EFFECTIVE JULY 7th, 2021										
All Suppliers seeking OCP Product Recognition are required to fill out this form.										
1) Name this file as follows:		YEAR Supplier Name PRODUCT (INSP or ACPT)				Year, Supplier name, Product Name or Model, OCP Inspired or OCP Accepted.				
2) Fill out the sheet depending on which Product Recognition you are seeking. See table below.										
3) Fill out Appendix B of the Base Spec on which the product is based. Add this link to this spreadsheet in the table.										
4) Complete the requirements for OCP Product Recognition: OCP Solution Provider Agreement, OCP Certification Mark Agreement, Copyright License Agreements, etc (links available here)										
5) Contact OCP with any questions										
For OCP Inspired™	**All Products**	**Notes**								
Supplier Details	X									
Open System Firmware										
Security (No Badge Level)	X	Needed for main board or any cards. For Additional Security Badges (Bronze/Silver/Gold), member can fill out the detailed Security Profile Requirements for that level.								
Hardware Management	X									
BMC										
For OCP Accepted™	**All Products**	**Notes**								
Supplier Details	X									
Open System Firmware	X	Initialization Firmware								
Security (No Badge Level)	X	Needed for main board or any cards. For Additional Security Badges (Bronze/Silver/Gold), member can fill out the detailed Security Profile Requirements for that level.								
Hardware Management	X									
BMC	X	Source Code + Binary Blobs								

Supplier Details				
	Name	Contributor(s)	Link in Contribution DB	
Base Spec				
Product Name				
Product Part #				
Product Landing Page				
Supplier Details				
Name of Supplier				
Address				
Point of Contact				
Email				
Phone #				
Scope of Services for Sales Support				
Presales				
Post Sales				
Project or Sub-Project				
Product Recognition				
Which Product Recognition?				
if OCP Accepted™, provide Design Package Link				

Open System Firmware Requirements Checklist (v1.2)

This form will help self-access compliance for Open System Firmware. Note these requirements only apply to the main application processor on server platforms. Please contact the OSF Leadership Team to see if your Product qualifies.

Note that all items marked below as required are a MUST in order to quality for OCP-Accepted™ product recognition.

Reference Document:

Open System Firmware Checklist

Instructions:

1. Upload artifacts listed in section 1.2 to OCP's GitHub: https://github.com/opencomputeproject/OpenSystemFirmware/
   Instructions on using GitHub can be found here: https://docs.github.com/en/github/managing-files-in-a-repository/adding-a-file-to-a-repository
   Note, these artifacts are made public as soon as they are uploaded.
2. Complete the form below.

1 Review Package	**Required?**		**Notes**
1.1. Required Supporting documentation		***Answer FREEFORM***	
a. Name of the platform under review	Yes		
b. Short description of the host firmware and its technical features	Yes		See Appendix B of the OSF checklist for what constitutes a "technical feature".
c. Emails to contact during the review process	Yes		
d. **PROVIDE URL** for submission on OCP's GitHub	Yes		Artifacts must be submitted to https://github.com/opencomputeproject/OpenSystemFirmware/
e. List of other URLs for any source code dependencies	Optional		For example, a link to https://github.com/tianocore/edk2
1.2. Required Artifacts		***Answer YES if the artifact is included on OCP GitHub***	
a. *Firmware image*	Yes		*Firmware image*: A binary file which, when written directly to the firmware medium (typically a NOR FLASH, but other mediums are valid), will boot the machine.
b. Description of the firmware ownership model	Yes		As described in section-3
c. Top-level build script	Yes		As described in section-4
d. Documentation	Yes		As described in section-5
e. Test results	Yes		As described in section-6
f. Tool for user modification	Yes		As described in section-9

