

Secure Boot: Getting your SHIM signed - The process and its challenges

Sherif Nagy

Rocky Linux Release Engineer / Accredited shim reviewer



LINUX
PLUMBERS
CONFERENCE

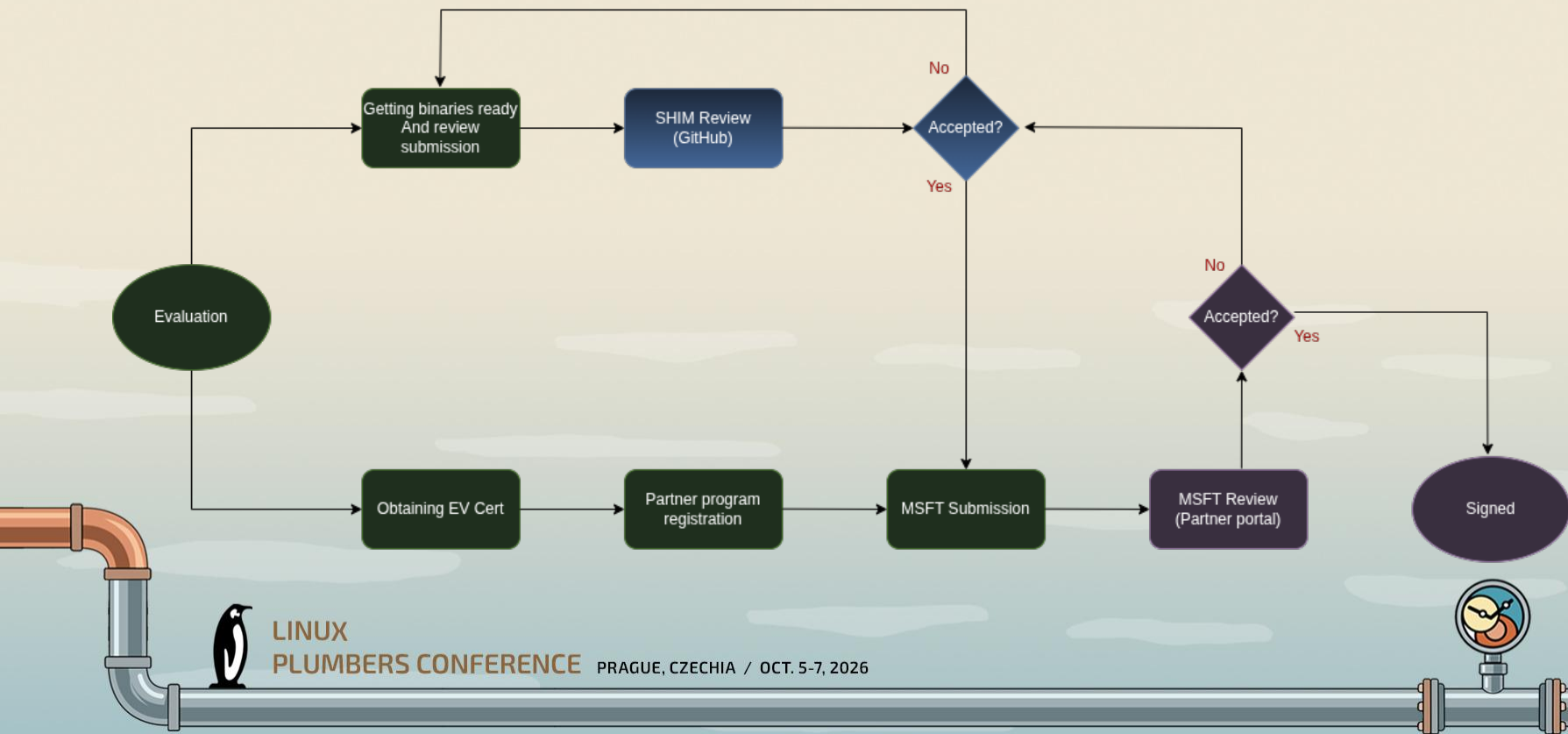
PRAGUE, CZECHIA / OCT. 5-7, 2026

Agenda

- Process overview
- Distribution requirements
- Microsoft registration process
- Community review pipeline
- Microsoft Submission & final review
- Timeline & common pitfalls
- Process improvements discussion + Q&A
- Contact & contribution channels



