



Security for Discovery and Connection management of ST 2110 Media Devices

Arne Bönninghoff – Head of IP Research
Riedel Communications GmbH & Co. KG



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Media Node Maturity Checklist

Media Node Maturity Checklist	
Brand / Product / Date:	
I. Media Transport	Single link video SMPTE ST 2110-20
	Software-friendly SMPTE ST 2110-21 Wide video receivers
	Universal, multichannel and low latency audio SMPTE ST 2110-30 Level C
II. Time and Sync	Stream protection with SMPTE ST 2022-7
	PTPv2 configurable within SMPTE and AES profiles
	AMSS interface PTP redundancy
III. Discovery and Connection	Synchronization of audio, video and data essences
	Discovery and Registration: AMBA IS-04
	Connection Management: AMBA IS-05
IV. Configuration and Monitoring	Audio channel mapping: AMBA IS-06
	Topology discovery: LLDP
	IP assignment: DHCP
V. Security	Open configuration management - e.g., API, config file, SSH CLI, etc.
	Open monitoring protocol - e.g., syslog, agent, SNMPv3, etc.
	EBU R 148 Security Tests
	EBU R 143 Security Safeguards
	Secure HTTPS API: AMBA BCP-003



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Why security

Media Node Maturity Checklist	
Brand / Product / Date:	
I. Media Transport	Single link video SMPTE ST 2110-20 Software-friendly SMPTE ST 2110-21 Wide video receivers Universal, multichannel and low latency audio SMPTE ST 2110-30 Level C Stream protection with SMPTE ST 2022-7
II. Time and Sync	PTPv2 configurable within SMPTE and AES profiles AES3 interface PTP redundancy Synchronization of audio, video and data essences
III. Discovery and Connection	Discovery and Registration: AMBA IS-04 Connection Management: AMBA IS-05 Audio channel mapping: AMBA IS-06 Topology discovery: LLDP IP assignment: DHCP
IV. Configuration and Monitoring	Open configuration management - e.g., API, config file, SSH CLI, etc. Open monitoring protocol - e.g., syslog, agent, SNMPv3, etc.
V. Security	EBU R 148 Security Tests EBU R 143 Security Safeguards Secure HTTPS API: AMBA BCP-003



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Why security

Media Node Maturity Checklist	
Brand / Product / Date:	
I. Media Transport	Single link video SMPTE ST 2110-20 Software-friendly SMPTE ST 2110-21 Wide video receivers Universal, multichannel and low latency audio SMPTE ST 2110-30 Level C Stream protection with SMPTE ST 2022-7
II. Time and Sync	PTPv2 configurable within SMPTE and AES profiles AES3 interface PTP redundancy Synchronization of audio, video and data essences
III. Discovery and Connection	Discovery and Registration: AMBA IS-04 Connection Management: AMBA IS-05 Audio channel mapping: AMBA IS-06 Topology discovery: LLDP IP assignment: DHCP
IV. Configuration and Monitoring	Open configuration management - e.g., API, config file, SSH CLI, etc. Open monitoring protocol - e.g., syslog, agent, SNMPv3, etc.
V. Security	EBU R 148 Security Tests EBU R 143 Security Safeguards Secure HTTPS API: AMBA BCP-003

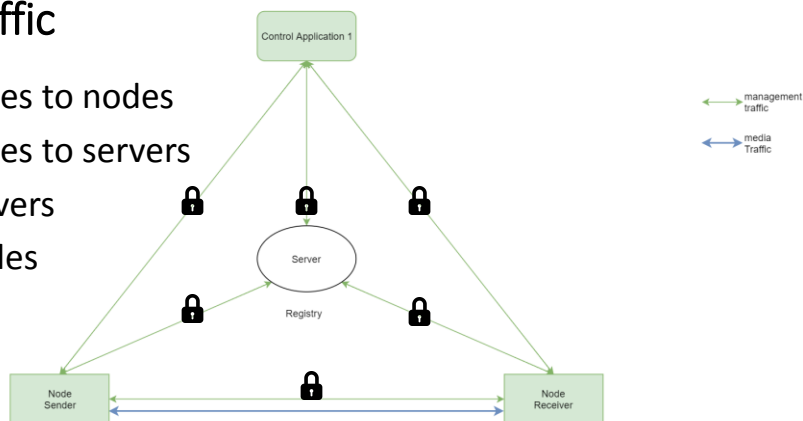


IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Types of traffic

- Control devices to nodes
- Control devices to servers
- Nodes to servers
- Nodes to nodes