2. Licensing and Redistribution	**Required?**		**Notes**
2.1. The entirety of the review package and artifacts are:		***Answer YES or NO***	
a. *redistributable*,	Yes		*Redistributable*: A software component (in source or binary form) with a license permitting redistribution from anyone to anyone by any means without an NDA, payment or royalties.
b. publicly available for download, and	Yes		
c. submitted during the review process under a license that allows OCP to host on the marketplace.	Yes		
2.2. All source code published as part of the review process must meet the definition of *open-source*.	Yes		*Open-source*: Source code which is *redistributable* under an OSI-compatible license as defined by https://opensource.org/licenses and is publicly available for download.
		Answer FREEFORM	Feel free to use Sheet2 for more room.
2.3. OSF is *open-source* by default. Closed-source items are allowed given an approved and reasonable exception reason such as "containing silicon IP". Each closed-source item must be redistributable, included in the submission and reasonably granular. It is strongly encouraged, but not required, that every severable firmware component (e.g. a UEFI driver) be so documented.	Optional		*Open-source*: Source code which is *redistributable* under an OSI-compatible license as defined by https://opensource.org/licenses and is publicly available for download.

3. Ownership and Reusability	**Required?**		**Notes**
3.1. *Owners* must have the ability to:		***Answer YES or NO***	*Owner*: The owner of the physical machine.
a. Update the firmware on the machine.	Yes		
b. If firmware needs to be signed*:* b.i. Choose their own firmware signing key and change it as needed over time OR obtain the necessary signing key(s) through a transfer of ownership process. b.i.1. Note that, in particular, a requirement to choose immutable keys in advance and provide to, e.g., a chipset vendor or ODM makes a system noncompliant.	Yes		
c. Change owners at least 8 times.	Yes		The number '8' is considered by end-users to be too low; it was chosen based on chipset vendor guidance concerning the limits of current chipsets. OCP reserves the right, in later versions of this spec, to increase the number. The most desirable value would be infinity, as in, e.g., Chromebooks
d. Transfer ownership to a non-predetermined owner.	Yes		

4. Build System	**Required?**		**Notes**
4.1. Build and update utilities must be:		***Answer YES or NO***	
a. *open-source*, or	Yes		*Open-source*: Source code which is *redistributable* under an OSI-compatible license as defined by https://opensource.org/licenses and is publicly available for download.
b. a *redistributable* binary which must run natively under at least Linux or Windows.	Yes		*Redistributable*: A software component (in source or binary form) with a license permitting redistribution from anyone to anyone by any means without an NDA, payment or royalties.
4.3. The top level build script shall be the only script needed to be run to fetch all source code, binary blobs needed, and to build an entire host firmware image.	Yes		
a. The top level build script may invoke other scripts and utilities to carry out its main function.	Yes		
b. It must be possible to build without a network connection once a suitable set of packages and binaries have been gathered.	Yes		
4.5. If the platform requires signed firmware, it shall be possible for the owner to sign the image with a user-provided key. It must be possible to re-sign the firmware with a new key. Signing must continue to work after End Of Support.	Yes		*Owner*: The owner of the physical machine.

5. Documentation	**Required?**	***Answer YES or NO***	**Notes**
5.1. Documentation describes features of firmware, and build and install procedures.	Yes		
a. The documentation shall describe the validation scope (i.e. the test regime).	Yes		
		Select LEVEL	
5.3. The documentation shall describe the readiness of the OSF with one of the following levels:	Yes		
a. Pre-silicon. The OSF is good enough for pre-silicon entrance on the corresponding OCP platform as-is.			
b. Power-On. The OSF is good enough for power-on entrance on the corresponding OCP platform as-is. This is the level described in this checklist.			
c. Pre-production. The OSF is good enough for pre-production entrance on the corresponding OCP platform as-is.			
d. Production. The OSF is good enough for production entrance on the corresponding OCP platform as-is.			

6. Test Regime	**Required?**	***Answer YES or NO***	**Notes**
6.1. The platform with OSF must be capable of booting an operating system whose code is openly available under an OSI-approved license (such as Linux).	Yes		
6.2. Bare minimum: The platform with OSF needs to be able to be cold re-booted into OS 100 times sequentially without issue.	Yes		
6.3. If the system advertises support for a warm reboot, the platform flashed with OSF needs to be able to be warm re-booted into OS 100 times sequentially without issue.	Optional		
6.4. Any support contract or warranty must confirm the system is conformant with such reboot tolerance.	Yes		

7. Standard Compliance	**Required?**	***Answer YES or NO***	**Notes**
7.1. For a given architecture family, the minimum standard interfaces required to boot and run a reasonable set of kernels must be provided. E.g., if required, ACPI should be available. On Power or RISC-V, flattened device tree should be available.	Yes		

