watching/different devices
- Live Access Control – No data is stored

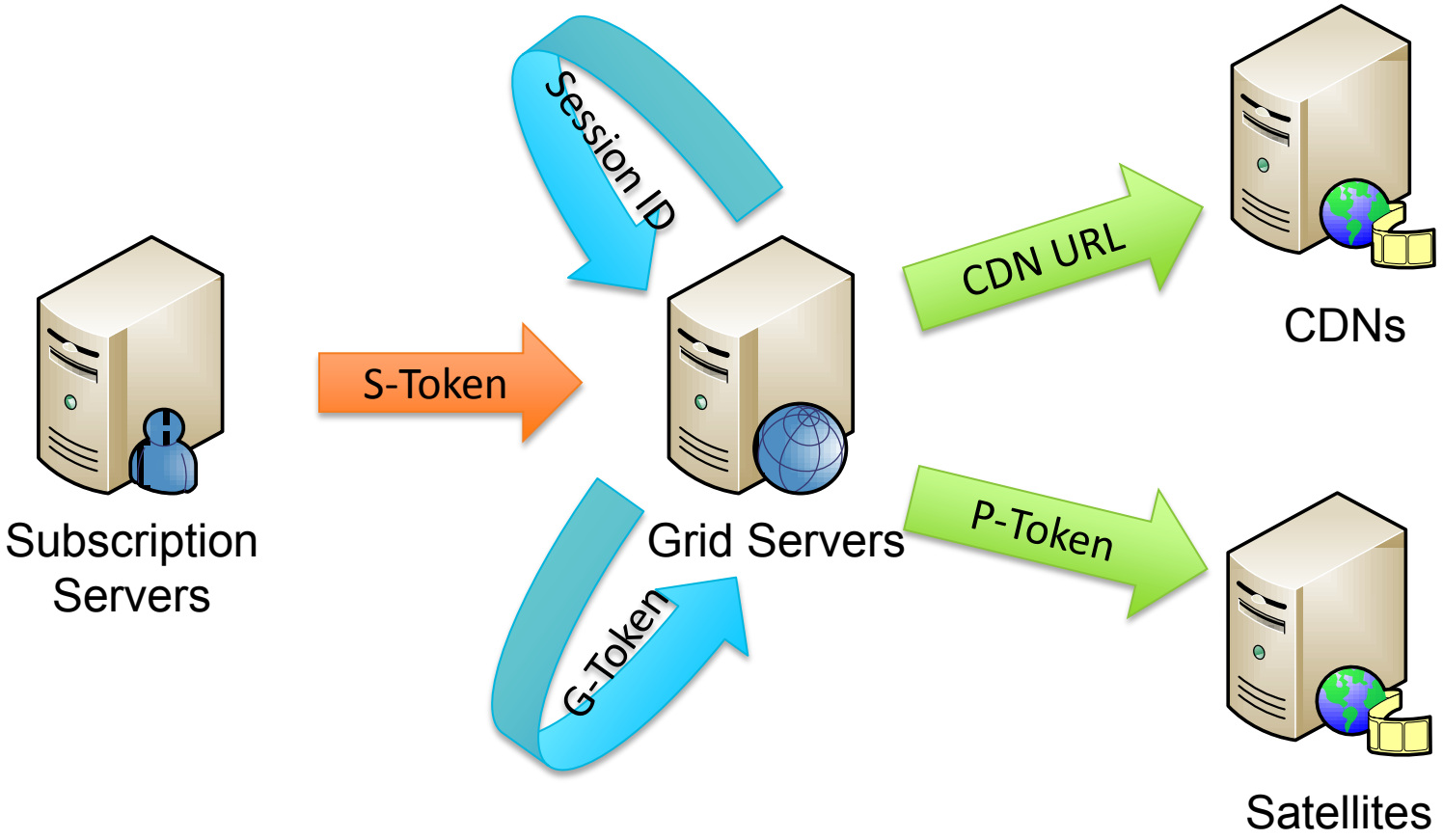
RayV solution doesn't use any data storage on customers' HW.

