So Many Crypto Libraries…
One FIPS 140-3 Certified Implementation!

Anthony Hu @ OpenSSL Conference

Quick Speaker Introduction

Anthony Hu
anthony@wolfssl.com
Senior Software Developer
Waterloo, Ontario, Canada
Member of the wolfSSL team for 4 years

For a copy of these slides, send an email to
facts@wolfssl.com

Agenda

- wolfCrypt FIPS 140-3 Level 1
  - Post-Quantum
- Target Distros
- Implementation Stories and Target Applications
  - OpenSSL
  - NSS
  - libGCrypt and gnuTLS
  - Linux Kernel
- IGEL Case Study
- Q&A

FIPS

FIPS 140-3: Available NOW

- NIST FIPS 140-3 Certificate #4718
  - https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4718
  - World's first SP800-140Br1 FIPS 140-3 Certificate
  - Sunsets in 2029
- NIST FIPS 140-3 Certificate #5041
  - https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5041
  - Sunsets in 2030

FIPS 140-3: Coming Soon

- Module Including SRTP-KDF, AES-XTS -CFB -KW, EDDSA, SHAKE and PBKDF2
  - https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List
  - SP800-140Br1 (Web-Cryptik) accelerated processing
- The Post-Quantum Module Including ML-KEM, ML-DSA, LMS (verification only) and XMSS (verification only)
  - Work in Progress

FIPS 140-3 Licensing Models

- Evergreen model is a annual automatic and easy subscription model to FIPS 140-3
- Laddered approach means always having a more recent FIPS 140-3 certificate available as your current one is sunsetting

FIPS 140-3

Webinar: Latest FIPS 140-3 developments at wolfSSL
https://www.youtube.com/watch?v=a-4FterEUek

Speaking of Post Quantum…

- Algorithm Implementations
  - ML-KEM (512, 768, 1024)
  - ML-DSA (44, 65, 87)
  - LMS/HSS
  - XMSS/XMSS^MT
- In TLS 1.3, pure ML-KEM as well as hybrid groups:
  - ECC NIST curves
  - X22519
  - X448
- Authentication hybrids via Chimera Certificates and X9.146 extensions in the the TLS 1.3 handshake
- SLH-DSA and FN-DSA are on the roadmap

PQC Integrations

- wolfSSH hybrid KEX leveraging wolfCrypt implementations
  - interoperability with AWS Transfer Family
- wolfMQTT leverages post-quantum TLS 1.3 from wolfSSL
- cURL
- Web Servers: APACHE-httpd, nginx, lighttpd
- stunnel
- Demos
  - Winbond LMS
  - STM32 post-quantum TLS 1.3 over UART
  - NXP FRDM-MCXN947 Post-Quantum TLS 1.3
  - NXP i.MX93 EdgeLock Enclave integration (soon)

Target Distros

What Distros Almost Have FIPS 140-3?

- Linux Distros with FIPS In-Process
  - Rocky Linux (perhaps available late 2026)

What Distros Already Have FIPS 140-3 Certificates?

	RHEL 9	Ubuntu 20.04	Suse Linux Enterprise	Oracle Linux 9	Alma Linux 9	wolfCrypt Full Linux FIPS
Kernel	#5034 Exp. 2030	#4894 Exp. 2026	#4727 Exp. 2026	#5036 Exp. 2030	#4750 Exp. 2026	**#5041 Exp. 2030**
NSS	#5022 Exp. 2030		#4728 Exp. 2026	#4801 Exp. 2026	#5031 Exp. 2030	**#5041 Exp. 2030**
OpenSSL Provider	#4857 Exp. 2026			#4779 Exp. 2026	#4823 Exp. 2026	**#5041 Exp. 2030**
gnuTLS	#4846 Exp. 2026	#4855 Exp. 2026	#4742 Exp. 2026	#5037 Exp. 2030		**#5041 Exp. 2030**
libgcrypt	#4754 Exp. 2026	#4793 Exp. 2026	#4722 Exp. 2026	#4993 Exp. 2030		**#5041 Exp. 2030**
StrongSWAN		#4911 Exp. 2026				**#5041 Exp. 2030**
OpenSSL		#4794 Exp. 2026	#4725 Exp. 2026			

What About wolfSSL Full Linux FIPS?

	wolfCrypt Full Linux FIPS
Kernel	#5041 Exp. 2030
NSS	#5041 Exp. 2030
OpenSSL1 via wolfEngine	#5041 Exp. 2030
OpenSSL3 via wolfProvider	#5041 Exp. 2030
gnuTLS	#5041 Exp. 2030
libgcrypt	#5041 Exp. 2030
StrongSwan	#5041 Exp. 2030

What Distros Already Have FIPS 140-3 Certificates?

