RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **OST-W09**

OpenSSL and FIPS... They Are Back Together!

Matt Caswell

OpenSSL - OMC/OTC/Committer

Ashit Vora

Vice President
Acumen Security
@aavora

#RSAC

Agenda

- History of OpenSSL and FIPS
- OpenSSL 3.0 Design
- OpenSSL 3.0 FIPS Module
- Current Status

History

The Story so far…

History of OpenSSL and FIPS

- OpenSSL FIPS Object Module 1.0/1.1/1.2
  - Project work: June 2002 to March 2006
  - OpenSSL release: OpenSSL-0.9.7 (last update early 2007)
  - Status: *Historical*
- OpenSSL FIPS Object Module 2.0
  - Project work: April 2009 to June 2012
  - OpenSSL release: OpenSSL-1.0.2 (end-of-life 31-Dec-2019)
  - Status: ***Sunset Date 21-Jan-2022***

History of OpenSSL and FIPS

- OpenSSL Versions
  - OpenSSL 0.9.8 – EOL 31-Dec-2015
  - OpenSSL 1.0.0 – EOL 31-Dec-2015
  - OpenSSL 1.0.1 – EOL 31-Sec-2016
  - OpenSSL 1.0.2 – EOL 31-Dec-2019 (Extended Support option)
  - OpenSSL 1.1.1 – ***EOL 11-Sep-2023***
  - OpenSSL 3.0.0 – currently in-development release

History of OpenSSL and FIPS

- OpenSSL FIPS validations always “special”
- Substantial resources invested in revalidation and porting work
- OpenSSL FIPS Object Module 2.0
  - 46 validation updates from 2012
  - 209 platforms (excluding private label validations)
- Over 250 other FIPS modules use OpenSSL