Types of attacks:
- DoS (on web servers, on grid servers, on network protocols)
- Watching without permission (Stealing AC, Geo targeting, Web container)
- Non repudiation (Statistical consistency)

Built on security standards:



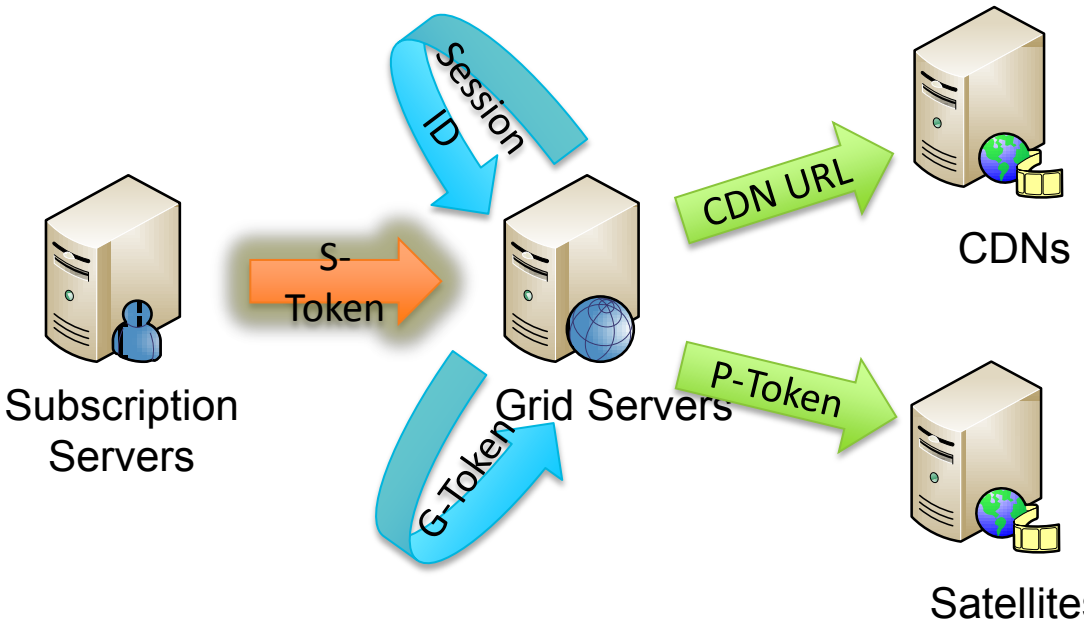
Access-Granting Data Structures



** All communications are via 'front channels' (client mediation).*

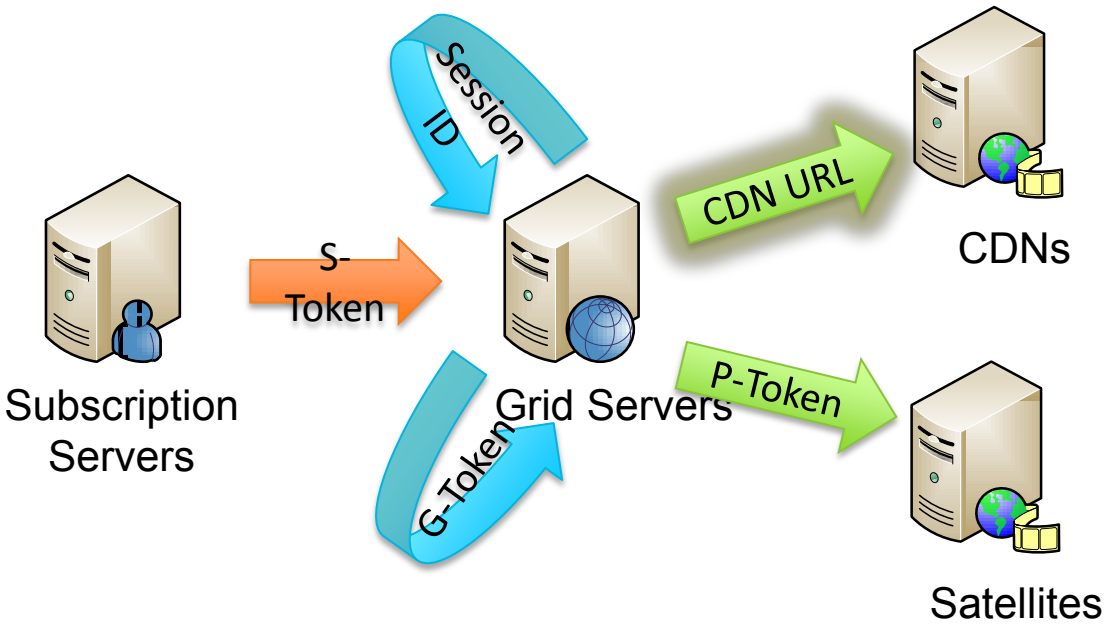
S-Tokens

- Issued by Subscription Servers
- Guard one or more Grid Service channels or VOD
- Time-limited, per IP
- Contents:
  - Channel IDs
  - Client IP address
  - User identity
  - Token expiration
  - Playback window
  - Hash of the above with shared secret