Process overview



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Distribution requirements

- Evaluation of the need for Microsoft signed shim
- Preparing your binaries to be signing ready
- Preparing the shim review submission for your distribution
- Obtaining an EV cert for your organisation
- Registration with Microsoft hardware portal



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Distribution requirements (*Evaluation*)

- Why do you need to sign your own shim?
- Can your distribution reuse other signed binaries?
- Will you be able to support your build?
- Will you be able to provide needed security contacts?
- Do you have a legal entity for your organisation (Ex. Company or non profit)?



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Distribution requirements (*Evaluation*)

 An official website of New York State. [Here's how you know.](#)

Department of State
Division of Corporations

Entity Information

[Return to Results](#) [Return to Search](#)

Entity Details

ENTITY NAME: SOFTWARE IN THE PUBLIC INTEREST, INC.	DOS ID: 2153209
FOREIGN LEGAL NAME:	FICTITIOUS NAME:
ENTITY TYPE: DOMESTIC NOT-FOR-PROFIT CORPORATION	DURATION DATE/LATEST DATE OF DISSOLUTION:
SECTION OF LAW: 402 NCL - NOT-FOR-PROFIT CORPORATION LAW	ENTITY STATUS: ACTIVE
DATE OF INITIAL DOS FILING: 06/16/1997	REASON FOR STATUS:
EFFECTIVE DATE INITIAL FILING: 06/16/1997	INACTIVE DATE:
FOREIGN FORMATION DATE:	STATEMENT STATUS: NOT REQUIRED
COUNTY: ALBANY	NEXT STATEMENT DUE DATE:
JURISDICTION: NEW YORK, UNITED STATES	NFP CATEGORY: CHARITABLE

[<](#) **ENTITY DISPLAY** [NAME HISTORY](#) [FILING HISTORY](#) [MERGER HISTORY](#) [ASSUMED NAME HISTORY](#)

Service of Process on the Secretary of State as Agent

The Post Office address to which the Secretary of State shall mail a copy of any process against the corporation served upon the Secretary of State by personal delivery:

Name: THE CORPORATION

Address: 80 STATE STREET, ALBANY, NY, UNITED STATES, 12207 - 2543

Electronic Service of Process on the Secretary of State as agent: Not Permitted

* Debian's registered non-profit's records

LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Distribution requirements (*Preparing your binaries*)

- First step is to look at other distributions' submissions, as many as you can
 - Review Microsoft shim signing requirements [here](#)*
 - Decide on your distribution's secureboot chain binaries
 - Usually those are shim, an open source bootloader (grub2, systemd-boot), kernel / UKI, fwupd, etc..
 - Try to use the latest shim and a well known downstream bootloader and kernel such as Debian's , CentOS's
 - Make sure your source code includes the right patches for secureboot related CVEs in those binaries
 - Start designing your key management and signing solution (HSM), CA for shim, certs for signing binaries ,etc...
 - Plan a strong revocation mechanism (using SBAT and DBX)
 - Check if you have NX enabled in your boot chain
 - Make sure your builds are reproducible using containers
 - Build the production infrastructure for signing
 - Build testing plans for your secureboot chain
- Test that everything works as planned



Distribution requirements (*Preparing your binaries*)

