FDO (F*ast*ID*entity*O*nline* Device Onboarding)

- Device onboarding scheme or protocols
- Preferably for IoT devices and IoT DMS platforms
- Late Binding -> Actual Device ownership assignment need not be required at Device Manufacturing
- Late Binding -> achieved using Ownership Transfer (TO) & ownership vouchers
- Rendezvous Server -> Both Device and Onboarding service meets at this server to publish their identity
- Mutual Trust Flows:
  - TO-0: Onboarding Service(Final Owner) registers ownership with RV(GUID + IP)
  - TO-1: Device connects to RV and gets IP of Onboarding Service
  - TO-2: Device connects to Onboarding Service and mutual trust

sZTP(secure Zero Touch Provisioning) (RFC-8572)

- Method to securely provision a networking device
- Defines a bootstrap strategy to securely obtain bootstrap data(onboarding/redirect info, owner certificate, ownership voucher)
- Defines RESTCONF data models for communicating bootstrap data
- Provisioning scope: update/install boot image, apply initial config and execute some scripts
- Sources of bootstrap data: DHCP/DNS/Bootstrap server
- Bootstrap server: A RESTCONF server Implements YANG data model
- Capable of using TLS for connections with device
- Device : TLS client certificate and any intermediate certificates leading to well-known CA certificates
- Device should possess TLS client certificate to authenticate itself with bootstrap server
- Device should possess trust anchor certificate(CA) of the owner certificate to verify signature on signed Boostrap data

sZTP vs FDO

sZTP	FDO
No clear specification on mechanism for mutual trust	Specifies a clear mechanism for mutual trust
Specifies multiple sources for bootstrap data like DHCP,DNS, bootstrap server (basis is existing mechanisms)	Specifies about Rendezvous server, Device onboarding servers,
More kind of networking device onboarding method.	A General device onboarding method.
Limited availability of reference implementations	Good reference implementations.
Relatively less infrastructure requirements	Require more infrastructure. Run multiple servers like RV, DMS, Onboarding servers.
Device Attestation using regular 1:1 Private & Public Key PKI	Device Attestation using EPID security scheme.

sZTP + FDO: How can both complement each other?

FDO: For Device Identity(Late Binding benefits) and Mutual trust

sZTP: For Data modeling specification(YANG/RESTCONF/NETCONF) to migrate existing network device/OS easily.