8. Firmware Configuration	**Required?**	***Answer YES or NO***	**Notes**
8.1. The OSF needs to provide a tool so that firmware configuration can be viewed and changed from, at minimum Linux, and optionally Windows.	Yes		
8.2. This tool must be released in source form under an OSI-approved license. Existing examples in Linux include efibootmgr, sysfs variables, etc..	Yes		

9. Firmware Upgrade	**Required?**	***Answer YES or NO***	**Notes**
9.1. *Open-source* software must exist to update the firmware OR sufficient public documentation exists to write such software.	Yes		*Open-source*: Source code which is *redistributable* under an OSI-compatible license as defined by https://opensource.org/licenses and is publicly available for download.
9.2. *Owners* must have the ability to update the firmware on the machine regardless of its state in its current life cycle.	Yes		*Owner*: The owner of the physical machine.

Security Checklist Assessment Form

This form will help you self-assess the security compliance level of the product you're submitting.

It is ok if you answer "no" as future adopters would like to still understand the Security Profile of your product. If you choose, you can apply for higher badge levels depending on the security of your product.

This Profile is REQUIRED for all product recognition, please fill it out for the main motherboard in your product or any cards.

Reference Documents:

For more details and background context on the questions in this Security Profile, please refer to the following detailed documents:

- Secure Boot - link
- Attestation of systen components - link
- Common Threats - link
- Secure Firmware Development Best Practices - link

Additional Security Badge Levels

If you are ready to apply for a "Security Badge" for your product as a differentiator, fill out the additional details on your Security Profile for each level.

This is an annual self assessment. Specific Badge requirements will evolve year over year so we are awarding this on an annual basis. To update your Security Badges to the latest year, the self assessment will be required for the latest criteria.

For 2021 Security Badges, you can qualify for either Bronze, Silver or Gold Security Badge levels, as described here:

2021 Bronze: secure boot + attestation support ("must" requirements)

2021 Silver: Bronze level + "should" requirements + secure update + secure recovery + threat model document + semi open (e.g. source code available to customers under NDA)

2021 Gold: Silver + full feature set (including support for "may" requirements), publicly open security code, and FIPS certification.

To qualify for a certain level, the product needs to meet all requirements marked as such in the Security Profile below.

Self-Assessment Form

1. Badge Level

a. What is being certified? *System = a motherboard, or the main board of a system.* *Card = a peripheral device, such as NIC, HBA, Disk, etc.*	**System**
b. What level of security badge are you applying for?	**No Badge**

2. Cryptography and Randomness	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does all the cryptography used in product follow the recommendations in relevant NIST Special Publications? (e.g. NIST, CNSA suite)	**[Yes/No]**	Bronze	
b. Are cryptographic implementations validated under the NIST Cryptographic Algorithm Validation Program (CAVP)??	**[Yes/No]**	Silver	
c. Are cryptographic modules validated at overall level 2 or higher under FIPS 140-2 or FIPS 140-3?	**[Yes/No]**	Gold	

3. Secure Provisioning	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Are initial provisioning operations carried out in a trusted facility?	**[Yes/No]**	Bronze	
b. Does the product have a unique and immutable device ID key, an attestation key, and a key identifying the authority over updates?	**[Yes/No]**	Bronze	
c. Does the product support authenticated ownership transfer?	**[Yes/No]**	Gold	

4. Secure Boot support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does secure boot start from an immutable source?	**[Yes/No]**	Bronze	
b. On each reset of a device, are secure boot public keys used to authenticate the first stage mutable code or manifest?	**[Yes/No]**	Bronze	
c. Is an anti-rollback mechanism provided?	**[Yes/No]**	Bronze	
d. Is error detection of critical security parameters implemented?	**[Yes/No]**	Bronze	
e. Is secure boot failure notification provided?	**[Yes/No]**	Bronze	
f. Is a secure boot key revocation mechanism provided?	**[Yes/No]**	Silver	
g. Does the device support multiple secure boot root keys or root key digests?	**[Yes/No]**	Silver	

