	A	B	C	D	E	F	G	H	I	J
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										

	A	B	C	D	E	F	G	H	I	J
1	**Hardware Space (seek to influence)**									
2	**Ecosystem and supply chain**		**Silicon**		**Commercial Firmware**		**Open Source Firmware**			
3	**AMD**	**Intel**	**AMD**	**Intel**	**3mdeb Dasharo (oreboot/coreboot/UEFI/OSF)**	**UEFI IBV**	**Intel**	**AMD**	**3mdeb**	**TrenchBoot Validation Test Suite**
4	Key signing for AMD HVB		AMD: Provide solution for SL DEV to IOMMU hand off		AGESA		FSP	AGESA	Coreboot base port	TPM accessible on standard bus address 0xfed4000
5	QEMU SKINIT emulation/virtualization for guest DRTM	QEMU SENTER emulation/virtualization for guest DRTM	fTPM should be compliant to PC profile (locality 4)		FSP	Produce DRTM ACPI table	Open SoC support code	IOMMU DMA protection	Produce DRTM ACPI table	
6	TB issues research paper [CITRIX, 3mdeb, Apertus]				coreboot base port	IOMMU DMA protection	NDA BtG provisioning	NDA AMD HVB provioning tools		
7					IOMMU DMA protection		Open Source Intel BtG provisioning tools	Open Source AMD HVB/PSB provisioning tools		
8					NDA BtG provisioning tools	Integrated Intel STM	Redistributable ACM BIOS	Open Source AMD SMM Supervisor		
9					NDA AMD HVB provisioning tools	Integrated AMD SMM Supervisor	Open Source ACM SINIT			
10					Open Source AMD HVB/PSB provisioning tools		Open Source ACM BIOS			
11					Open Source Intel BtG provioning tools		Open Source TXT provisioning tools (TXT can be fused off by ME)			
12					AMD oreboot (Rust) for EPYC					
13	Halo									
14	Hard to fullfill dependencies									

	K	L	M	N	O	P	Q	R	S	T
1										**Software Space**
2	**UEFI**		**GRUB**		**iPXE**	**LZ or New Name**		**Xen**	**Linux**	
3	**3mdeb**	**Apertus**	**Apertus**	**3mdeb**	**3mdeb**	**Apertus**	**3mdeb**	**Apertus**	**Apertus**	**3mdeb**
4	TB support in Shim, make Shim kick Linux with DRTM		Intel support upstream	AMD support upstream	AMD support upstream	Implement solution using AMD solution for SL DEV to IOMMU hand off		Add SHA and TPM support to Xen hypervisor	Intel support upstream	AMD support development
5	Have Microsoft sign the modified Shim				RNG for HTTPS			Build Security Engine for DomB Boot Domain	AMD support upstream	
6										
7										
8						[Future] Measured Secure Boot				
9										
10										
11										
12										
13										
14										

	U	V	W	X	Y	Z	AA	AB	AC	AD
1	**(seek to contribute)**									
2	**Linux KVM**				**Linux User Space**					
3	**Apertus**	**Oracle**	**3mdeb**	**Microsoft**	**Yocto**		**Debian**	**Canonical (Ubuntu)**	**LF Edge**	**RedHat (Fedora)**
4	Upcoming capability early access available under NDA		AMD Demo		**Apertus**	**3mdeb**	Create packages for TrenchBoot components	Create packages for TrenchBoot components	Create packages for TrenchBoot components	Create packages for TrenchBoot components
5	QEMU SKINIT emulation/virtualization for guest DRTM				Review and upstream	Update Yocto recipes	CI for testing packages build for each release	CI for testing packages build for each release	CI for testing packages build for each release	CI for testing packages build for each release
6	QEMU SENTER emulation/virtualization for guest DRTM					Add meta-trenchboot to OE layer index	Set up a TrenchBoot package feed	Set up a TrenchBoot package feed	Set up a TrenchBoot package feed	Set up a TrenchBoot package feed
7	Kexec preamble support for DRTM reLaunch					Add more supported platforms (e.g. the EPYC one)	Upstream packages	Upstream packages	Upstream packages	Upstream packages
8						Add more test cases (CI)				
9										
10										
11										
12										
13										
14										

	AE	AF
1		
2		
3	**Apertus**	**Others**
4	Publish roadmap spreadsheet	Create a webinar about TB roadmap, have everybody there, not later than end of March
5	Strong RoT vTPM vs. weak RoT swtpm	GitHub tools for planning, roadmaps
6	Remote attestation for TrenchBoot	
7	Create a Consulting section on TB page	
8	Create TDF (TrenchBoot Developer Forum)	
9		
10		
11		
12		
13		
14		