- Limited FIPS options force expensive choices
  - **1 server** (1-2 sockets) with **unlimited VMs** + **Premium support (24x7)**

$4,398.90 / year [link]

$3,400 / year [link]

$3,980 / year [link]

$2,499 / year [link]

Cost Difference Example (Perpetual License)

Red Hat Enterprise Linux (RHEL)

20 CPUs x $4,398 = $87,960/year

5-year TCO = **$439,800**

Plus any forced migration costs = ??

wolfSSL Full Linux FIPS

Perpetual wolfCrypt FIPS license = $125,000

Annual premium support = $28,500

1 OE addition to FIPS cert = $50,000

5-year TCO = **$317,500** **(-$122,300)**

No forced migration!

This example assumes:

- 20 servers / CPUs
- 5 Years
- 1 OE
- Premium Support

What Distros Need Full FIPS 140-3 Linux via wolfCrypt?

- Yocto (OpenEmbedded)
- Arch Linux
- Fedora
- Mint
- Pop!_OS
- Debian
- Gentoo
- KALI Linux
- Alpine
- CentOS
- Devuan
- Mandriva
- Manjaro
- PCLinuxOS
- Solus
- Name your favourite distro!!

OpenSSL

OpenSSL 1.0.2: wolfEngine with wolfCrypt FIPS

Very old; no longer maintained by OpenSSL.

OpenSSL 1.1.1: wolfEngine with wolfCrypt FIPS

Old; but still used; no longer updated by OpenSSL.

3.x.y: wolfProvider with wolfCrypt FIPS

Actively developed by OpenSSL.

Picking wolfProvider or wolfEngine

```
$ openssl version


if (3.x.y) {
    you need wolfProvider
}
else {
    you need wolfEngine
}
```

But don’t worry!! This will “just work” via under the hood plumbing.

Projects Supported by Engine/Provider with wolfCrypt FIPS

apache-httpd
asio
stunnel
sudo
Python
nginx
libimobiledevice
realm
openldap
openpegasus
openresty
openssh
hitch
hostap
ipmitool
jwt-cpp
bind9
tcpdump
qt
ntp
websocket
rng-tools
rsyslog
sblim-sfcb
socat
memcached
pam-ipmi
mosquitto
msmtp
krb5
chrony
urllib3
cyrus-sasl
ffmpeg
freeradius
git
grpc
haproxy
sqlcipher
sssd
ppp
pyopenssl
net-snmp
libest
cjose
libsignal
libspdm
libssh2
libvncserver
lighttpd
mariadb

OSP Repo (Open Source Projects)

https://github.com/wolfSSL/osp

Generally, these are supported via our OpenSSL compatibility layer.

For full Linux FIPS, we will test wolfProvider and wolfEngine against these.

Clear Differentiators between OpenSSL and wolfSSL

- Sizing on Embedded Linux
- Embedded development trade offs through build time crypto-agility
- Safety critical (custom trimming for DO-178)
- Vulnerability management (36 hour average time to fix)
- Bare metal and RTOS

NSS

Network Security Services: Before

Firefox

UI Library

Rendering Library

.....

Localization

NSS

TLS

.....

CMS

(PKCS11 Interface and implementation)

AES

RSA

.....

ECC

Network Security Services: After

Firefox

UI Library

Rendering Library

.....

Localization

NSS

TLS

.....

