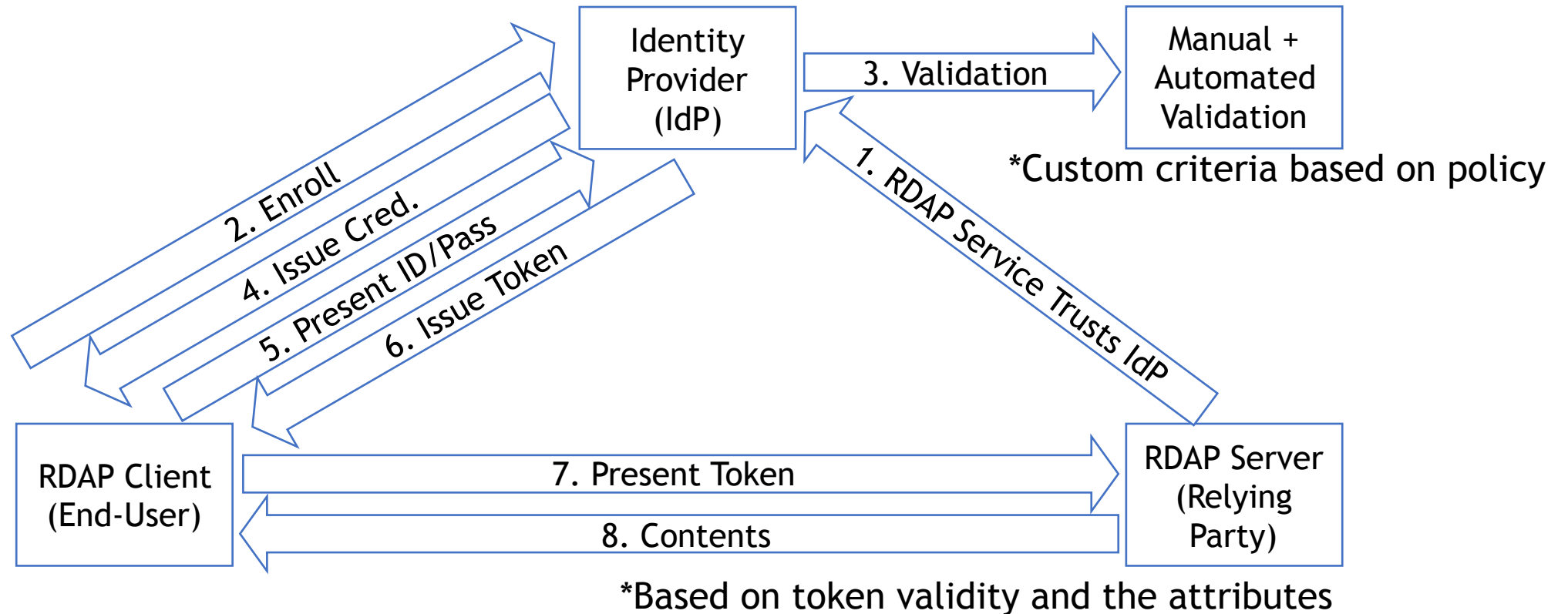


# Comparison of Federated Authentication and TLS Client Authentication

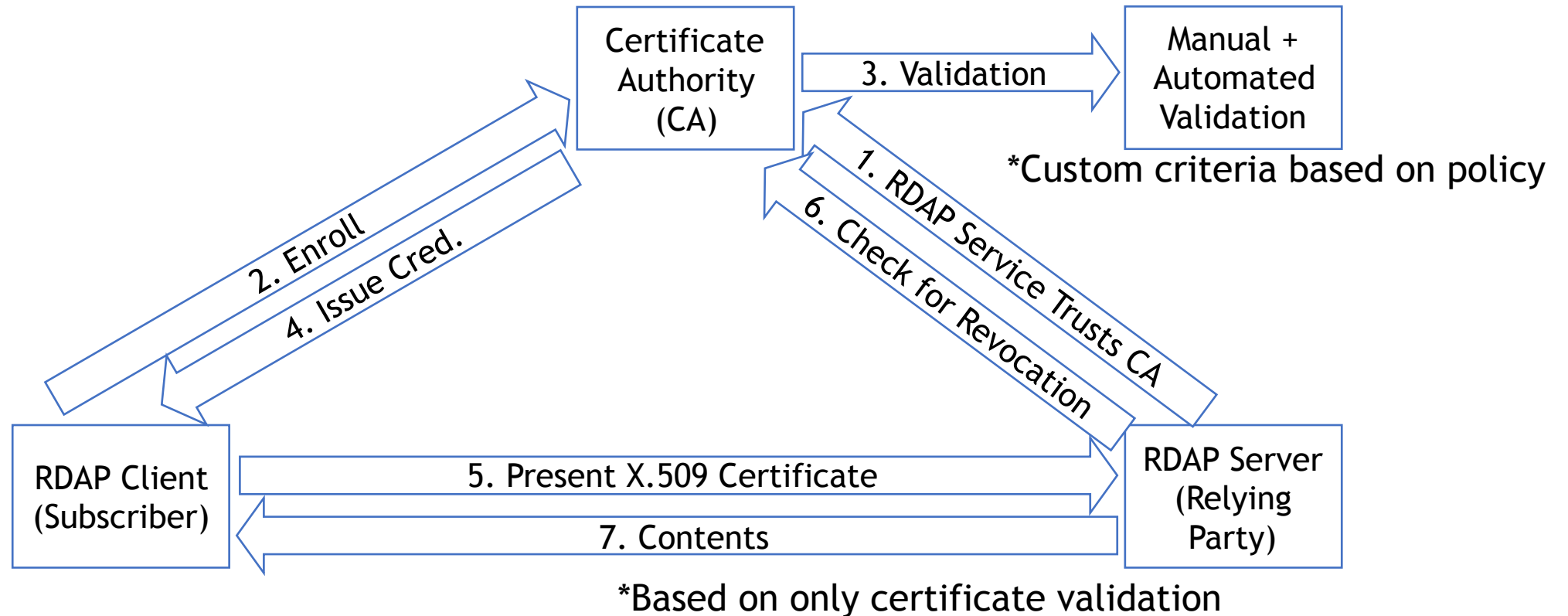
Tomofumi Okubo

DigiCert, Inc.

# Federated Authentication High-Level Overview



# TLS Client Authentication High-Level Overview



# High-Level Comparison Chart

	Federated Authentication	TLS Client Authentication
Protocol	OAuth2.0 (rfc6749)	TLS (rfc5246)
Layer	Application Layer	Transport Layer
Credential	ID and Password	Digital Certificate
Credential strength	<b>What you know</b>	<b>What you have + What you know</b>
Support accreditation based on policy	Yes	Yes
Support immediate cred. revocation	Yes	Yes
Support basic access control	Yes	Yes
Support attribute based access control out-of-box	Yes	No
Tokens/creds carry attributes out-of-box	Yes	Yes
Servers understands attributes out-of-box	Yes	No
Cred. management overhead on User	No	Yes
Credential reissuance (Forgot/Lost Credential)	Instant	Moderate
Binds identity to the credentials	No	Yes

# High-Level Comparison Chart Cont'd

Trust (Anchor) Management	Simple	Moderate
Risk of bad implementation out-of-box	Low	Low
Risk of bad implementation handling attributes	Low	Moderate
Mitigates TLS man-in-the-middle	No	Yes
Cred. support hardware (Physical Token)	No	Yes
Flexibility to add attributes	Limited	Unlimited
Supports non-repudiation	No	Yes
Implementation lead time	Short	Long

# Observations

- Due to the tight deadline (90 days?), it is sensible to choose Federated Authentication for the short-term solution.
- A hybrid model where the authentication and validation of the end-user is done CA-style then issue a credential for federated authentication would provide optimal security.
- In the future, if there is a need for extensibility or the RDAP operator to confirm identity of the end-user is needed, usage of X.509 certificates could be taken into consideration.
- Also, since these two technologies do not collide, both can be used in the future if maximum security is desired. (Needless to mention, the balance between convenience and security needs to be considered.)

Thanks