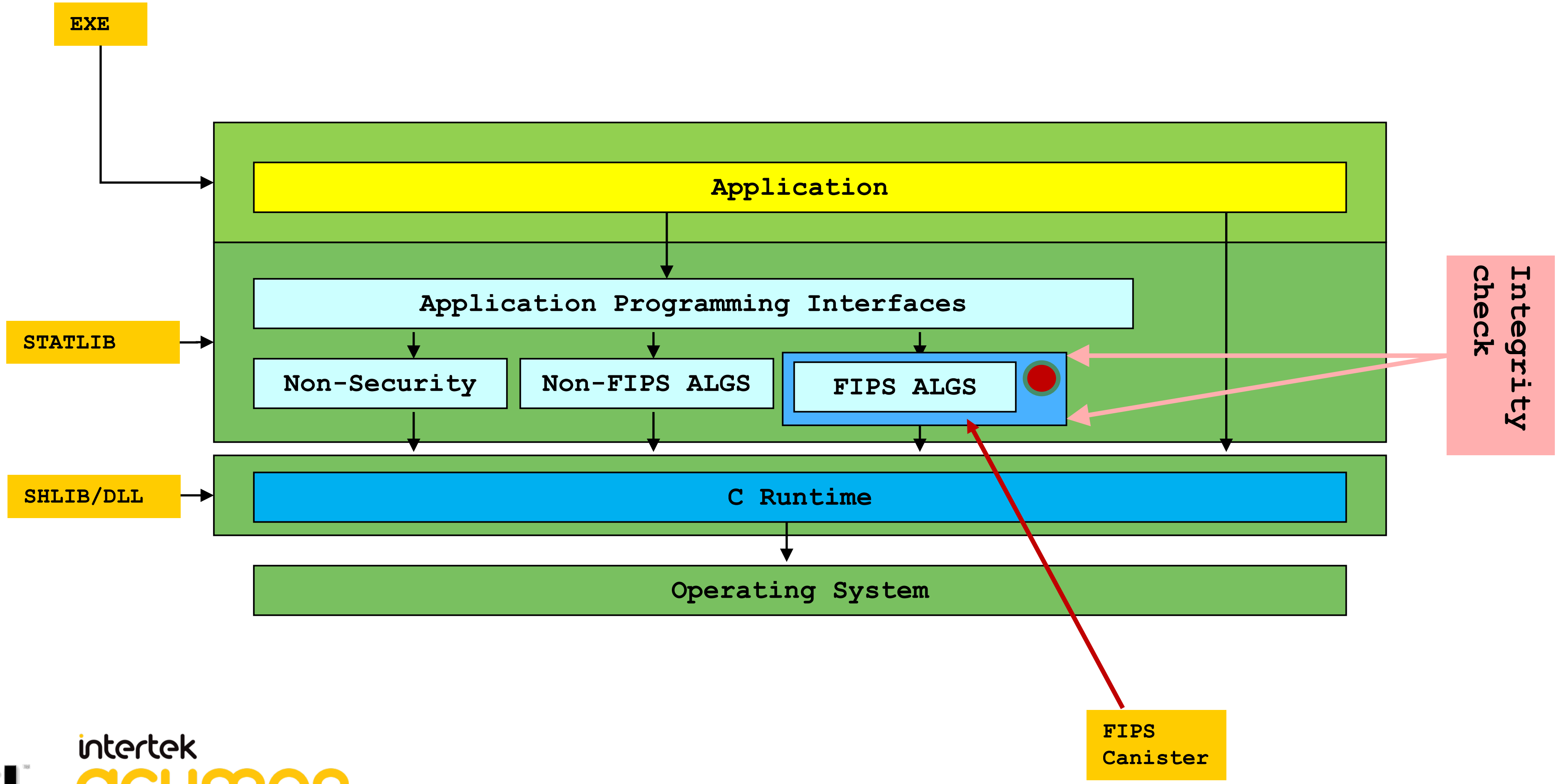
FIPS Validations to date

Cert #	Version	Validation Date	Status
642	1.0	22-Mar-2006	Historical
733	1.1	06-Feb-2007	Historical
918	1.1.2	29-Feb-2008	Historical
1051	1.2	17-Nov-2008	Historical
1111	1.2	03-Apr-2009	Historical
1747	2.0	27-Jun-2012	21-Jan-22
2398	2.0.9+	24-Jun-2015	21-Jan-22
2437	2.0.9/10	13-Nov-2015	21-Jan-22