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Levels of security

- **Confidentiality** Data passing between client and the APIs is unreadable to third parties.
- **Identification** The client can check whether the API it is interacting with is owned by a trusted party.
- **Integrity** It must be clear if data travelling to or from the API been tampered with.
- **Authentication** The client can check if packets actually came from the API it is interacting with, and vice versa.
- **Authorisation** The API can determine whether the client interacting with it has authorisation to carry out the operation requested.



courtesy Simon Rankine BBC R&D

IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Work areas AMWA BCP-003

Establishing Trust

- Public key infrastructure with x509 certificates
- Explore how PKI can be used in a broadcast environment

Connection Security

- HTTP over TLS (HTTPS) – IS-04, -05, -06, (-07), -08, -09
- Identify cipher suites for interoperability
- Establish best practice for use of TLS with AMWA NMOS APIs

Client Authorisation

- OAuth 2.0 with JSON Web Tokens
- Identify what is needed to ensure interoperability



courtesy Simon Rankine BBC R&D

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Work areas AMWA BCP-003

Establishing Trust

- Public key infrastructure with x509 certificates
- Explore how PKI can be used in a broadcast environment

Connection Security

- HTTP over TLS (HTTPS) – IS-04, -05, -06, (-07), -08, -09
- Identify cipher suites for interoperability
- Establish best practice for use of TLS with AMWA NMOS APIs

Client Authorisation

- OAuth 2.0 with JSON Web Tokens
- Identify what is needed to ensure interoperability

BCP-003-01



courtesy Simon Rankine BBC R&D

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Work areas AMWA BCP-003

Establishing Trust

- Public key infrastructure with x509 certificates
- Explore how PKI can be used in a broadcast environment

Connection Security

- HTTP over TLS (HTTPS) – IS-04, -05, -06, (-07), -08, -09
- Identify cipher suites for interoperability
- Establish best practice for use of TLS with AMWA NMOS APIs

Client Authorisation

- OAuth 2.0 with JSON Web Tokens
- Identify what is needed to ensure interoperability