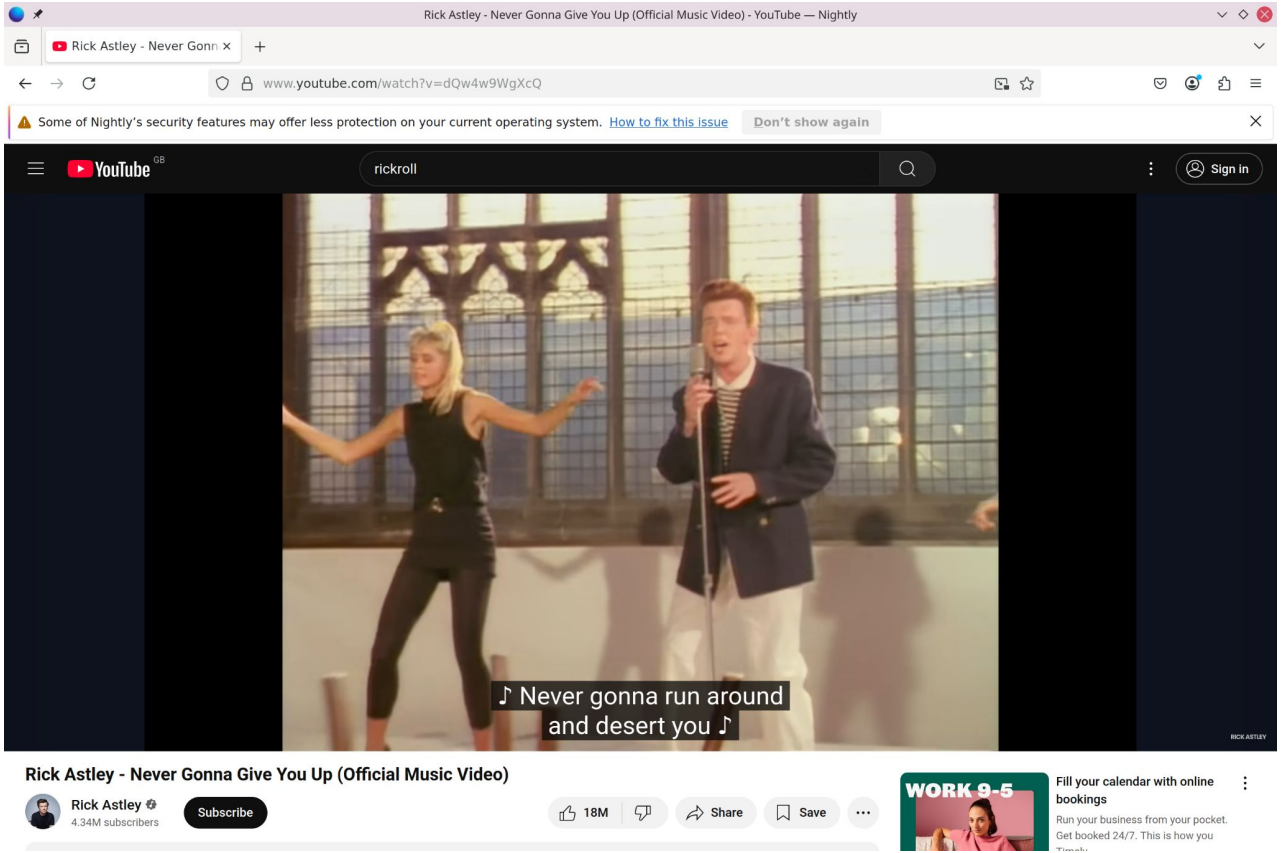
wolfPKCS11

CMS

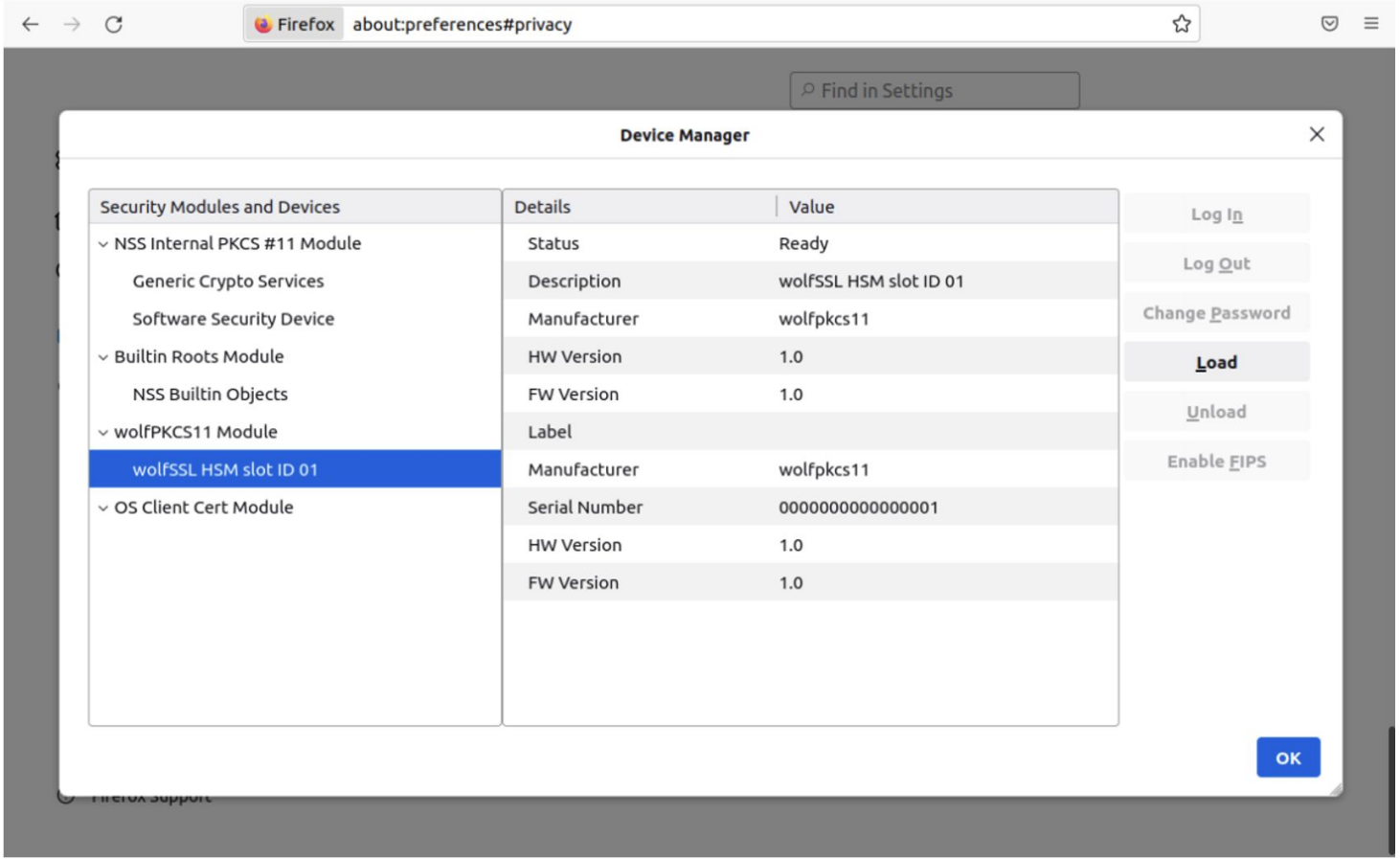
wolfSSL

wolfCrypt FIPS

NSS with wolfPKCS11 and wolfCrypt FIPS



NSS with wolfPKCS11 and wolfCrypt FIPS



Application Supported by NSS via wolfCrypt FIPS

Firefox

Thunderbird