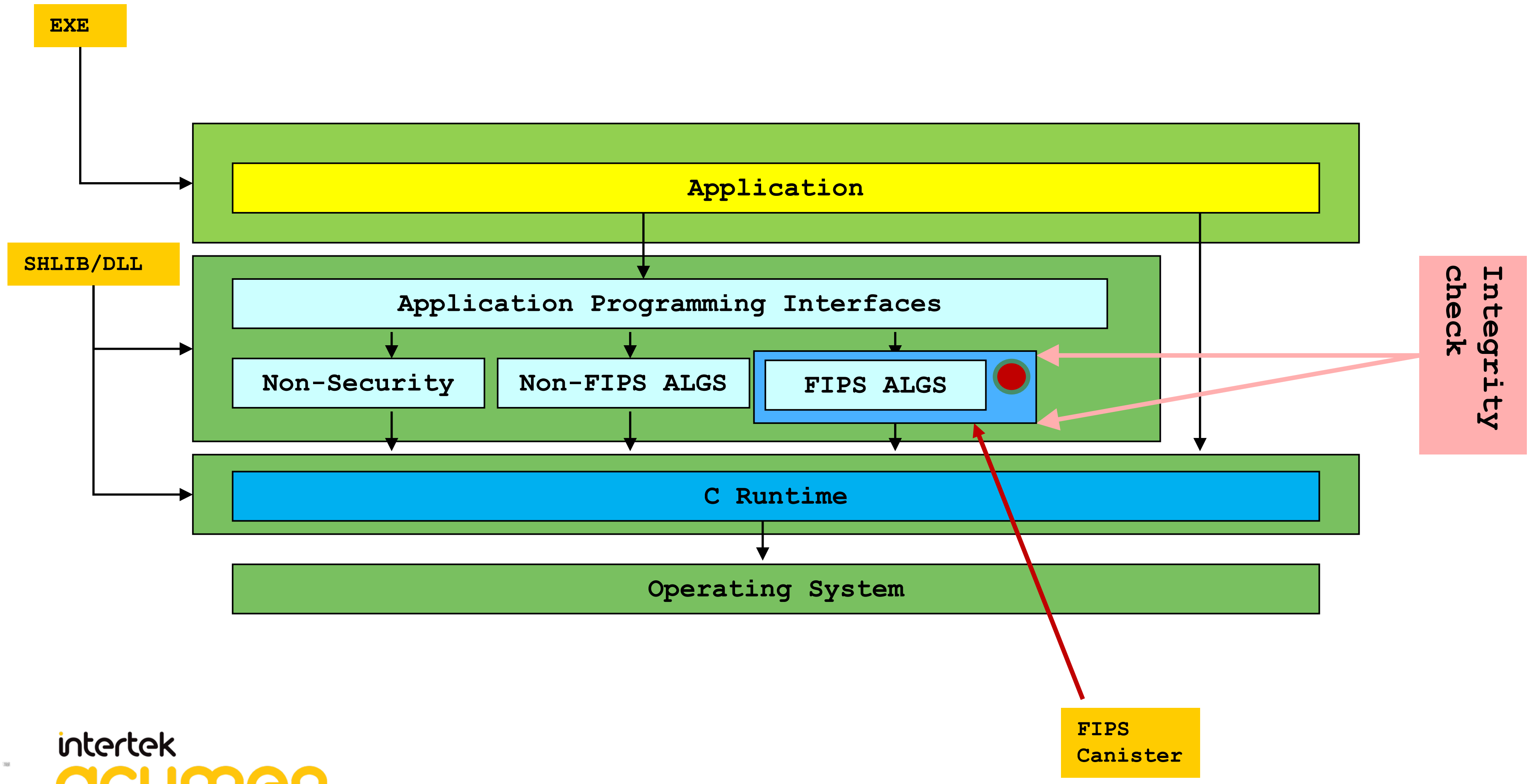
FIPS Validations to date

- Low-level FIPS approved crypto algorithms
- Source was separately maintained and versioned
- Re-certifications were ad-hoc
- Validated crypto “module” was a statically linked object
  - Either for statically linked applications; or
  - Inserted into a shared library for dynamically linked applications

FIPS140 Boundary – OpenSSL with STATLIB 2.0



FIPS140 Boundary – OpenSSL with SHLIB 2.0



FIPS Validations to date

- Common challenges
  - Code effectively forked long ago
  - Orphaned unmaintained code base
  - Too many platforms
  - Too few people involved in the coding and testing
- This was not the original plan …
- Note: over 250 other FIPS modules use OpenSSL

OpenSSL 3.0 Design

OpenSSL 1.1.1 Recap

- TLS v1.3
- New unified build system
- Data structures opaque
- Automatic cleanup
- Thread handling routines
- Changed cipher suite handling and defaults
- X25519, ChaCha20, Poly1305 support
- Cleaned up IPv6 handling
- DANE TLSA peer authentication
- Removed export (insecure) cipher suites
- ASYNC support
- SSL/TLS state machine rewrite
- Reworked “apps” command line parsing, help strings, option consistency
- OCB mode support
- Many bug fixes
- More test cases and new testing framework
- More documentation
- Obsolete/dead/unsupported code removed