BCP-003-02
IS-10



courtesy Simon Rankine BBC R&D

IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



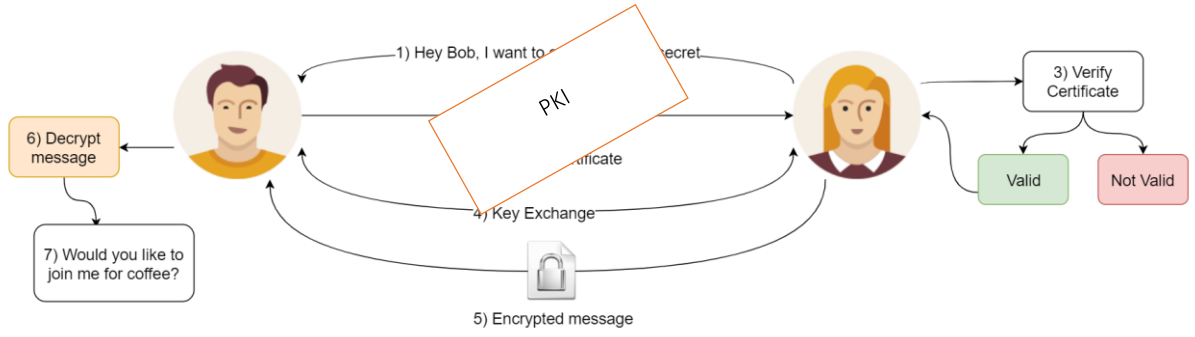
Key Exchange – establish trust



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



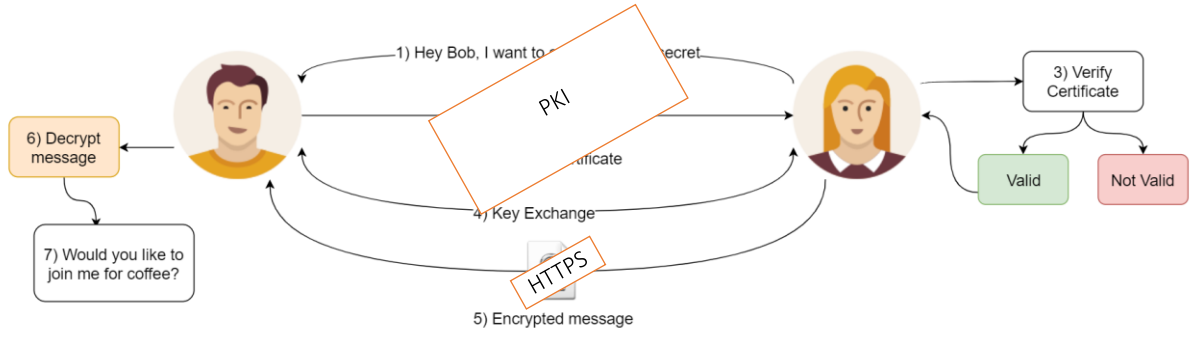
Key Exchange – establish trust



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



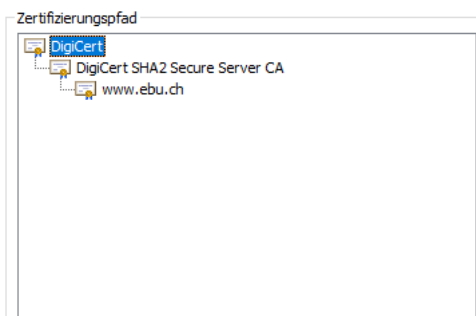
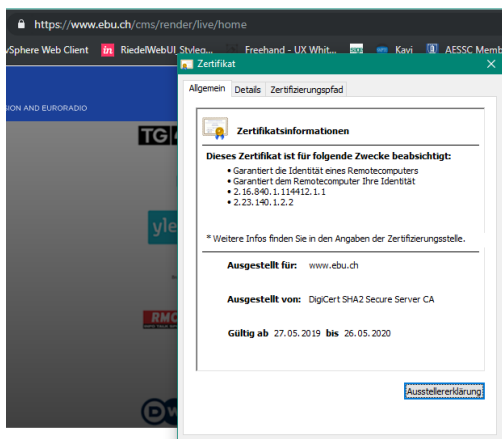
Key Exchange – establish trust



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



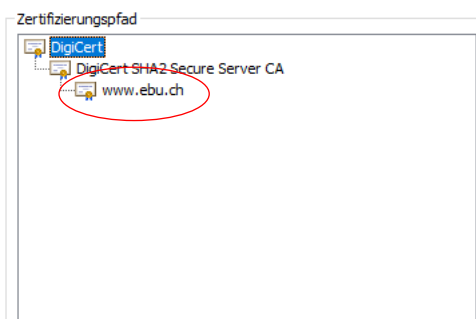
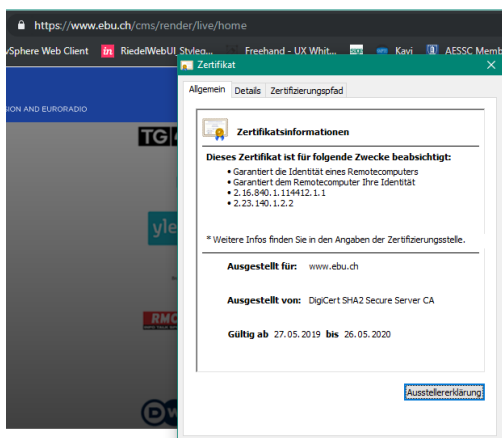
Key Exchange – DNS as a prerequisite