13. SHIM submissions are exempt from obtaining an independent security audit only if your SHIM is handing off execution to an open source bootloader. In this case you must first submit to the SHIM review board and be approved before submitting to Microsoft for signing. This review board will check to ensure the following:
- Code signing keys must be backed up, stored, and recovered only by personnel in trusted roles, using at least dual-factor authorization in a physically secured environment. Additionally, keys must either be retained at the same level of security or be destroyed and rendered unrecoverable, including after expiration of the certificates.
 - The private key must be protected with a hardware cryptography module which must have a security level at least equal to FIPS 140-2 Level 2. This includes but is not limited to: HSMs, smart cards, smart card-like USB tokens, and TPMs.
 - The operating environment must achieve a level of security at least equal to FIPS 140-2 Level 2.
 - We recommend that you use an EV certificate because this will speed up UEFI CA signing turnaround.
 - Submitter must design and implement a strong revocation mechanism for everything the shim loads, directly and subsequently.
 - If you lose keys or abuse the use of a key, or if a key is leaked, any submission relying on that key will be revoked. Discovery of loss, abuse or leakage must be reported here: [MSRC Researcher Portal](#)
 - For this, we require that you use source code of 15.8 or higher from [shim - GitHub branch](#) for this SHIM.
 - For iPXE SHIM, we recommend that you use source code from this [iPXE shim](#)
14. For other usages of SHIM that do not meet the open source/public SHIM criteria, your submission must:
- Package all code that executes before ExitBootServices within a single bootloader.
 - Obtain an independent external security audit from the [OCP SAFE Program](#) before being submitted for review and signing to Microsoft.
15. If your submission contains iPXE functionality, then additional security steps are required. Previously, Microsoft has completed an in-depth security review of 2Pint's iPXE branch. For new submissions with iPXE to be signed, they must complete the following steps:
1. Pull and merge from 2Pint's commit: [iPXE - GitHub branch](#)
 2. Get a security review from a verified vendor on the [OCP SAFE Program](#). Refer vendor to the [iPXE Security Assurance Review](#). Emphasis of the review should be on:
 - NFS functionality is not included.
 - Non-UEFI loaders are not included
 - Ensuring all known reported security problems are fixed (identified in the [iPXE Security Assurance Review](#)).
 3. Share the specific commits that are made to the project, allowing Microsoft to ensure the expected changes are made

LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

<https://techcommunity.microsoft.com/blog/hardware-dev-center/updated-microsoft-uefi-signing-requirements/1062916>



Distribution requirements (*Preparing your binaries*)

```
# objcopy --dump-section .sbat=/dev/stdout shimx64.efi
sbat,1,SBAT Version,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
shim,4,UEFI shim,shim,1,https://github.com/rhboot/shim
shim.rocky,3,Rocky Linux,shim,16.1,security@rockylinux.org
```

=====

```
# objcopy --dump-section .sbat=/dev/stdout grubx64.efi
sbat,1,SBAT Version,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
grub,5,Free Software Foundation,grub,2.06,https://www.gnu.org/software/grub/
grub.rh,2,Red Hat,grub2,2.06-126.el9_8,mailto:secalert@redhat.com
grub.rocky,2,Rocky Linux,grub2,2.06-126.el9_8.rocky.0.3,mailto:security@rockylinux.org
```



LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Distribution requirements (*Preparing your binaries*)

```
# objcopy --dump-section .sbatilevel=/dev/stdout shimx64.efi
7sbat,1,2023012900
shim,2
grub,3
grub.debian,4
sbat,1,2025051000
shim,4
grub,5
grub.proxmox,2
```



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Distribution requirements (*shim review submission*)

- Assign two security contacts
- Clone the github repo <https://github.com/rhboot/shim-review/> and follow the instructions (Fill in the questionnaire, upload your shim, upload your build logs, docker file, add certificates, GPG keys for security contacts, commit and then tag it *myorg-shim-arch-YYYYMMDD*)
- Create an issue under <https://github.com/rhboot/shim-review/issues/> for review
- While waiting, help the community by reviewing other distributions' submissions (It's a community peer review process after all!)