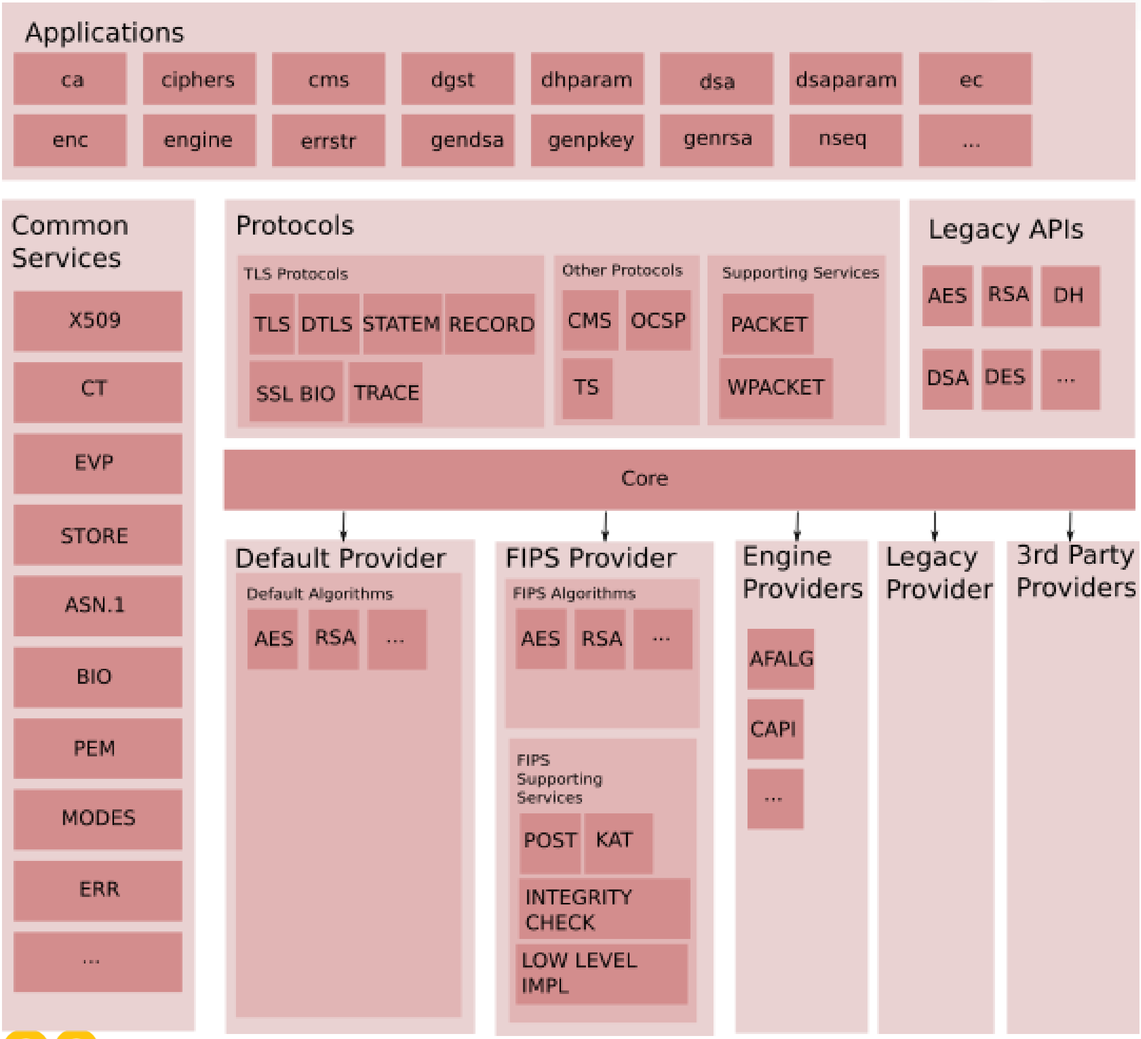
OpenSSL 3.0 Design Meeting

OMC+SPONSORS+ACUMEN MEETING IN BRISBANE, AUGUST 2018

OpenSSL 3.0 Overview

- OpenSSL 3.0 is the next version after OpenSSL 1.1.1
- Removal of unsupportable code in OpenSSL 1.1.1 provides cleaner base for future work
- Major reworking of OpenSSL internals
- Algorithm selection challenges
- Published documents on design
- Published future design objectives

OpenSSL 3.0 – Conceptual Component View



Applications
- ca, ciphers, cms, dgst, dhparam, dsa, dsaparam, ec
- enc, engine, errstr, gendsa, genpkey, genrsa, nseq, ...

Common Services
- X509
- CT
- EVP
- STORE
- ASN.1
- BIO
- PEM
- MODES
- ERR
- ...

Protocols
- TLS Protocols: TLS, DTLS, STATEM, RECORD, SSL BIO, TRACE
- Other Protocols: CMS, OCSP, TS
- Supporting Services: PACKET, WPACKET

Legacy APIs
- AES, RSA, DH, DSA, DES, ...

Core

Default Provider
- Default Algorithms: AES, RSA, ...