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Key Exchange – DNS as a prerequisite



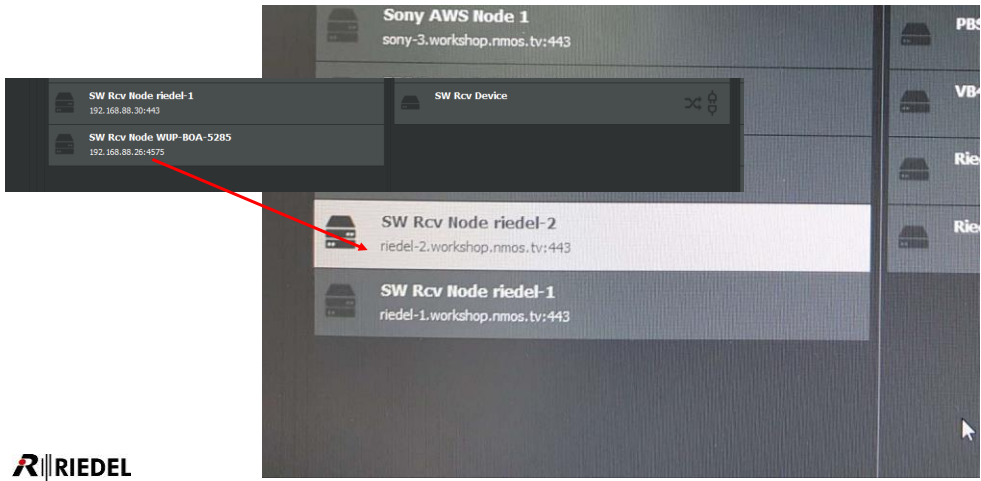
- Issued on Hostname not on IP Address
- DNS resolution essential



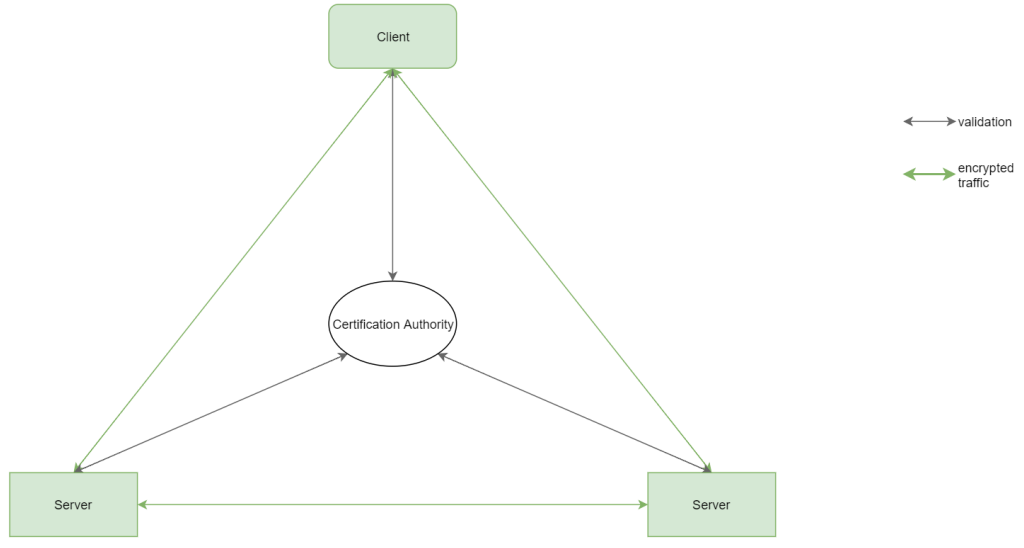
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