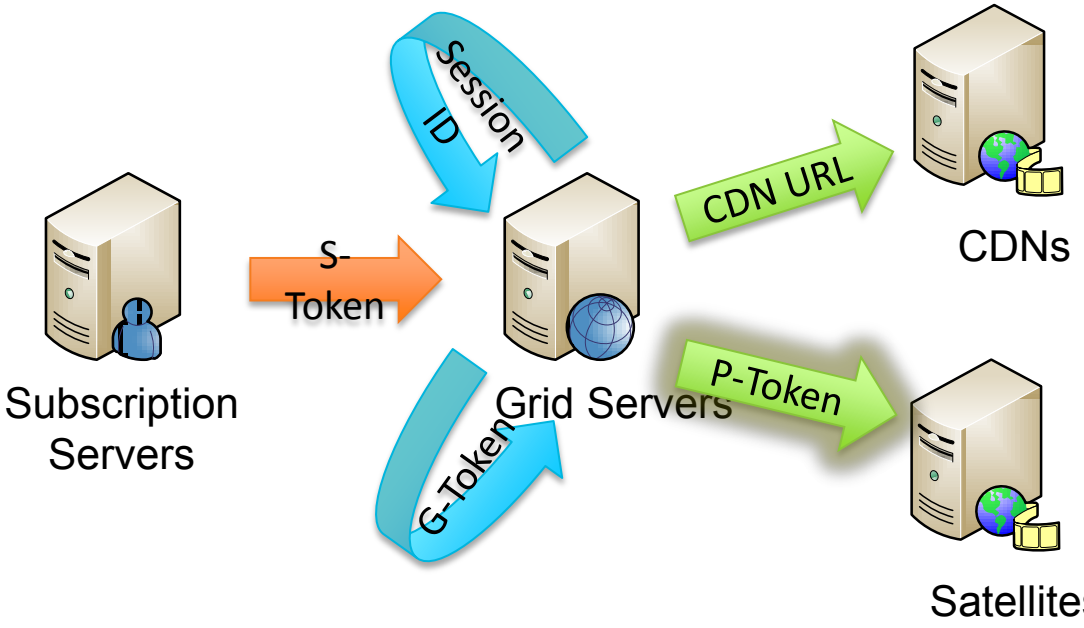
CDN URL

- Issued by Grid Servers
  - Each CDN has its own URL structure
- Guard CDN streams
- Time-limited, per IP
- Hashed with shared secret