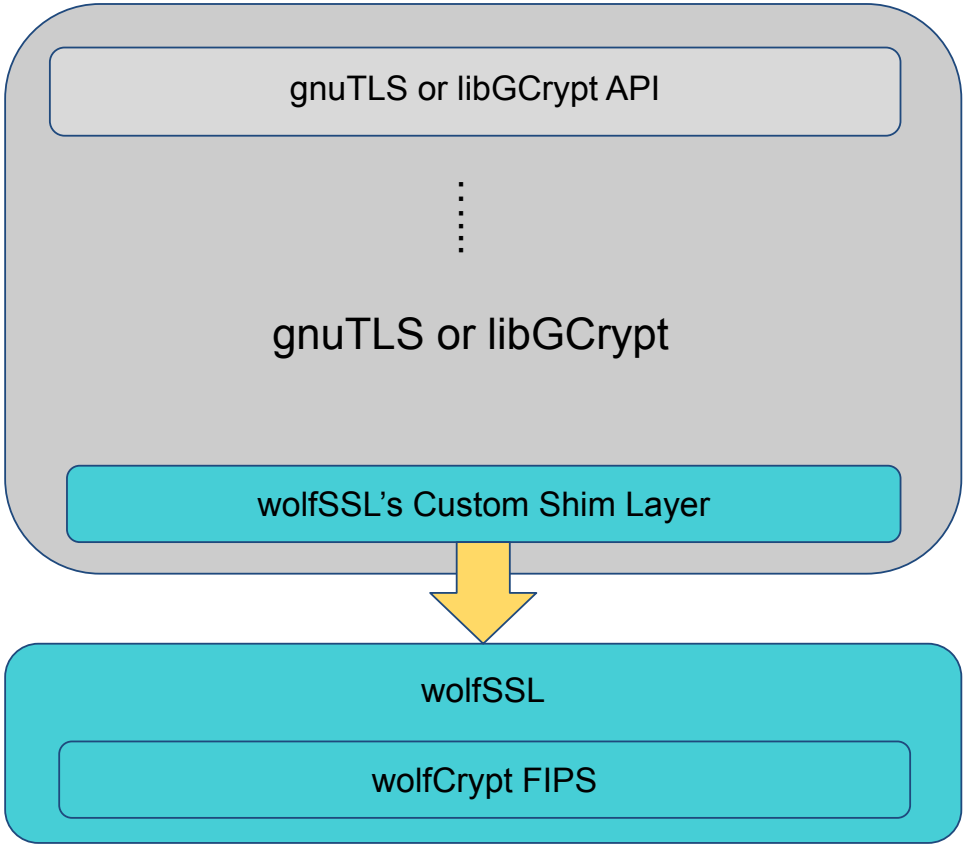
- NSS Tools
- Network-manager
- libpoppler

libGCrypt and gnuTLS

libGCrypt and gnuTLS with wolfCrypt FIPS

The approach to libGCrypt and gnuTLS is to leave as much of the upper architectural layers as intact as possible and only have a thin shim at the bottom that overrides the original cryptographic implementations and instead calls into wolfSSL/wolfCrypt FIPS.

The advantage of this approach is ease of maintenance and no need for applications that depend on libGCrypt or gnuTLS to be modified.