DNS Resolution – follow TR-1001



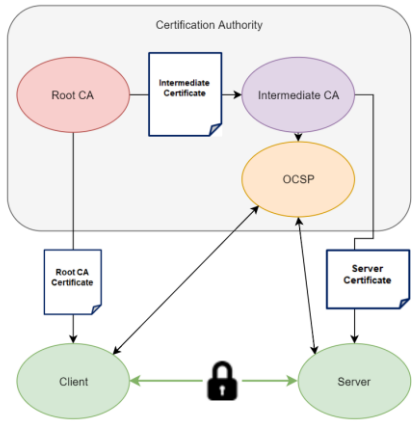
IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



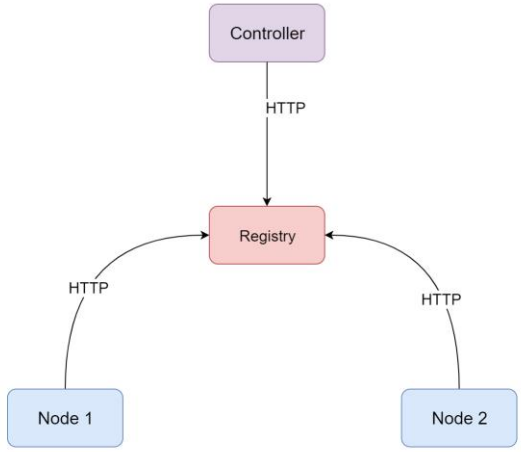
Certification Authorisation



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



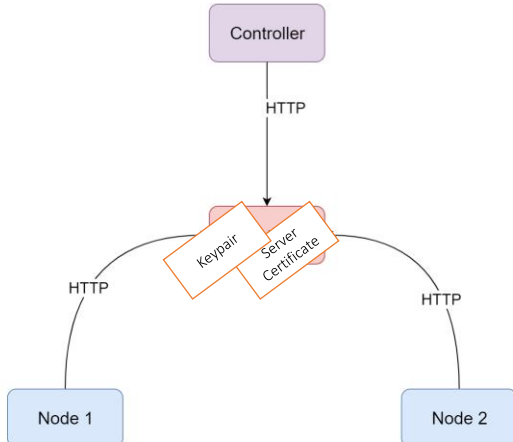
Client and Server: Example IS-04



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



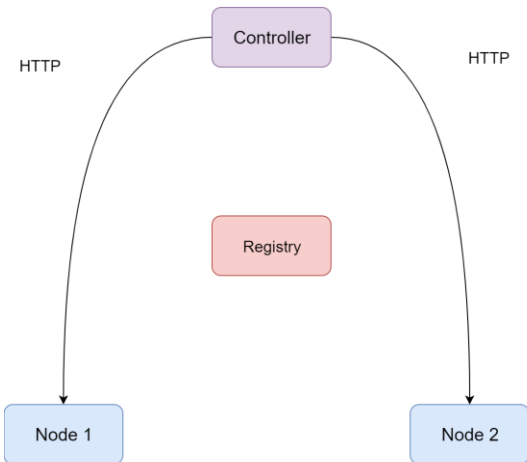
Client and Server: Example IS-04



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



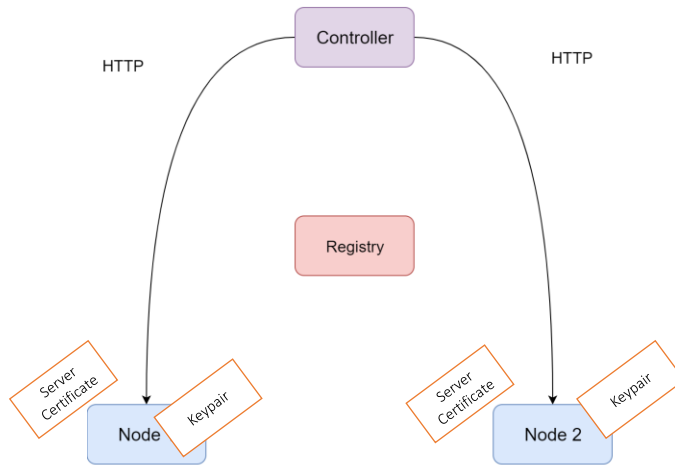
Client and Server : Example IS-05



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Client and Server : Example IS-05



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Connection Security – Interoperable HTTPS Cipher Suites for keys

- Should support {
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- Shall support {
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Use TLS v1.2 – be ready for v1.3 when available!