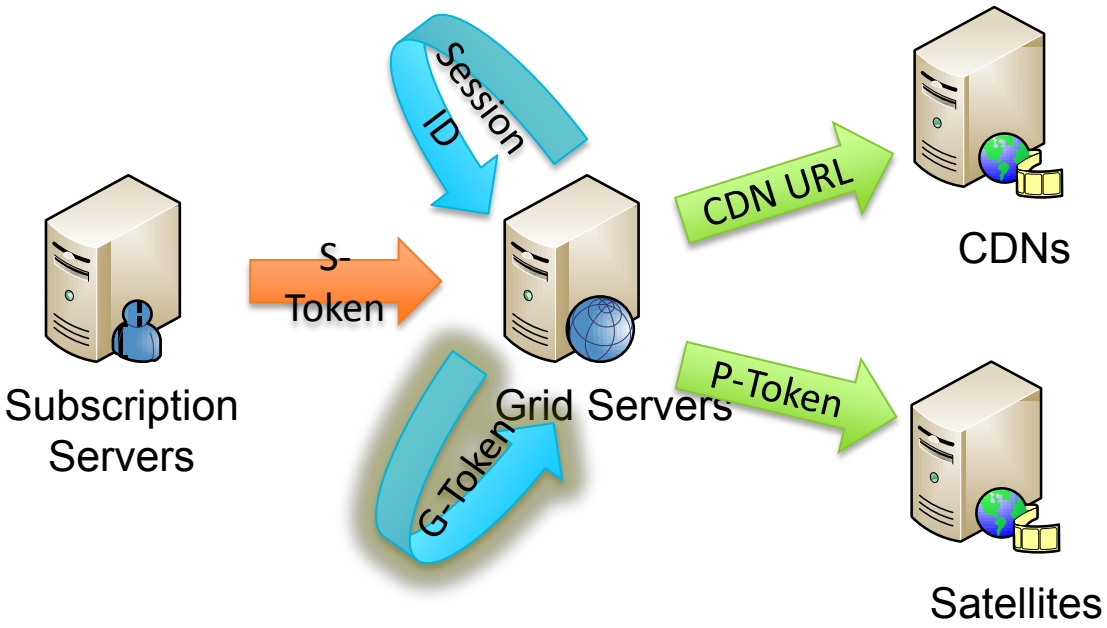
P-Tokens

- Issued by Grid Servers, in the peer list
- Each P-token protects a satellite
- Time-limited, periodically updated
- Per external IP
- Hashed with shared secret



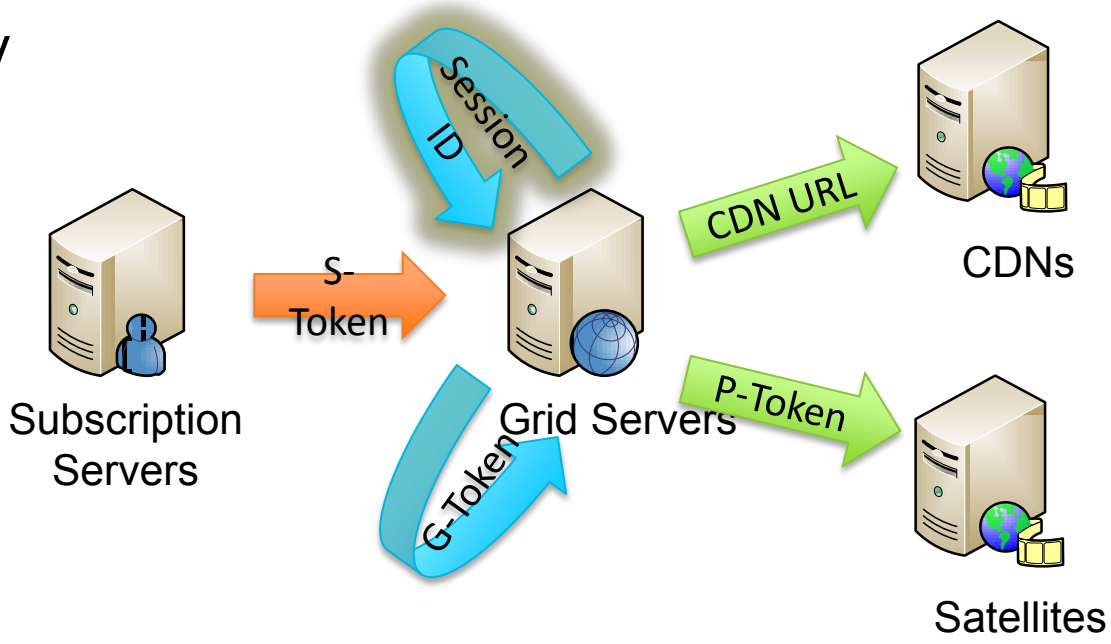
G-Token

- Issued by a Grid Server instance
- Used by clients during server failover (e.g. balancer failure)
- Proves client was joined to a channel
  - Removes the need for full authorization flow
  - Allows transparent instance failover
- Time-limited, periodically updated
- Contains:
  - Transport IP
  - STUN-derived IP (if exists)
  - Channel ID
  - Pipe
  - User identity
  - Playback window
  - G-token expiration

