The Printer Working Group

OAuth 2.0 Updates:
Trust Analysis and Resource Identifiers

Smith Kennedy, HP Inc.

2023-04-11

Use Case Scenarios

1. Enterprise Printing
   - Printing in an office that has sophisticated network infrastructure
   - Printer may be a Logical Device or Physical Device
     - Physical device usually has a unique hostname
     - Logical device may not have a unique hostname

2. Cloud Printing
   - Printing to a "cloud hosted printer"
   - Printer is very likely a Logical Device
   - Reachable over the Internet
   - May or may not have a unique hostname

3. Hybrid Work Home Office Managed Printing
   - Printing in a home or small office that lacks sophisticated network infrastructure
     - NAT router
     - .local domain hostnames
     - access is authorized by non-local authority (e.g. employer)
   - Printer is most likely a Physical Device
   - VPN may or may not be active for Client and/or Printer

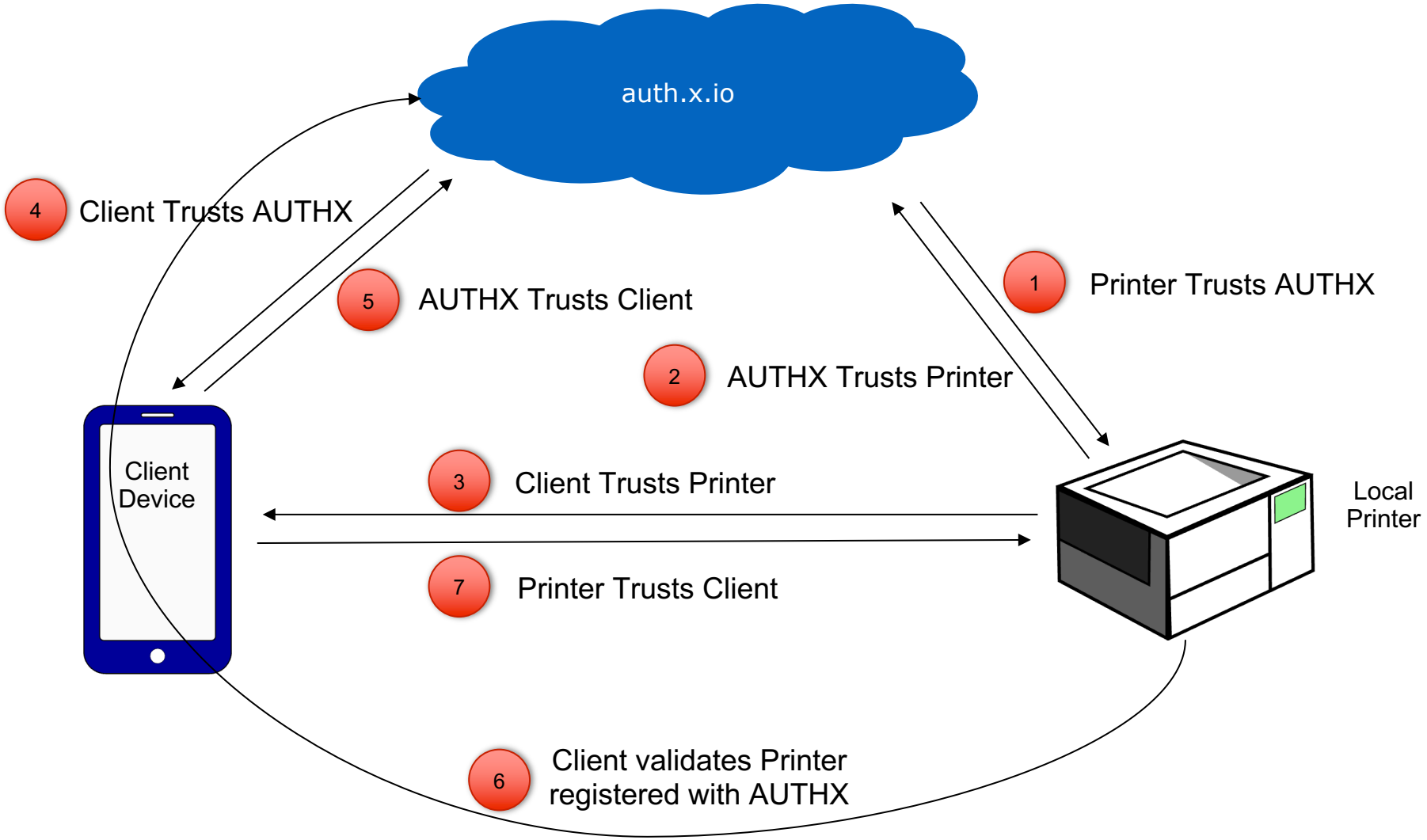
Defined Terms

- Token Exchange
  - An OAuth 2.0 operation where one Access Token is used to acquire another access token
  - For printing, a "Cloud Access Token" or "environment access token" (acquired shortly after user authentication) is "exchanged" for a "Device Access Token" (one that authorizes use of the device / print service specified by the Resource Identifier