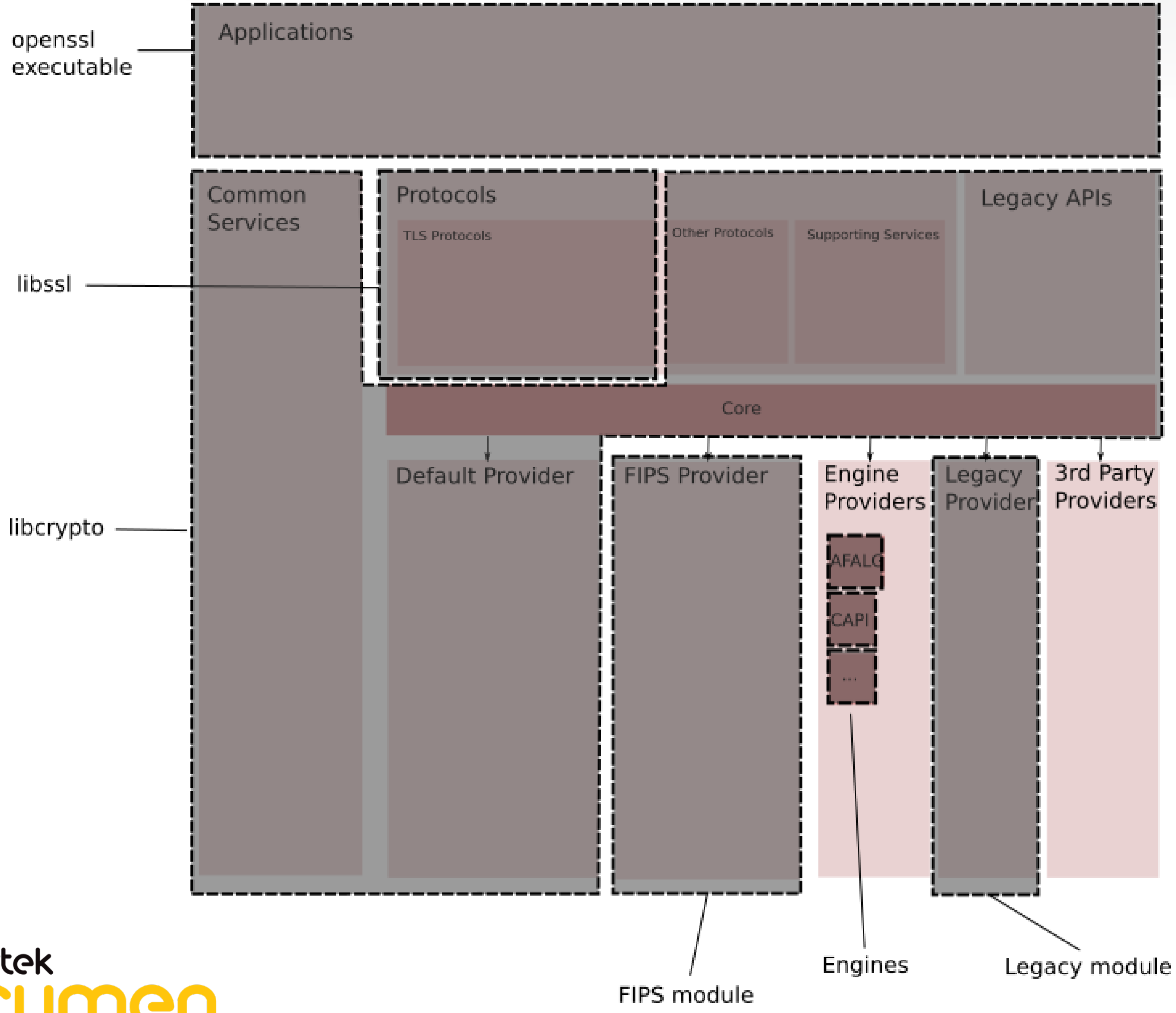
FIPS Provider
- FIPS Algorithms: AES, RSA, ...
- FIPS Supporting Services: POST, KAT, INTEGRITY CHECK, LOW LEVEL IMPL

Engine Providers
- AFALG
- CAPI
- ...

Legacy Provider

3rd Party Providers

OpenSSL 3.0 – Packaging View



OpenSSL 3.0 Design Overview

- All development is public
- Issues raised
- Pull requests
- Incremental changes of components
- Comments welcome

OpenSSL 3.0 Design Overview

- Minimal impact on majority of existing applications
- Only recompilation will be necessary for the majority of existing applications working with OpenSSL 1.1.1
- No marked deprecated API will be removed
- Many low-level functions will be marked as deprecated but remain for this release
- Packaging changes – component / provider based

OpenSSL 3.0 FIPS Design

OpenSSL FIPS Modules - Recap

Cert #	Version	Validation Date	Status
642	1.0	22-Mar-2006	Historical
733			istorical
918			istorical
1051			istorical
1111			istorical
1747			1-Jan-22
2398	2.0.9+	24-Jun-2015	21-Jan-22
2437	2.0.9/10	13-Nov-2015	21-Jan-22

None of these modules work with OpenSSL v1.1 or **OpenSSL v3.0**

History of OpenSSL and FIPS

- OpenSSL FIPS Object Module 3.0
  - Project started seeking sponsors from 2012
  - Initial planning work with potential sponsors in 2015
  - Sponsors finally confirmed mid 2018
  - Project kick off was in late 2018
  - Currently in-development release
  - Everything is public
    - www.openssl.org
    - github.com/openssl/openssl
    - https://www.openssl.org/docs/OpenSSL300Design.html

OpenSSL 3.0 and FIPS

- Sponsors
  - Akamai Technologies
  - Blue Cedar
  - NetApp
  - Oracle
  - VMware
- FIPS Validation Laboratory
  - Acumen Security
- OpenSSL Project Roadmap
  - Core feature is a FIPS module for validation