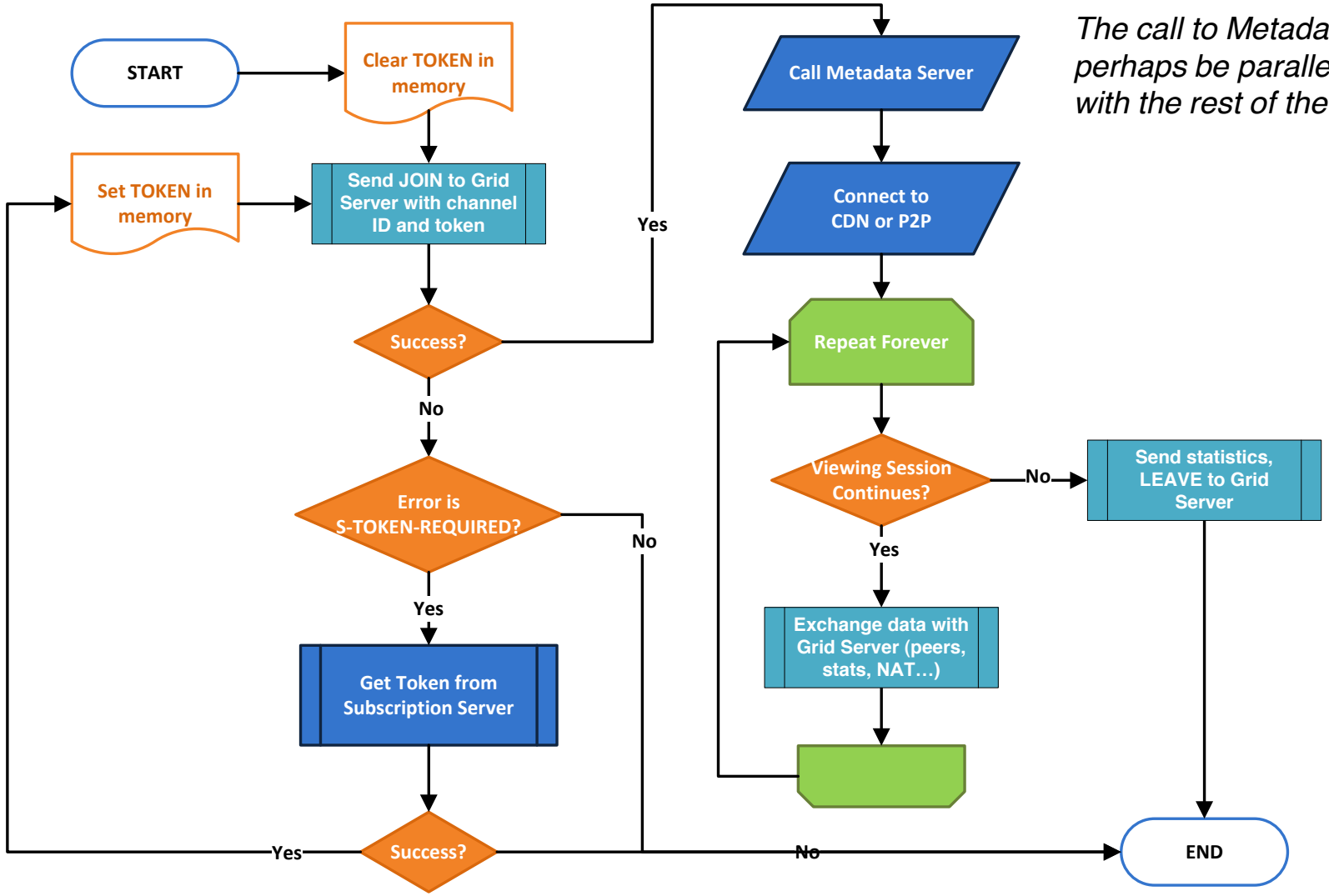


Grid Server's Session ID

- Issued by a Grid Server instance
- Protects a client's state at that instance
- Time-limited, periodically updated
- Associated with STUN-derived IP (too many simultaneously used IPs sometimes disallowed)
- Associated with **SSL** Session ID (multiple active SSL session IDs may indicate fraud)