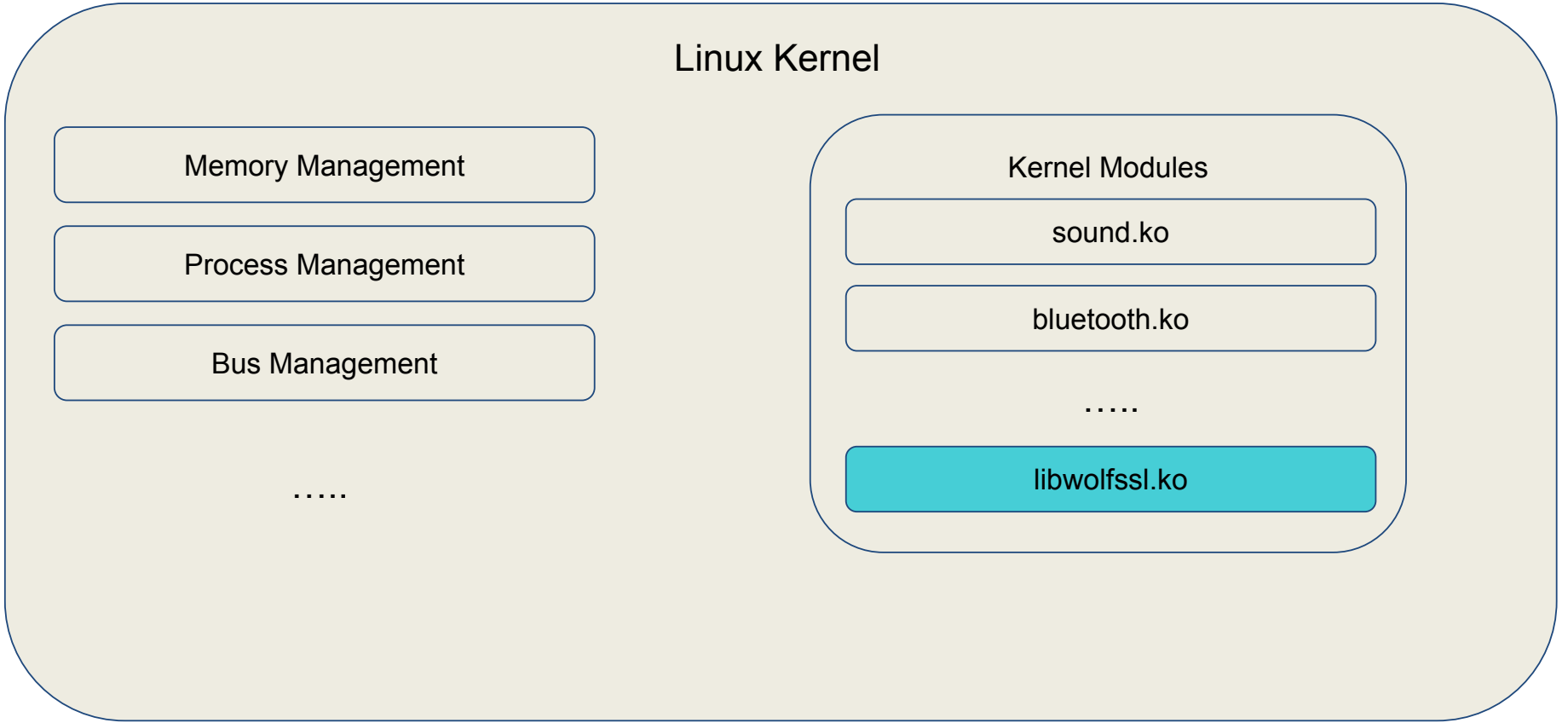


Projects Supported by libGCrypt or gnuTLS with wolfCrypt FIPS

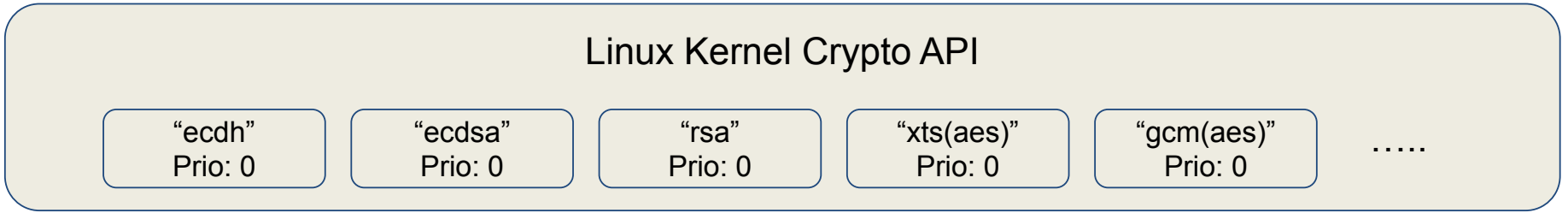
- CUPS
- nm
- Systemd
- fwupd
- libnice
- VNC
- rsyslog

