Actors

- Client
- AUTHZ (Authorization Server)
- Printer

Dictionary

Public certificate
Certificate bought for public address. It is signed (directly or indirectly) by one of the public root CA.

Private certificate
Certificate issued by a local PKI and signed by a private root CA. Only clients having the private root CA installed can validate these certificates.

Public FQDN (Fully Qualified Domain Name)
Full hostname that can be registered in a public certificate (not IP number, not mDNS address). It DOES NOT mean that the hostname is resolvable on the Internet (it may be accessible only from the local network).

Local address
Host address not being a public FQDN.

Some facts

- The same certificate can be used for many hosts and/or Printers:
    - Printers with the same hostname (differs only by path)
    - Multi-domain certificates
    - Wildcard certificates

- In the local network, the uniqueness of public FQDNs is an illusion
    - By changing network and/or DNS configuration we can create a fake server with any FQDN (at least I believe so …)
    - … but these fake servers are not trusted because they do not have valid certificates.
    - This observation raises a question: In a local network environment, is there any difference between local addresses and public FQDN?

Possible TLS configuration of Clients

1. Clients have only public root CAs
    a. AUTHZ and all printers need public certificates
    b. AUTHZ and all printers must have public FQDN (even if visible only inside local network)
    c. Can be set up and maintained with some extra work and money (all certificates must be bought)

2. Clients have public root CAs and a private root CA
    a. AUTHZ and printers may have public and private certificates
    b. AUTHZ and printers with private certificates may have local addresses
    c. Admin must make sure that there are no conflicts between addresses (two private certificates with the same hostname or a pair of private/public certificates with the same public FQDN).
    d. But sometimes the conflicts are intentional, e.g.: each local network in the company has the same address to a local print server.

3. Clients have public root CAs and more than one private root CA
    a. Problem if the private CAs are managed by different entities
    b. Private certificates can be issued for any addressed, including public FQDN existing on the internet or on other local networks

We have to rely on the sanity of the admins here

TLS configuration requirements

Connection Client → AUTHZ

AUTHZ always has a certificate that the client can validate. Two cases are possible:

- AUTHZ has a public certificate
- AUTHZ has a private certificate AND the client has a private root CA installed

Connection Printer → AUTHZ

There are two possible options:

1. The Printer never talks to the AUTHZ - requirements (all must be met):
    a. OAuth token is a JWT containing everything that the Printer needs (there is no need for Token Introspection Request).
    b. The Printer has a public FQDN
    c. The URL of the Printer is registered (manually) on the AUTHZ.
    d. The URL of the AUTHZ is set (manually) on the Printer.
2. The Printer must connect to AUTHZ (to register itself OR to do Token Introspection Request). Two cases are possible (the same like for the Client):
    a. AUTHZ has a public certificate
    b. AUTHZ has a private certificate AND the Printer has a private root CA installed

Connection Client → Printer

The Printer has …	**public FQDN**	**local address**
Public certificate	Just works	Not possible
Private certificate	● The Client has a private root CA installed	● The Client has a private root CA installed ● Admin has to make sure that there is no other printers with the same address
Other certificate	It is possible only when the Printer allows for configuring hostname but not for setting the certificate (the certificate is self-generated). ● The Client must pin the certificate	● The Client must pin the certificate ● Admin has to make sure that there is no other printers with the same address

Trust Relationship

Requirements:

- Client can connect to AUTHZ
- Client can connect to Printer
- Printer can connect to AUTHZ
- TLS is in place
- AUTHZ has ~~public FQDN~~ (to be defined)
- Printer has ~~public FQDN~~ (to be defined)

Trust relationship	Mechanism	Configuration
Client trusts AUTHZ	Client has the URL of the AUTHZ on its “list of trusted AUTHZ”. It means that the administrator or the user explicitly added the URL to the list.	Initial configuration of the Client
AUTHZ trusts Client	AUTHZ challenges Client for Authentication Also, Client must be registered (this is optional, the AUTHZ may allow for dynamic registration)	
Printer trusts AUTHZ	The URL of the AUTHZ is set in the Printer configuration by the administrator/user (“oauth-authorization-server-uri”)	Initial configuration of the Printer
AUTHZ trusts Printer	AUTHZ has the Printer’s URL saved on its internal “list of printers”. During Token Introspection the Printer has an OAuth token (got it from the Client)	The administrator/user has registered the Printer with the AUTHZ.
Client trusts Printer	AUTHZ confirms the Printer URL during Token Exchange	
Printer trusts Client	Client has an OAuth token	

Possible attacks

Introducing a new node to the system (man-in-the-middle)

The new node can be created in two ways:

- Create a new node with a public certificate and some unused public FQDN
- Take control over existing node with working certificate (e.g.: frustrated employee)

The new node cannot be used as AUTHZ because:

- Clients trust only AUTHZ from “list of trusted AUTHZ”
- Printers has AUTHZ set in the configuration

The new node cannot be used as a Printer because:

- Client verifies the Printer’s URL in TokenExchange
- AUTHZ has “list of printers” with printers URLs

Taking control over Client

Intercept users credentials/sessions and obtain access to their printers and other resources.

Taking control over Printer

Intercept everything that goes through the printer.

Taking control over AUTHZ

Depends on the implementation/system architecture (pretty serious for sure).