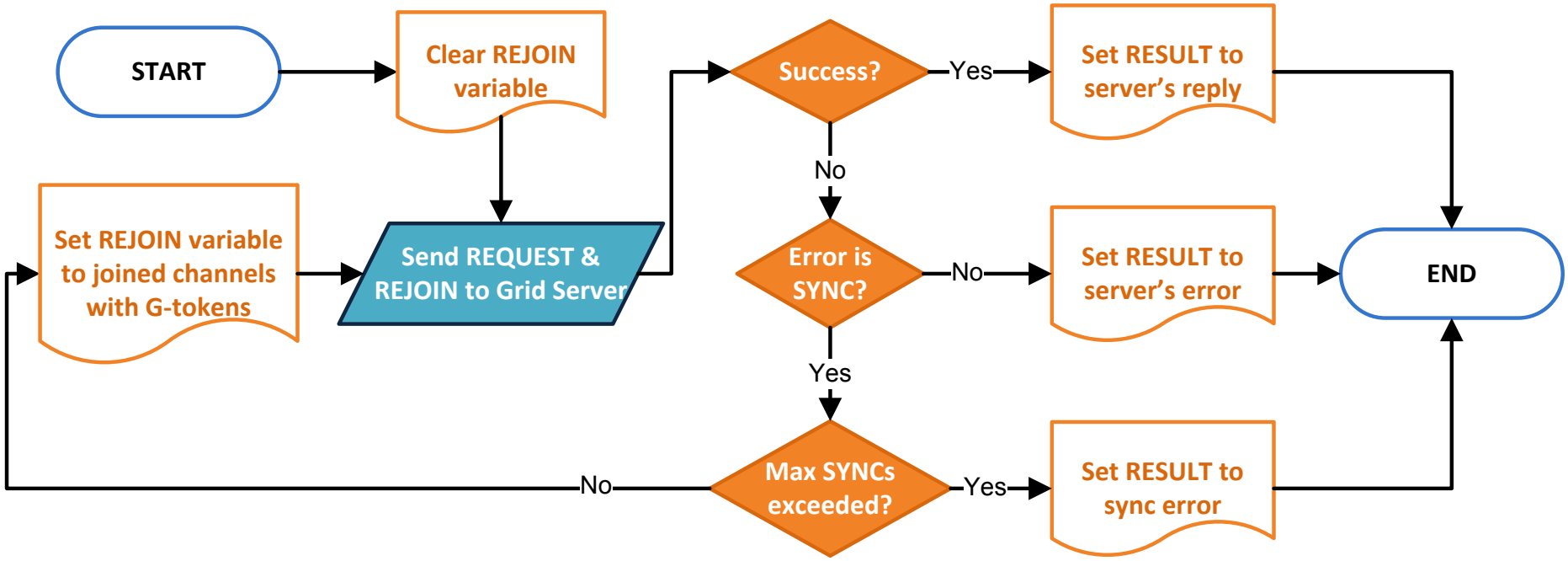
Simplified Player Flow



The call to Metadata can perhaps be parallelized with the rest of the process

** Grid server communications are elaborated in the next slide.*

Simplified Comm. with Grid Server – Details



** All communications use TLS/SSL*

*** Client must keep sending HTTP header/cookie containing server-specified session ID*

Step 0 – Preconditions

- The flow starts with a channel ID (or VOD title ID)

- The channel ID is:
  - Either part of the embedding HTML tag
  - Or chosen by the user from a list of favorites in standalone mode.

Step 1 – Client Fails to Join without a Token

Scenario	Eavesdropping Threats	Redistribution Threats
Client tries to join the channel in the grid server. Grid server returns *s-token-required*.	None	None

Step 2 – Client Sends Credentials to Subscription

Scenario	Eavesdropping Threats	Redistribution Threats
Client sends username and password to Subscription Server over HTTPS.	TLS/SSL offers reasonable protection.	User may distribute username and password. **Defenses:** 1. Abusers must use the same IP in all forthcoming communications (including P2P UDP). This is doable via a proxy. 2. Grid Servers can be configured to allow a maximum of N sessions per credentials ▪ This is done via *user identity*, which is passed in the S-token. ▪ Limitation: will not work during the first 10 seconds after the first viewing session joins.

Step 3 – Token Received and Sent to Grid Server

Scenario	Eavesdropping Threats	Redistribution Threats
Subscription Server returns over HTTPS an S-token to the client. Client sends over HTTPS the token to the Grid Server to join the channel.	TLS/SSL offers reasonable protection.	User may distribute S-token. **Defenses:** 1. Abusers must use the same IP in all forthcoming communications (including P2P UDP). This is doable via a proxy. 2. Abuse can only be done within 1 minute or so. 3. Again, Grid Servers can be configured to allow a maximum of N sessions per credentials ▪ This is done via *user identity*, which is passed in the S-token. ▪ Limitation: will not work during the first 10 seconds after the first viewing session joins.

Step 4a (P2P) – Grid Server Returns Peers

Scenario	Eavesdropping Threats	Redistribution Threats
Grid Server chooses a pipe and sends over HTTPS the list of peers, including satellites. For each satellite, the server returns a P-token. Client must be connected to at least one satellite, over Scotch-G protocol on top of UDP.	When client contacts a satellite, P-token may be sniffed. **Defenses:** 1. Abusers must use the same IP (doable). 2. Abuse must be perpetrated within a few minutes. 3. Scotch-G protocol may pose additional obstacle, since the sniffed satellite is most likely used by the original client (seq num).	User may distribute satellite UDP endpoint & P-token. **Defenses:** 1. Abusers must use the same IP (doable). 2. Abuse must be perpetrated within a few minutes.

