	BRSKI	SZTP
standardization	RFC 8995	RFC 8572
Related RFCs	Voucher artifact [RFC 8366]	
Aim	Results in the pledge storing a root certificate sufficient for verifying the registrar identity. The installed Trust anchor can be used for later certificate enrollment protocols (EST)	Without any manual interference beyond physical placement, securely update the boot image, commit an initial configuration, and execute arbitrary scripts to address auxiliary needs.
communication channels covered by the protocol	Pledge<->Registrar<->MASA	Device<->Owner(<->MASA: not protocol inherent)
remote(Internet accessible)/local bootstrapping sources support	local	remote and local
Device bootstrap sources	Domain Registrar	Removable storage, DNS server, DHCP server, or Bootstrap server
protocol initiator	Device	Device
Functionality support (M): Mandatory (O): Optional	- (M) Pledge-Registrar Discovery - (M) MASA: voucher issuance - (M) MASA: voucher renewal - (M) Pledge: polling - (M) MASA voucher audit log - (M) if EST following BRSKI: CSR attributes retrival request - (O) Manufacturer: Ownership tracking	(M) Device: polling (M) MASA: voucher issuance (M) if Bootstrap serveris used: provide redirect information and/or onboarding information (M) DHCP/DNS server: can provide redirect information only due to technical limitations
device initial state	IDevID manufacturer installed trust anchor(s) associated with the manufacturer's MASA	- IDevID Optional: - TLS client cert & related intermediate certs - Trust anchors to validate ownership voucher (signed by manufacturer) - List of well-known bootstrap servers - Trust anchors to authenticate configured well-known bootstrap servers
discovery of bootstrap sources	yes, mDNS/ GRASP	only through redirections from device supported bootstrap sources
Device authentication	IDevID	IDevID

device authorization	- a specific device (serial number) from a specific vendor - a specific device type or a specific vendor	based on device's serial number
bootstrap source authentication	Intially, Provisional TLS	Initially, Provisional TLS if no TA available
enrollment protocol integration	(R) EST	None
bootstrapping data	voucher	redirect information (auxilary) onboarding information: boot image, configuration, post-config scripts, ownership voucher, owner certificate
bootstrapping data protection	signed	trusted channel: may be signed and/or encrypted untrusted channel: signed and may be encryped
owner voucher-request time	nonced: in-band nonceless: Out-of-band	nonceless: owner-manufacturer enrollment phase nonced: in-band
Acceptance of device by Domain	checking voucher and its presence in the MASA audit-log	checking the voucher
determining MASA to contact	URI in IDevID or manual confiuration of registrar	out of scope
progress reports	yes, voucher status telemetry	yes, only to trusted servers
Timeliness	nonceless vouchers: expiry time nonced vouchers: nonce (and expiry time)	
revocation checks	- No revocations for vouchers - certificate revocation checks only, depending on pledge capabilities	
ownership transfer	yes, By voucher issuance	out of scope (Owner<->MASA communication is not inherent to the protocol, but ownership transfer is possible through new vouchers by the MASA)
updatable Trust Anchors	out-of-scope	out of scope (through a verifiable process, such as a software upgrade using signed software images)
transport protocol	HTTP (or CoAP) / TLS1.2+	HTTP/TLS
Required crypto algorithms	None	None
Domain specific configuration provisioning to device	out of scope	yes

Terminology defenition in sheet 2

Terminology comparison in sheet 3