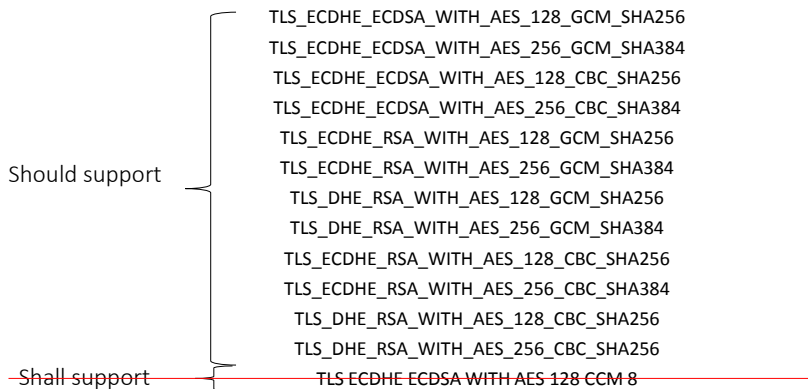


<https://www.bbc.co.uk/rd/publications/whitepaper337>

IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Interop Workshop discussion



Use TLS v1.2 – be ready for v1.3 when available!



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Interop Workshop discussion

TLS v1.2 Summary

Most-supported ciphers (by all who submitted results):

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Note that the sample size below is just **four** implementations



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



Conclusion BCP-003-01

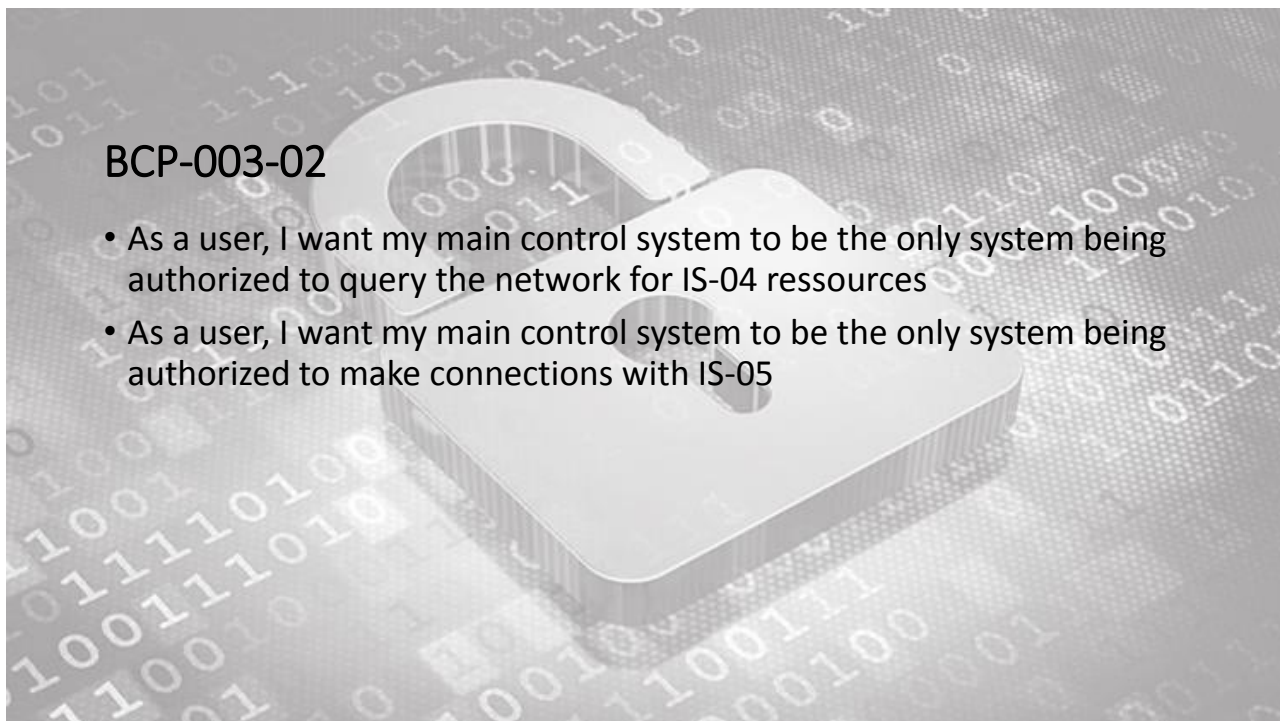
- Broadcast devices need to be able to import Root CA certificates (trust Servers) as well as import or generate Key/Certificate pairs (acting as server)
 - Broadcast devices need to support range of required cipher suites
 - Broadcast Controller need to trust Root CA certificates
 - **Broadcast Infrastructure needs to provide CA or Internet Access**
 - **Broadcast Infrastructure needs to provide DNS workflow**
- Security implementation simple for end devices – cipher suite topic aside
 - Infrastructure more challenging
 - CA, DNS, DHCP -> TR-1001
 - Needs more participation from vendors, all AMWA workshops now based on TLS
 - NMOS APIs prepared for TLS