Step 4b (CDN) – Grid Server Returns Peer

Scenario	Eavesdropping Threats	Redistribution Threats
Grid Server chooses a pipe (a CDN) and sends over HTTPS the 'secure URL' for the CDN. Client uses the URL to connect over unsecured HTTP.	The CDN's URL can be sniffed. **Defenses:** 1. Abusers must use the same IP (doable). 2. Abuse must be perpetrated within a minute or so. ▪ This level of protection is what CDNs offer, unless DRM is used.	User may distribute the CDN URL **Defenses:** 1. Abusers must use the same IP (doable) 2. Abuse must be perpetrated within a minute or so. ▪ This level of protection is what CDNs offer, unless DRM is used.

Step 5a (P2P) – Server Sends New Peers

Scenario	Eavesdropping Threats	Redistribution Threats
Client periodically exchanges updates with the Grid Server over HTTPS. A session ID sent by the client allows the server to find the client's session state. The session state indicates the channels to which the client is joined. Grid Server may return a new peer list to the client, which includes new satellites and their P-tokens.	TLS/SSL offers a reasonable protection against eavesdropping on the session ID.	Session ID might be distributed. The session stores the fact that the user is joined. **Defenses:** 1. Abusers must use the same IP (doable). 2. Expiration time (to be confirmed). 3. Grid Server may observe the use of multiple **SSL** Session IDs (not to be confused with regular session IDs) and return *s-token-required*.

Step 5b (CDN) – Server Sends New Peers

Scenario	Eavesdropping Threats	Redistribution Threats
No such scenario: *sync* and *rejoin* does not cause the Grid Server to resend the CDN URL. As a result, content cannot be stolen even if rejoin succeeds. At most, bad stats can be sent.	N/A	N/A

Step 6 – Server Failover

Scenario	Eavesdropping Threats	Redistribution Threats
When client originally joined the channel, grid server sent over HTTPS not only the peers, but also a G-token. When exchanging updates with the Grid Server over HTTPS, client reaches a new instance, which returns a *sync* request. Clients performs *rejoin* of its channel, with the G-token received originally during join.	TLS/SSL offers reasonable protection.	G-token might be distributed. This would allow any user to rejoin and receive new peers. **Defenses:** 1. Abusers must use the same IP (doable). 2. Abuse must be perpetrated within a minute or so. 3. Grid Server may observe the use of multiple **SSL** Session IDs and return *s-token-required*. 4. For CDN channels, peers are not sent during rejoin.

Threat Summary

Data Structure	Eavesdropping	Redistribution
Credentials	TLS/SSL	1. IP 2. Limit on concurrent sessions
S-Token	TLS/SSL	1. IP 2. Short expiration time 3. Limit on concurrent sessions
CDN URL	1. IP 2. Short expiration time	1. IP 2. Short expiration time
P-Token	1. STUN IP 2. Short expiration time	1. STUN IP 2. Short expiration time
Session ID	TLS/SSL	1. IP 2. Expiration time (to be confirmed) 3. Limit on concurrent SSL Session IDs
G-Token (rejoin)	TLS/SSL	1. With CDN channels, peers not sent during sync &rejoin (no threat) 2. Socket IP & STUN IP 3. Short expiration time

Conclusion

- Protection relies on two components:
  - IP address (socket IP, STUN IP or both)
  - One or both of the following:
    - Either a short time window
    - Or a limit on concurrent sessions
- TLS/SSL acceptable against eavesdropping.