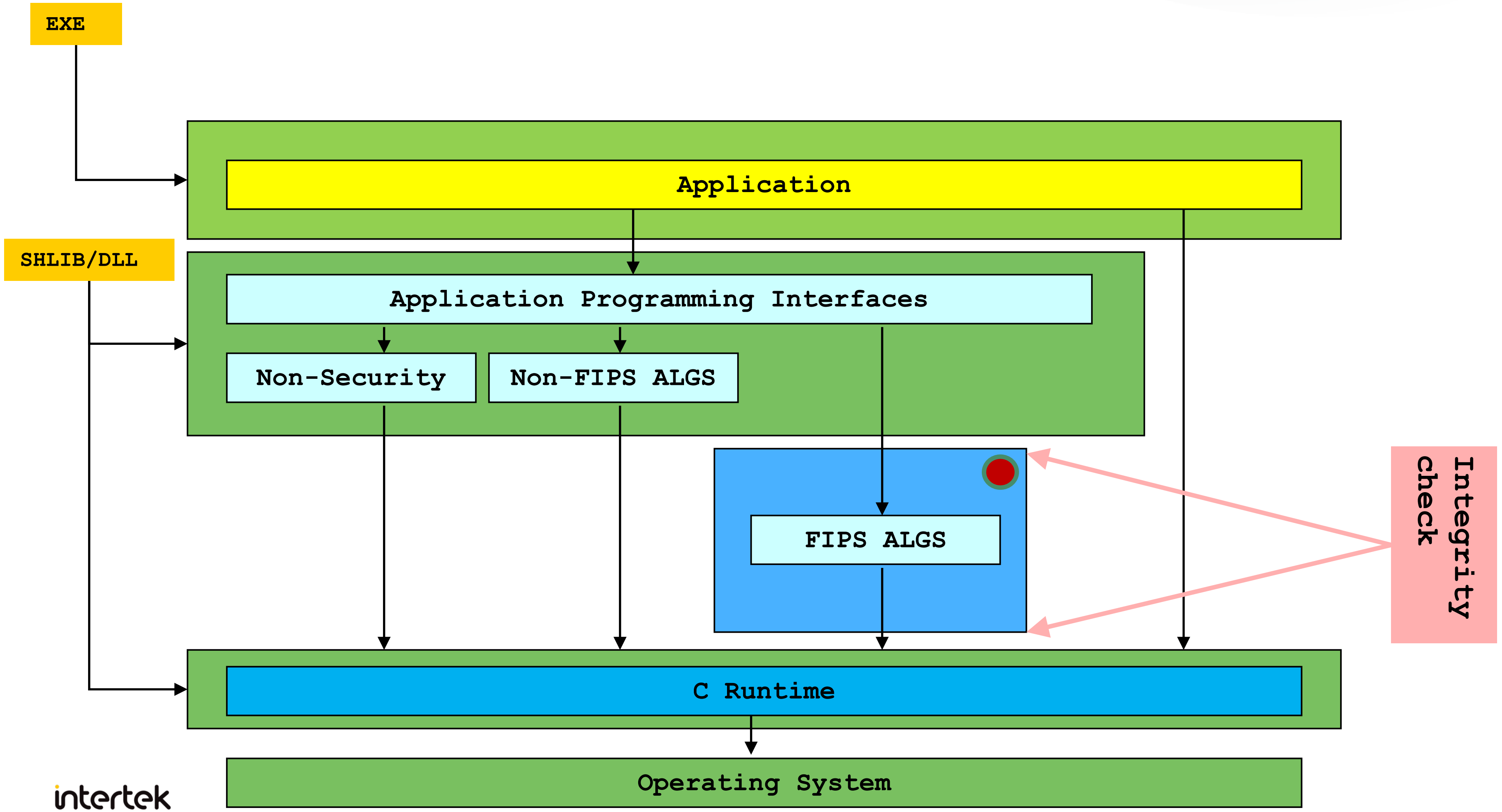
OpenSSL 3.0 and FIPS

- Goals for this validation are
  - Small set of operational environments (OEs) tested
  - Core set of algorithms
  - Enable others parties to perform their own validations
  - Maintaining validation made easier
  - Cross-release validation compatibility
- Core restructuring in 3.0 to support these goals

OpenSSL 3.0 FIPS Design – High Level

- New concept of Providers
- Validated FIPS module will be a Provider
- FIPS module is integrated into main line OpenSSL
  - No need for a separate download
  - FIPS module version aligned with main OpenSSL
- The old "fips canister" approach will not be used
- Module boundary will be a dynamically loaded Provider