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019

BCP-003-02

- As a user, I want my main control system to be the only system being authorized to query the network for IS-04 resources
- As a user, I want my main control system to be the only system being authorized to make connections with IS-05





BCP-003-02

- Describes techniques how to retrieve a token and get authorized access
- Describes techniques for NMOS nodes how to validate tokens
- Describes the type of information stored in the token



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



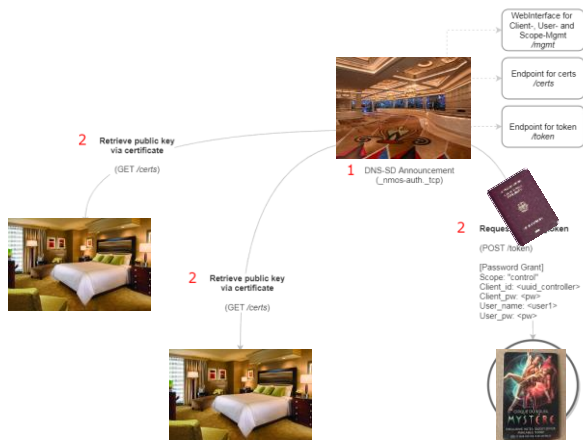
How to become authorized?



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



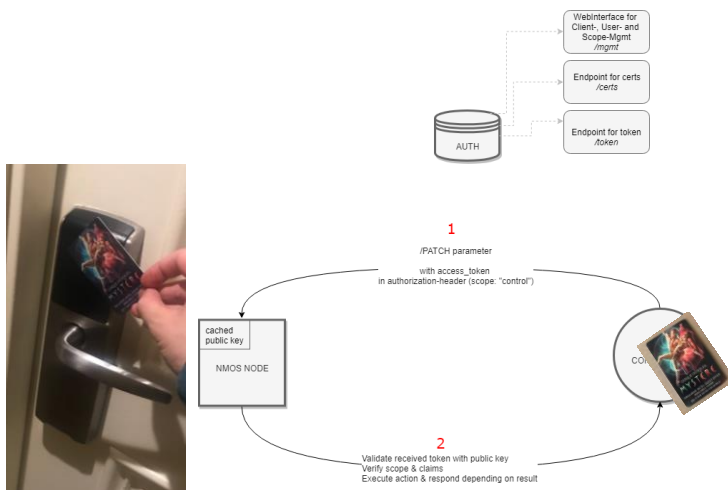
Initial setup – IS-10



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Accessing Resources



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



OAuth2 + JWT for NMOS

- Authorization server issues keys to ressource servers (=NMOS Nodes)
 - Needed to be able to decrypt tokens for validation
 - Keys are refreshed in short intervals (1 hour)
- Authorization server issues tokens to Clients (=control systems)
 - Needed to be able to perform actions against ressource servers
 - Clients need to be listed in advance in the auth server (out of scope)
 - LDAP/AD/SSO