- Resource Identifier
  - An identifier for a particular resource that is provided as the value of the "resource" parameter in a Token Exchange request (RFC 8693 section 2.1)
  - Value MUST be an absolute URI (RFC 3986 section 4.3)
  - In our cases, a "resource" is a printer or scanner service

- AUTHX
  - Authentication Service (avoiding use of "AUTHZ")

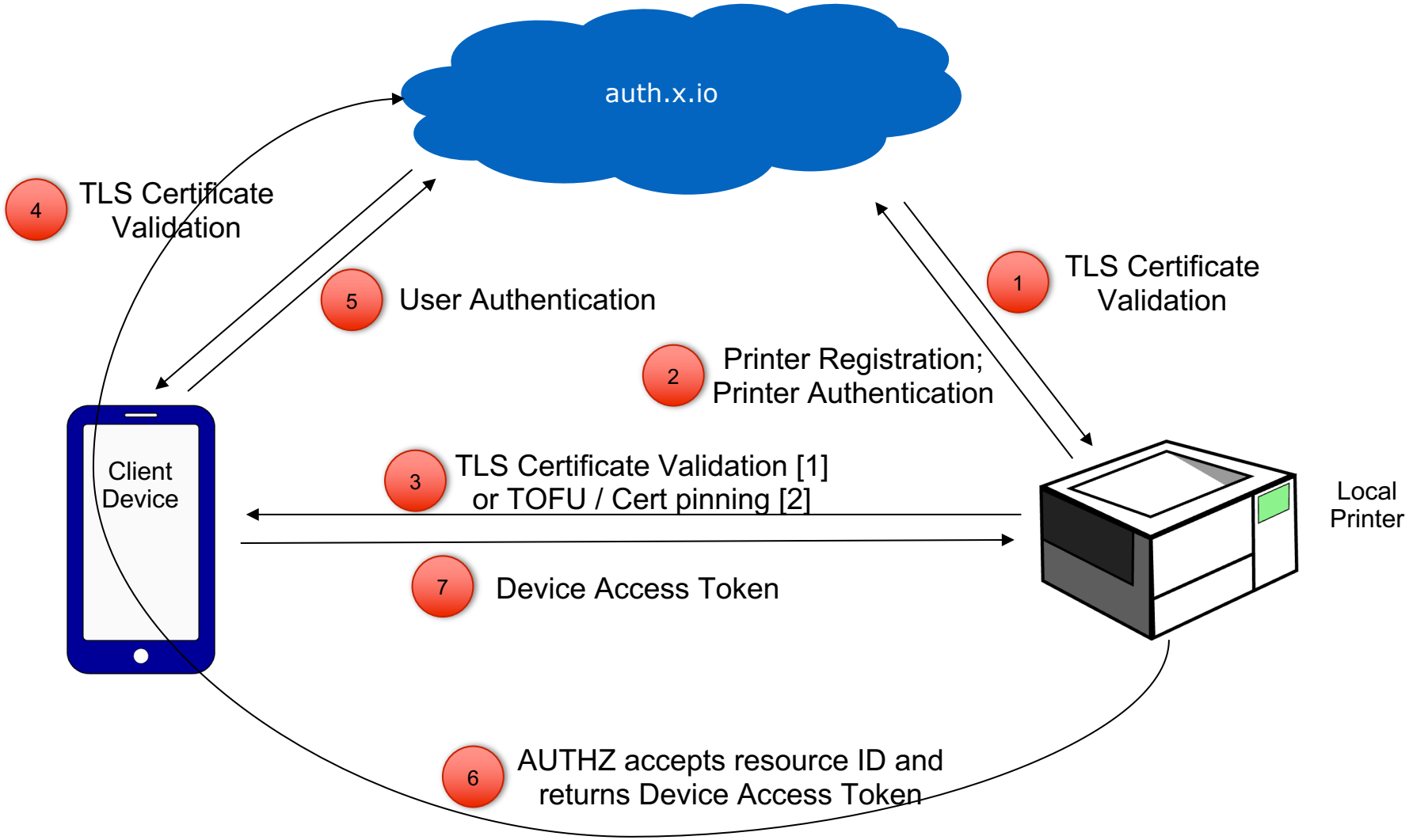
OAuth 2.0 Trust Relationships



OAuth 2.0 Trust Relationships

Relationship	Mechanism	Comments
1. Printer Trusts AUTHX		
2. AUTHX Trusts Printer		
3. Client Trusts Printer		
4. Client Trusts AUTHX		
5. AUTHX Trusts Client		
6. Client validates Printer registered with AUTHX		
7. Printer Trusts Client		

OAuth 2.0 Trust Relationships



OAuth 2.0 Trust Relationships

Relationship	Mechanism	Comments
1. Printer Trusts AUTHX	TLS Certificate Validation	AUTHX has valid certificate issued by trusted CA
2. AUTHX Trusts Printer	Device Authentication	Registration likely required; registration "artifacts" can be used for Resource Identifier
3. Client Trusts Printer	TLS Certificate Validation [1] or TOFU / Cert pinning [2]	
4. Client Trusts AUTHX	TLS Certificate Validation	AUTHX has valid certificate issued by trusted CA
5. AUTHX Trusts Client	User Authentication	User account creation might be needed
6. Client validates Printer registered with AUTHX	AUTHX accepts resource ID and returns Device Access Token	Trustworthiness depends on quality of the Resource Identifier
7. Printer Trusts Client	Device Access Token	