FIPS140 Boundary – OpenSSL with SHLIB 3.0



OpenSSL 3.0 FIPS Design

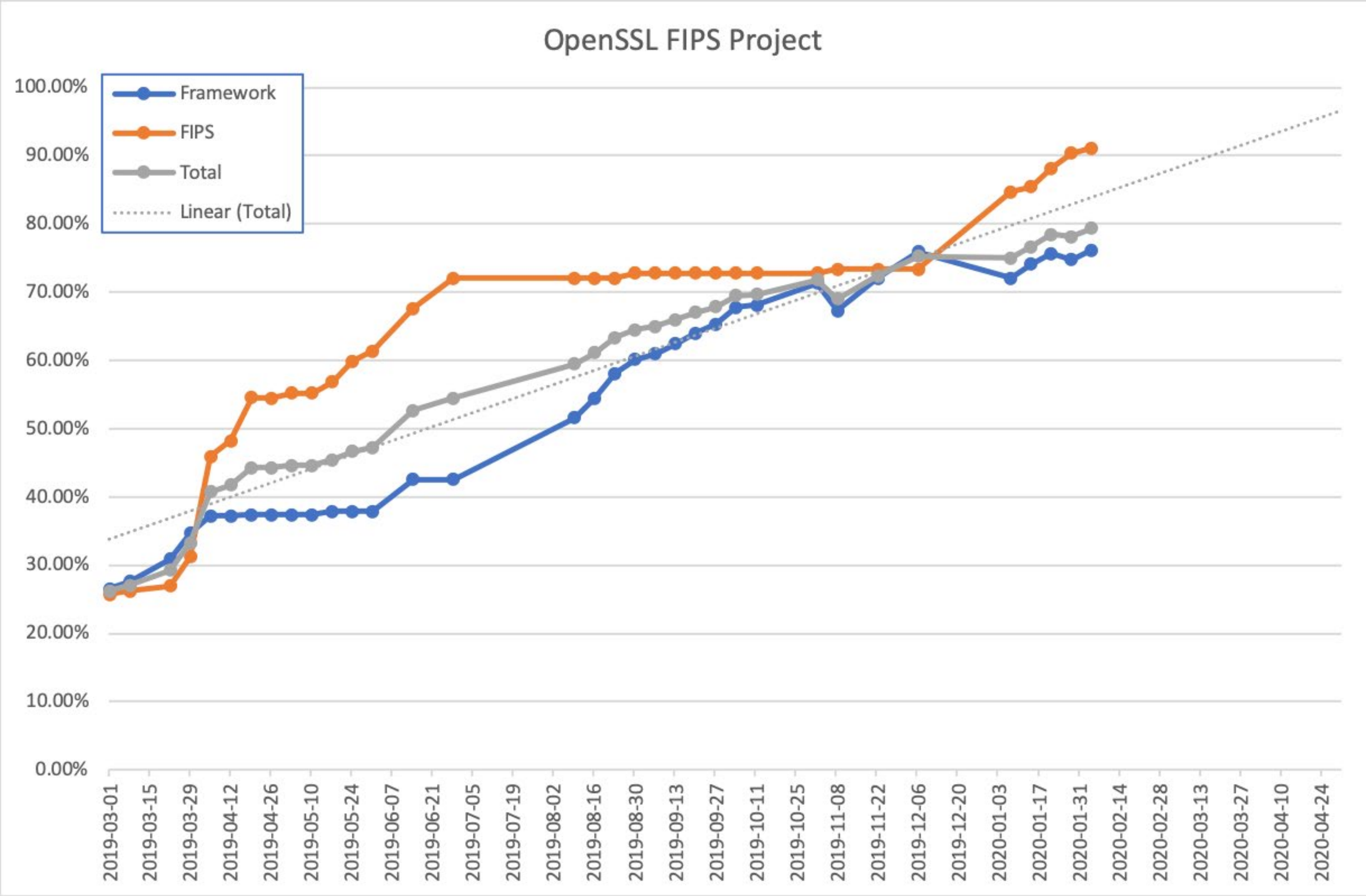
- Total of 12 OEs to be tested
  - Various Linux distributions
  - Windows, FreeBSD, Solaris
  - iOS, Android
- Typical set of crypto algorithms
- Highlights: AES KW, SHA-3, HMAC-SHA-3, SP 800-56A (DH and ECC), SP 800-132 (PBKDF2), TLS 1.2 and 1.3 PRF
- Reduction of self-tests overhead using IGs 9.1, 9.2, 9.3, 9.4 and 9.11
- Integrity test for image on disk