5. Attestation support	Self-Assessment	Badge Level	Additional Explanation (if needed)
5.1 Measurement and Attestation *(only needed if certifying a component device)*			
a. Does the device support the OCP Attestation protocol, as an attester device?	**[Yes/No]**	Bronze	
b. Is the first measurement taken by an immutable root of trust?	**[Yes/No]**	Bronze	
c. Must the device be reset in order to clear the measurements?	**[Yes/No]**	Bronze	
d. Is the measurement storage integrity protected (e.g., in a TPM)?	**[Yes/No]**	Bronze	
e. Are dynamic changes in configuration or firmware measured?	**[Yes/No]**	Silver	
f. Does the vendor provide a list of what is measured (code and configuration)?	**[Yes/No]**	Silver	
g. Does the vendor provide expected measurement values?	**[Yes/No]**	Gold	
h. Does the device offer a structured log of measurements?	**[Yes/No]**	Gold	
5.2 Verification Support *(only needed if certifying a platform)*			
a. Does the platform support the OCP Attestation protocol, as a verifier?	**[Yes/No]**	Bronze	
b. Does the platform support comparing the inventory to a manifest containing expected devices and their configurations?	**[Yes/No]**	Gold	

6. Secure Firmware Update support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does the product support secure firmware updates (i.e. validate firmware signatures upon update)	**[Yes/No]**	Silver	
b. If yes, please provide link to relevant feature documentation:	**[Link]**	Silver	
c. Are dynamic updates authenticated and / or measured?	**[Yes/No]**	Silver	

7. Recovery support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does the product support automatic recovery in case of firmware corruption?	**[Yes/No]**	Silver	
b. If yes, please provide link to relevant feature documentation:	**[Link]**	Silver	

8. Threats Assessment	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Are there any known **unfixed** CVE's in the product or one of its components, as-of the date of release? *(If yes, please provide explanation on how the security risk is mitigated)*	**[Yes/No]**	Bronze	
b. What is the mechanism available for getting future firmware patches? (e.g. provide a link to a documented security response process, or free form explanation)	**[Freeform text, or Link to documentation]**	Bronze	
c. Please provide a link to a threat model document for the product. *(For an example template for a threat model document, please refer to appendix A of the common security threats document)*	**[Link]**	Silver	
d. Was the product developed following any documented SDL (Security Development Lifecycle) ?	**[Yes/No]**	Silver	
e. If Yes, and the SDL is available publicly, please provide a link to it.	**[Link]**	Silver	

9. Access to firmware source code	Self-Assessment	Badge Level	Addtional Explanation (if needed)
a. Is the source code for security-relevant features available for review (e.g. code available under NDA, or via a trusted 3rd party audit report)?	[Yes/No]	Silver	
b. Is the source code and build environment for all security features available in a public repository?	[Yes/No]	Gold	
c. If Yes, please provide the link to the source code:	[Link]	Gold	

Needed for both OCP Inspired™ and OCP Accepted™ product recognition			
Please answer the following questions:	**Required?**	**Answer**	**Action**
Did you execute and pass the Redfish Service Validator v1.3.9?	Yes		If yes, upload report in Contribution Portal. If no, provide reason.
Did you execute and pass the Redfish Protocol Validator v1.0.2?	Yes		If yes, upload report in Contribution Portal. If no, provide reason.
Does the platform's manageability interface conform to the Redfish Interop Validator v1.1.7 with the appropriate Redfish profile?	Yes		If yes, upload report in Contribution Portal. If no, provide reason.
If applicable, which platform does the manageability interface conform to?	Select One	Server	If yes, upload report in Contribution Portal. If no, provide reason.
Did you execute and run the Redfish Usecase Checker v1.0.6 (reco	Yes		If yes, upload report in Contribution Portal. If no, provide reason.
All exceptions will need to be approved by the Project Leads. If approved, then it will proceed to the IC for review for consideration.			

BMC (if applicable)	Needed for OCP Accepted™ product recognition					
Submission Type	**Description**	**License**	**Recognition**	**Action**		
For Source Code + Binary Blobs	Package: source code and instructions enabling one to build a binary		for OCP Accepted™	https://github.com/opencomputeproject/OpenSystemFirmware/[vendor_name]/[product_name]/		