[1] – Printer has CA issued certificate and globally unique FQDN
[2] – Printer has self-signed certificate which is less trustworthy than a certificate issued by a trusted CA

3. Client Trusts Printer

BEST: TLS Certificate Validation + FQDN

- Conventional TLS certificate validation possible
- Certificate pinning may be used but not necessary
- Requires printer to have a globally unique FQDN and a certificate issued by a trusted CA

FAIR: Self-signed certificate + TOFU / Certificate Pinning

- Local printing in network environments that lack all but the most basic infrastructure
  - NAT router
  - Private IPv4 address range (RFC 1918)
  - ".local" domain hostnames are not guaranteed globally unique
- Trust on First Use / Pinning means accept it at first use, cache and compare at subsequent connections
- Can be improved with a trustworthy Resource Identifier

6. Client Trusts AUTHX & Printer Know Each Other

Authentication Service responds to Token Exchange with a Device Access Token

- Authentication Service returns a Device Access Token IF AND ONLY IF (a) the End User is authorized to access the resource; AND (b) the resource is known to the Authentication Service

- Trustworthiness of the Resource Identifier affects resistance to MITM attack between Client and Printer

7. Printer Trusts Client

- Client supplies an OAuth 2.0 Device Access Token as a bearer token in its HTTP request

- Printer validates OAuth 2.0 Access Token to authorize execution of the protected IPP operation
  - Get-User-Printer-Attributes
  - Validate-Job
  - Create-Job
  - Get-Jobs

Resource Identifier Types & Their Trustworthiness

Identifier	Source	Trustworthy?	Discussion
"printer-uuid"	IPP / mDNS	No	MITM can trivially acquire and reuse any openly available attributes
Printer URI	DNS + IPP + TLS Validation	Globally Unique FQDN: Yes Self-signed / .local domain: MAYBE	Depends on #5 Full URI including resource path needed
JWE or JWT	Non-standard web service	Maybe	Trustworthiness depends on quality of JWE / JWT design; needs countermeasures (fields, Client validation methodology) to prevent reuse by MITM
Printer TLS Certificate SHA-256 fingerprint	Printer TLS certificate	Yes	Printer registers current certificate fingerprint with AUTHX whenever certificate is updated Works equally well with CA-issued or self-signed TLS certificates;

"printer-uuid" for Resource Identifier

- Value needs to be recorded by Authentication Service at device registration time

- "printer-uuid" like any IPP attribute is not trustworthy
  - "naked" value not contained in a cryptographically secure wrapper
  - Adding it to the X.509 certificate would require certificate generation changes that could be awkward

Printer URI as Resource Identifier

- Current PWG "plan of record"

- Trustworthiness depends on several factors
  - Type of hostname in the URI
  - Type of TLS certificate the printer possesses
  - Full URI with resource path element needed – bare hostname not sufficient.
    - Print servers have one hostname supporting multiple "logical" printer instances, each at a unique resource path
  - Client MUST validate that TLS certificate CN or SAN matches URI hostname

- Trustworthiness of hostname / cert pairs
  - Globally Unique FQDN/CA-issued cert: YES
  - Globally Unique FQDN/Self-signed cert: No (TOFU?)
  - ".local" hostname/CA-issued cert: No (TOFU?)
  - ".local" hostname/Self-signed cert: No (TOFU?)

JWE / JWT as Resource Identifier

- Client sends JWE / JWT Resource Identifier request to Printer (mechanism TBD [1])
- Printer requests and receives JWE Resource Identifier from the AUTHX, and returns it to the Client
- Client submits received JWE / JWT as Resource Identifier to Token Exchange
- AUTHX returns a Device Access Token if Resource Identifier value is valid [2]

Issues to be addressed:

1. New operation / non-IPP operation / new IPP attribute
2. Trustworthiness depends on design of JWE / JWT to prevent reuse by a MITM

Printer TLS Certificate SHA-256 Fingerprint as Resource Identifier

(Idea proposed by Google last year in a PWG F2F meeting)

- Immutable value taken from the printer's TLS certificate
- Value registered by the Printer with the Authentication Service at device registration time
  - **Update needs to be sent whenever the printer's current TLS certificate changes**
- Trustworthy regardless of whether the printer's TLS certificate is self-signed or CA-issued
- Trustworthy regardless of whether the printer has a globally unique FQDN or a self-issued ".local" domain hostname

Resource Identifier Type Framework

Authentication Service requirements for Resource Identifier type(s) supported – is this a matter of policy?

If so, then the PWG may want to define or help define a "framework" that...

- Allows the Authentication Service to indicate what Resource Identifier type(s) it supports for its Token Exchange
- Allows a Client to discover what Resource Identifier types the Authentication Service supports

Would this be part of OAuth? Defined in PWG or elsewhere?