Linux Kernel

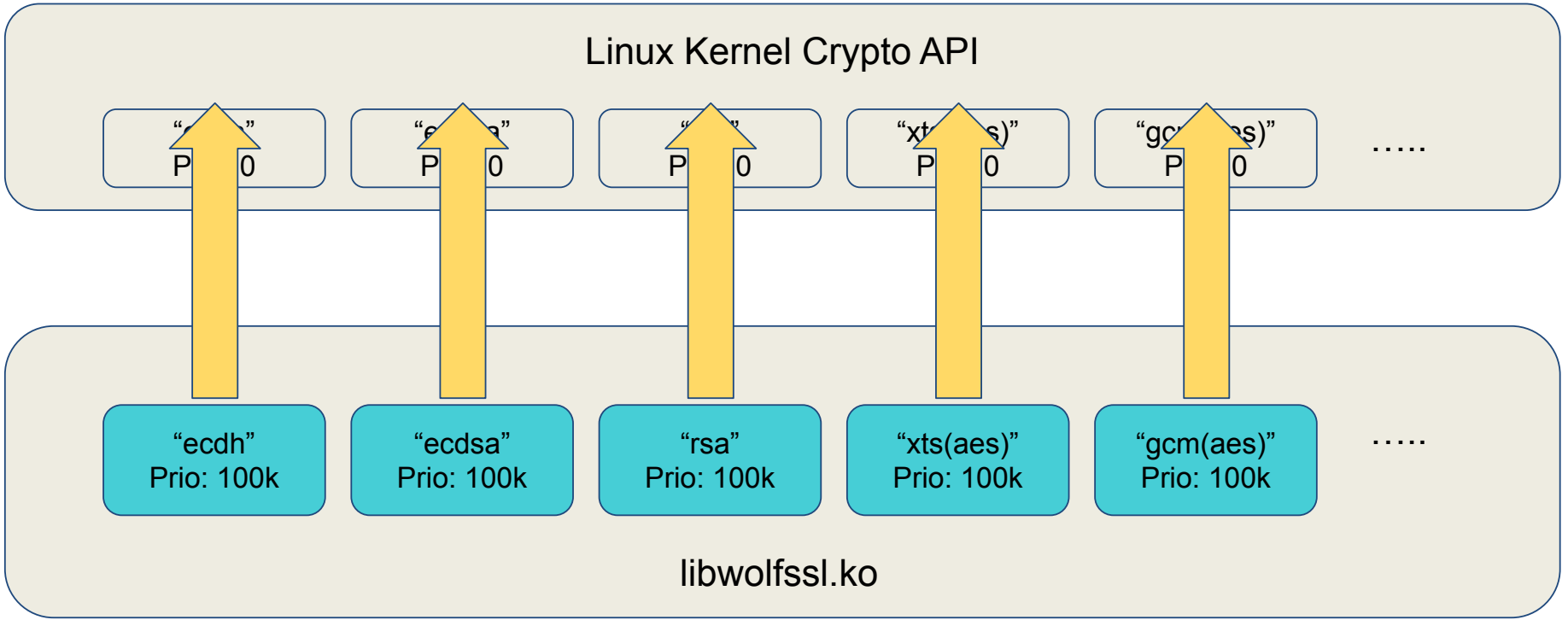
wolfCrypt FIPS as a Linux Kernel Module: What is it?



Before wolfCrypt FIPS as a Linux Kernel Module



wolfCrypt FIPS as a Linux Kernel Module



Use Cases for wolfCrypt FIPS as a Kernel Module

- Cryptographic off-load Disk Encryption
  - DM-Crypt
  - LUKS
  - fscrypt
- Cryptographic off-load for network packet flow
  - VPN
  - IPsec
  - MACsec
  - TLS offload
  - **wolfGuard**

NOTE: this is to enable kernel space cryptographic operations to serve kernel space applications. Can also be accessed by user space applications, but then much of the performance advantage disappears.

More Details

Webinar: Linux kernel Module with FIPS 140-3
https://www.youtube.com/watch?v=UY0rPAJxTIk

wolfSSL Full Linux FIPS

...one crypto library to rule them all!

Sell to US or Canadian Federal Government? You MUST be FIPS 140-3 certified. We make it simple and easy for you.

IGEL

Case Study

- IGEL is working together with wolfSSL to make this happen
- This project will be integrated into their products
- Why doesn't IGEL use existing FIPS Certified Distros?
  - Flexible Licensing Vs. Per Seat Subscription Models
  - Support (Best in Class)
  - FIPS 140-3 #4718 Until 2029 and beyond (Laddered Approach)
  - Consulting (New Library Integrations: ie BoringSSL)

Questions?

Email: facts@wolfssl.com