Microsoft registration process (*EV cert & reg.*)

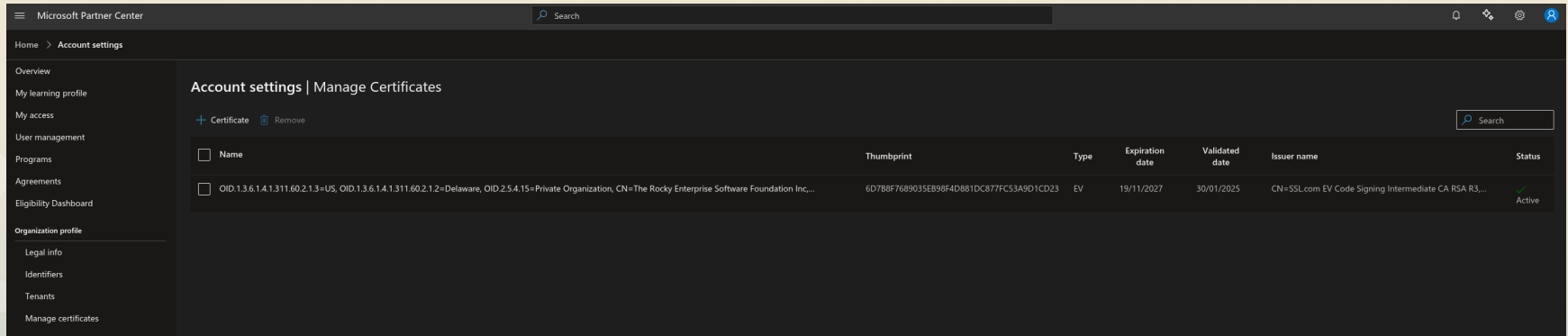
- Get an EV cert for your organisation
- Register an account at <https://partner.microsoft.com/> which will require some Azure registration as well and join the Windows Hardware Developer Program
- While uploading the EV cert, you will be asked to sign a test file to verify the EV certificate
- Once this is done, make sure you have access to File Signing Service

With your first submission, you will get a questionnaire from Microsoft, answer it and return it back to them

- Microsoft will use the EV cert to verify the organisation alongside the information you provided
- You will have to submit some legal documents and assign legal contact and developer contact personnel
- Microsoft uses 3rd party companies to conduct identity verification
- Once all is done, the contact and the organisation should be verified and you are good to go



Microsoft registration process (*EV cert & reg.*)



Microsoft Partner Center

Home > Account settings

Account settings | Manage Certificates

+ Certificate Remove

Name	Thumbprint	Type	Expiration date	Validated date	Issuer name	Status
OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.2.5.4.15=Private Organization, CN=The Rocky Enterprise Software Foundation Inc...	6D7B8F7689035EB98F4D881DC87FC3A9D1CD23	EV	19/11/2027	30/01/2025	CN=SSL.com EV Code Signing Intermediate CA RSA R3,...	Active



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Community review pipeline (*Shim review process*)

- A reviewer will set labels on the issue (new vendor, aarch64, contact verification needed, etc..)
- If contact verification needed, this gets done
 - Security contacts will get signed and encrypted email from one of the accredited reviewers
 - Security contacts will need to post the strings into the issue's comment section
- Reviewers will start looking into the submission and try to answer some questions:
 - Which bootloader, modules and kernel versions being used and which CVEs patches they include?
 - Is the SBAT correct for all the binaries? Which revocation policy being applied?
 - Is shim reproducible and generate same HASH?
 - Are the build logs uploaded and make sense or not?
 - Is the CA included in the shim valid? Was it used on signing vulnerable binaries?
 - Is NX enabled?
 - What is the revocation story? Is it sane? Are older vulnerable binaries being added to the dbx?
 - Is the key management sane and using HSM? And are kernel modules built with ephemeral keys?
- If all good, the submission gets marked as accepted, now you may submit it to Microsoft for signing



LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

<https://github.com/rhboot/shim-review/issues/561>



Microsoft submission & final review (*Submission*)

(You may want to wait until the github shim review is done before preparing the CAB file)

- Preparing the shim to be signed by Microsoft
 - You need to put all the binaries in a single CAB file, you may use *gcab* for example
 - Sign that CAB file with your EV Cert
- You can use Windows machine for this or *osslsigncode*

```
osslsigncode sign -pkcs11engine /usr/lib64/engines-3/pkcs11.so -pkcs11module /usr/lib64/libykcs11.so.2.7.3 -key  
"pkcs11:id=%01;type=private" -certs ~/resf.crt -h sha256 -ts http://ts.ssl.com -in ~/rockylinux-10-shim-16.1-  
x86_64-aarch64-20260308.cab rockylinux-10-shim-16.1-x86_64-aarch64-20260308.cab
```