Video authenticity

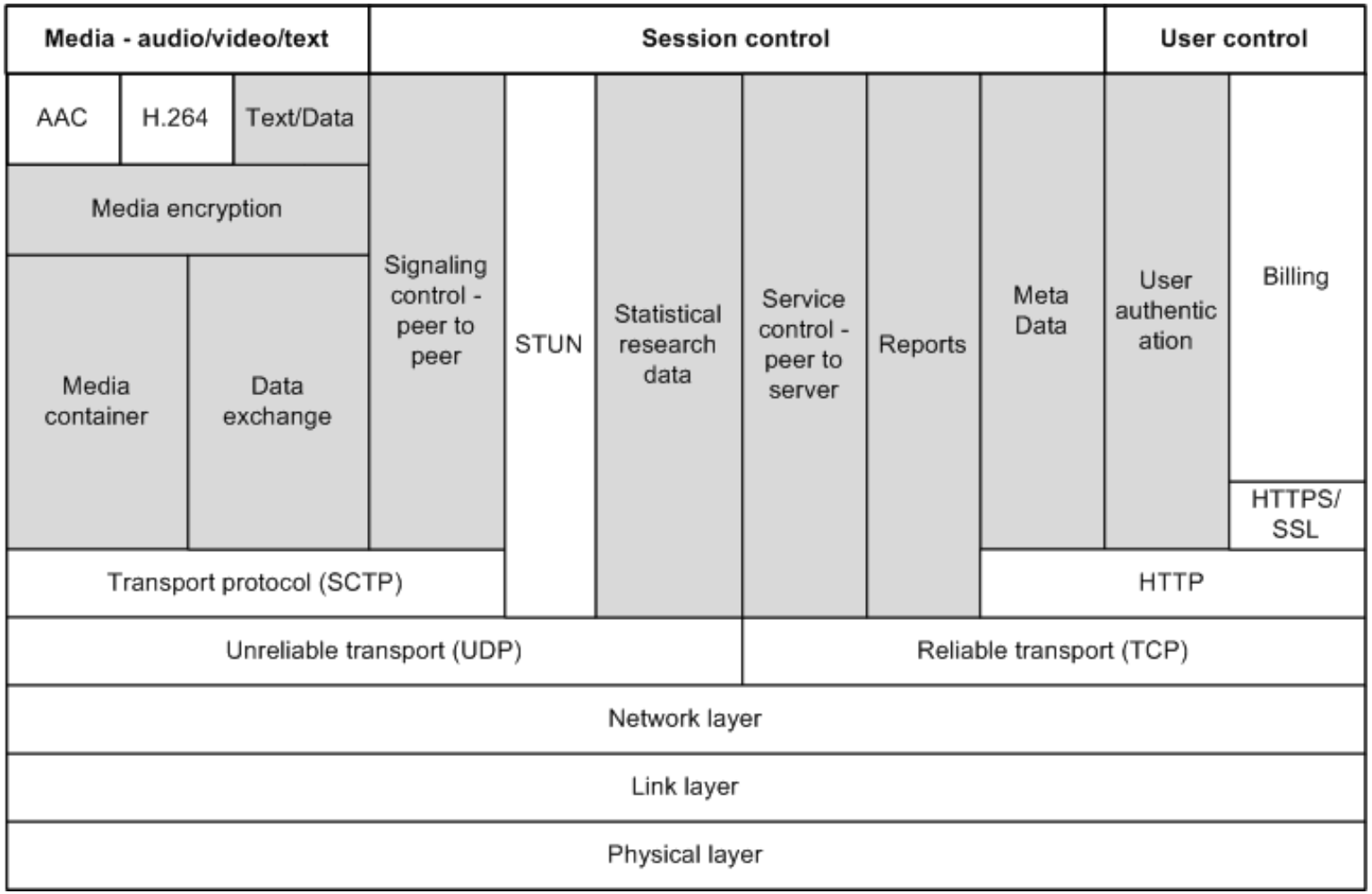
• All data is encrypted by means of a secret shared between the encrypting and the decrypting party. The Grid Service regularly changes the shared secret. (Note that symmetric encryption was chosen here for reasons of performance.)

• The Grid Service periodically (e.g. every 10 minutes) generates a shared Media Secret Key (MSK) for each channel. Each key in each channel is given a Media Key ID (KID). The Grid Service also chooses activation time (AT) for each key, so that the key is in effect after the Grid Service has the opportunity to notify all clients of the new key.

• The key is sent to the broadcaster, and to media-consuming clients. With the keys, two more data are sent: the Key ID, and the activation time. The broadcaster uses its in-effect latest key to encrypt the stream, and broadcasts the Key ID with the stream.

• Any client may happen to receive a new key before the broadcaster. Hence, the old key remains in effect, until the broadcaster starts to send the new Key ID. The client thus decrypts the stream with the key specified by the broadcaster by means of Key ID

Layers


Media - audio/video/text
Session control
User control
AAC
H.264
Text/Data
Media encryption
Media container
Data exchange
Signaling control - peer to peer
STUN
Statistical research data
Service control - peer to server
Reports
Meta Data
User authentic ation
Billing
HTTPS/ SSL
Transport protocol (SCTP)
HTTP
Unreliable transport (UDP)
Reliable transport (TCP)
Network layer
Link layer
Physical layer