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



JWT

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOiJlMjE2MTg1OTQsInVzZXIiOiJqYXNwZXIiLCJzY29wZSI6ImFkbWluIn0.2p09GURs9ZSskA7Banf53qB8ZizFt8sm_onnbtNuoF4
```

Decoded EDIT THE PAYLOAD AND SECRET

<p>HEADER: ALGORITHM & TOKEN TYPE</p> <pre>{ "typ": "JWT", "alg": "HS256" }</pre>
<p>PAYLOAD: DATA</p> <pre>{ "exp": 1521618594, "user": "jasper", "scope": "admin" }</pre>
<p>VERIFY SIGNATURE</p> <pre>HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), 3026ca5d3d13e5cc31c38b) <input type="checkbox"/> secret base64 encoded</pre>

- Header, Body, Signature
- Body containing claims
- Rfc7519
- Issued key needed to verify the signature
- only valid tokens are processed



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



```
{
  "iss": "https://auth.example.com",
  "sub": "username@example.com",
  "aud": "https://node.example.com",
  "iat": "1548779460",
  "exp": "1548783060",
  "x-nmos-api": {
    "name": "is-04",
    "node-read": true
  }
}
```

- Simple claims today
- More granular claims in future
 - Location
 - Role

```
"x-nmos-api": {
  "name": "is-04",
  "version": ["1.0", "1.1", "1.2"],
  "node-read": true
}
```

IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



BCP-003-02 in the “NMOS World”

- Authorisation server visible through DNS-SD
- Backwards compatible
 - Just send IS-04 and IS-05 without token
- Also applicable for IS-04 query API
 - Example: only some controllers are allowed to retrieve information



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Real word considerations

- Device exchange takes time
- Automating certificate handling and key exchange is a vulnerability
- Don't let additional effort stop you from implementing security best practices



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Security - Conclusion

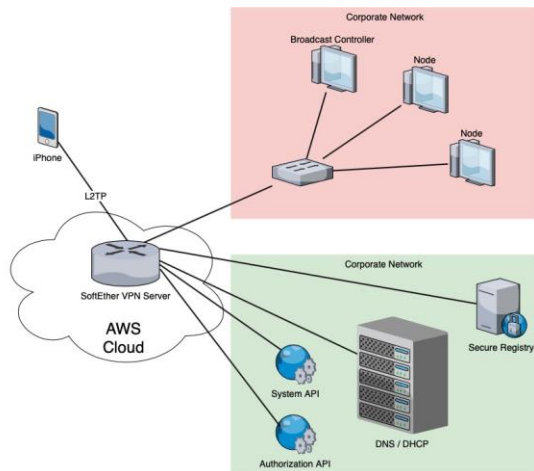
- IS-0x are based on standard IT technology
- HTTP and JSON are used by many other applications
- Other applications use OAuth2 and JWT already in large scale
- Key exchange workflow provides the fundamental environment for HTTPS transport
- Secure Transport enables OAuth2
- **TR-1001 workflows a must have**



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Virtual Workshop June 3-7 2019



- VPN Setup
 - DHCP
 - DNS
 - CA
 - Registry (HTTP/HTTPS)
 - Authorization
- Still online
- Become AMWA member
- Contact Thomas Edwards



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019



Thank you

Arne Bönninghoff

arne.boenninghoff@riedel.net | +49 177 8347500

Thank you to our Media Partners



IP SHOWCASE THEATRE AT IBC2019 : 13-17 SEPT 2019 42