- Submit via Microsoft partner website under file signing service



LINUX
PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Microsoft submission & final review (*Submission*)

Microsoft Partner Center

Home > Hardware > File Signing Services

Drivers

Device metadata

File Signing Services

Submit New UEFI Submit New LSA

Search submissions for

ID	Product Name	Type	Submitted	Status
14604256611709613	rockylinux-8-shim-16.1-ia32-x86_64-aarch64-20260604	UEFI	6/5/2026	Completed
1392786321224212	rockylinux-9-shim-16.1-x86_64-aarch64-NX-20260529	UEFI	6/4/2026	Completed
14159419755865550	rockylinux-10-shim-16.1-x86_64-aarch64-NX-20260529	UEFI	6/4/2026	Completed
14036958718340821	rockylinux-10-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Completed
14456406556260321	rockylinux-9-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Completed
13621414004407027	rockylinux-9-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Preparation
13878700104882372	rockylinux-9-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Preparation
1392626046353671	rockylinux-10-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Preparation
13728041943988872	rockylinux-10-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Preparation
14237334315666286	rockylinux-9-shim-16.1-x86_64-aarch64-20260308	UEFI	5/19/2026	Preparation
14245975913590158	rockylinux-8-shim-15.8-ia32-x86_64-aarch64-20240214	UEFI	3/6/2024	Completed
13758662584372243	rockylinux-9-shim-15.8-x86_64-aarch64-20240214	UEFI	3/1/2024	Completed
13754584092826982	rockylinux-8-shim-15.8-ia32-x86_64-aarch64-20240214	UEFI	3/1/2024	Scanning
14460228699919626	rocky-8-shim-15.6-20220817	UEFI	8/17/2022	Completed
14607686334015979	rocky-9-shim-15.6-20220816	UEFI	8/17/2022	Completed
13765341761864248	Rockylinux-8-shim	UEFI	10/27/2021	Completed

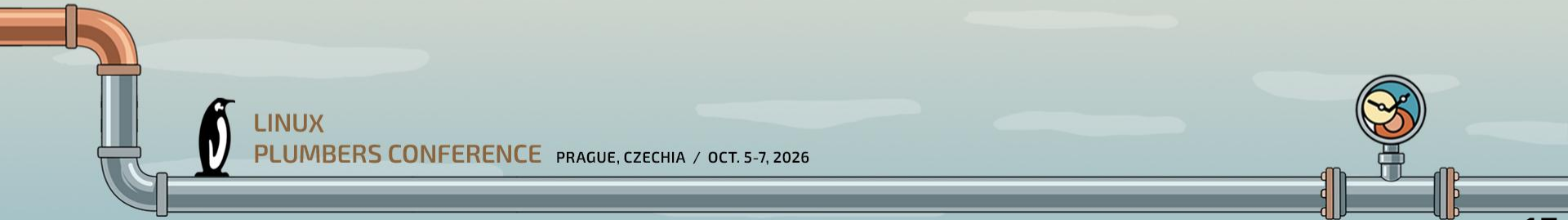


LINUX
PLUMBERS CONFERENCE PRAGUE, CZECHIA / OCT. 5-7, 2026



Microsoft submission & final review (*Review*)

Community shim review is valuable because it gives Microsoft a transparent, expert review of the open-source Linux Secure Boot chain. But that review can only stand in for additional security review when the code and trust chain actually fall within what the community was able to assess.



Microsoft submission & final review (*Review*)

- Microsoft reviews the github issue submission and verified the organisation that made the request
- After the upstream shim gate is satisfied, the submission remains subject to Microsoft's broader UEFI signing requirements. Those requirements include things such as:
 - The submission must be *production-quality code* intended for release.
 - Code with *known security vulnerabilities* is not eligible for signing
 - Microsoft's requirements govern licensing of code receiving the Microsoft signature; Microsoft's documentation specifically identifies GPLv3 code such as GRUB 2 as not directly eligible for Microsoft UEFI signing.
- Microsoft's broader current program requires independent security audits, with a defined exception for qualifying shim submissions that have gone through the shim review process.
- Once Microsoft's review team is satisfied, you get your shim signed!



Microsoft submission & final review (*Review*)

Microsoft Partner Center

Home > Hardware > File Signing Services > rockylinux-8-shim-16.1-ia32-x86_64-aarch64-20260604

Drivers

Device metadata

File Signing Services

IoT

Device model hierarchy

Analyze

Partner analytics

Driver flight status

Driver install and health summary

rockylinux-8-shim-16.1-ia32-x86_64-aarch64-20260604

Package Acceptance Preparation Scanning Validation Review Signing Finalize

Submission Details

Submission ID	14604256611709613
File Name	rockylinux-8-shim-16.1-ia32-x86_64-aarch64-20260604.cab
Created Date	6/5/2026
Company	RESF
Created By	Sherif Nagy

Download Signed Package



LINUX
PLUMBERS CONFERENCE PRAGUE, CZECHIA / OCT. 5-7, 2026



Timeline & common pitfalls

- shim review timeline varies and depends on many things:
 - Is your submission straight forward (no in-house patches, downstream grub2 and kernel)
 - We are volunteers, but we try to finish reviews fast and mostly in FIFO basis
 - Microsoft process has no SLA, it could take couple of days, or a couple of weeks
 - In cases of emergencies such as the 2023 UEFI CA swap, reviews completed in days
- If you are signing multiple architecture such as x86_64 and aarch64, please use single submission
- Make sure your Microsoft account is active, you accepted all agreements and everything is verified
- Use static build repos or shim specific container for shim reproducibility builds
- You can obtain the EV cert in parallel while registering with Microsoft portal and getting your shim reviewed by the community
- If you are using a closed source bootloader, you won't go through the shim process, but you will need to get external audit for the code as per Microsoft requirements
- Use FIPS 140-2 Level 2 HSMs
- Don't be afraid to ask questions



LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Timeline & common pitfalls

Microsoft Partner Center

Home > Hardware > File Signing Services > rockylinux-8-shim-15.8-ia32-x86_64-20240214

Drivers

Device metadata

File Signing Services

IoT

Device model hierarchy

Analyze

Partner analytics

Driver flight status

Driver install and health summary

rockylinux-8-shim-15.8-ia32-x86_64-20240214

Package Acceptance Preparation Scanning Validation Review Signing Finalize

You can download your full error report [here](#) for more information about what went wrong and how to fix the issue.

Submission Details

Submission ID	13754584092826982
File Name	rockylinux-8-shim-15.8-ia32-x86_64-aarch64-20240214.cab
Created Date	3/1/2024
Company	RESF
Created By	Sherif Nagy



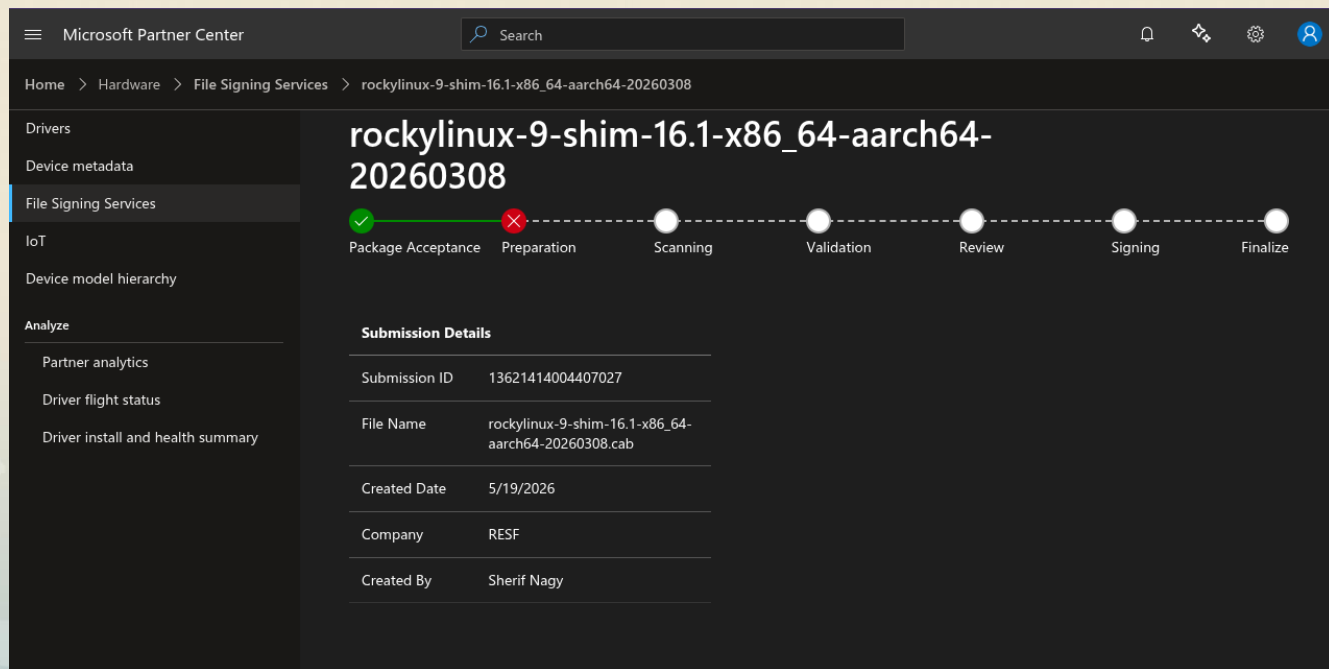
LINUX

PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Timeline & common pitfalls



The screenshot shows the Microsoft Partner Center interface for File Signing Services. The breadcrumb trail is: Home > Hardware > File Signing Services > rockylinux-9-shim-16.1-x86_64-aarch64-20260308. The left sidebar lists navigation options: Drivers, Device metadata, File Signing Services (selected), IoT, Device model hierarchy, and Analyze (with sub-items: Partner analytics, Driver flight status, and Driver install and health summary). The main content area displays the submission name 'rockylinux-9-shim-16.1-x86_64-aarch64-20260308' and a progress timeline with seven steps: Package Acceptance (green checkmark), Preparation (red X), Scanning (white circle), Validation (white circle), Review (white circle), Signing (white circle), and Finalize (white circle). Below the timeline is a 'Submission Details' table.

Submission Details	
Submission ID	13621414004407027
File Name	rockylinux-9-shim-16.1-x86_64-aarch64-20260308.cab
Created Date	5/19/2026
Company	RESF
Created By	Sherif Nagy



LINUX
PLUMBERS CONFERENCE

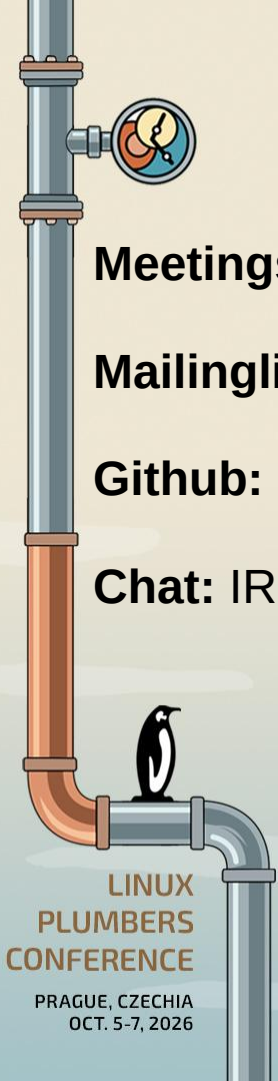
PRAGUE, CZECHIA / OCT. 5-7, 2026



Process improvements discussion + Q&A

Any thoughts, ideas and suggestions?





Meetings: Mondays 15:00 UTC / GMT @ <https://pexipdemo.com/steve.mcintyre>

Mailinglist: <https://lists.freedesktop.org/mailman/listinfo/shim-review>

Github: <https://github.com/rhboot/shim-review>

Chat: IRC @ OFTC #shim-reviews

Thank You!