Current Status

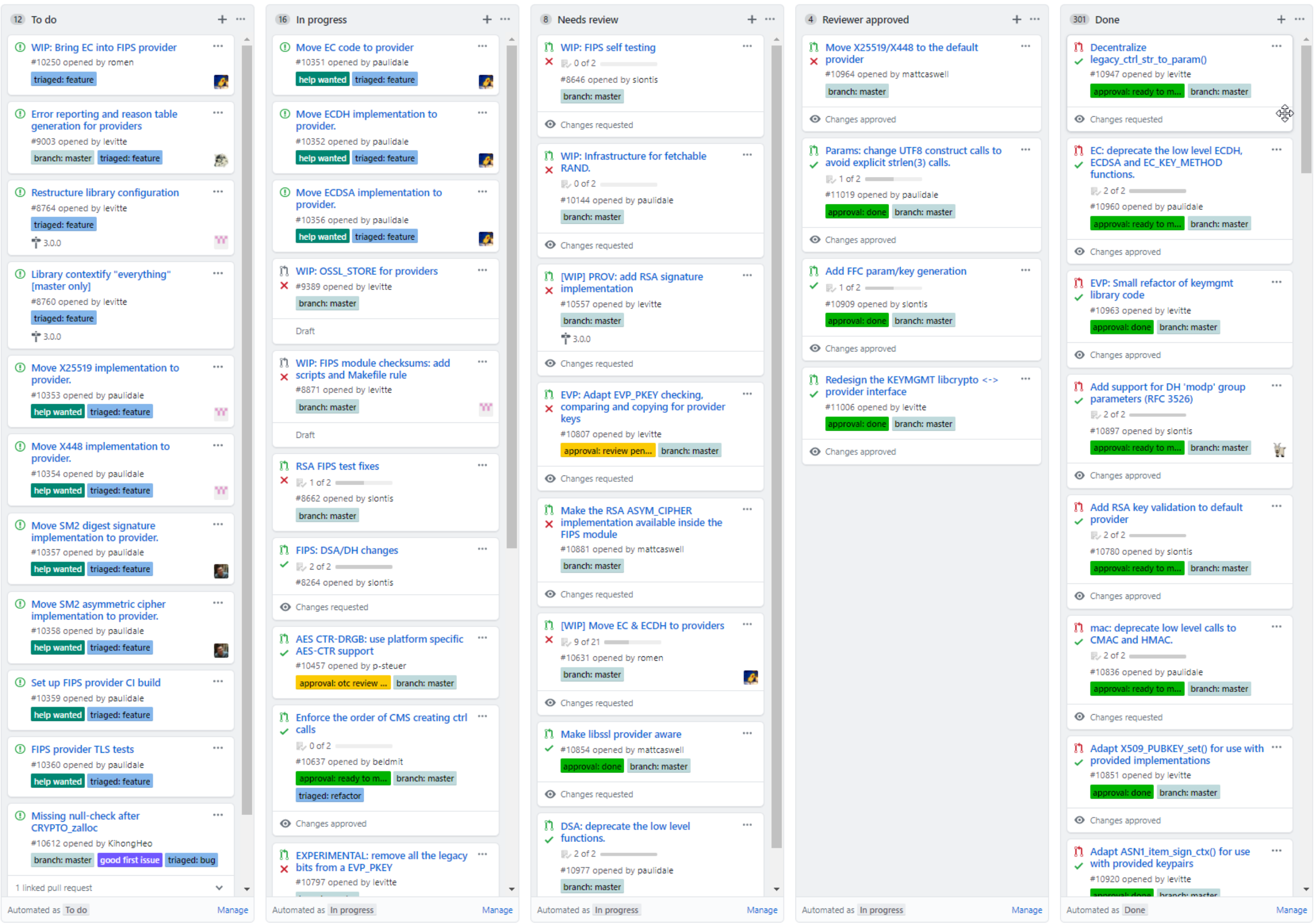
Current Status – OpenSSL 3.0 Schedule

- Alpha1, 2020-03-31: Basic functionality plus basic FIPS module
- Alpha2, 2020-04-21: Complete external provider support (serialization, support for new algs, support for providers which only include operations in a class)
- Alpha3, 2020-05-21: Aiming to test the API completeness before beta1 freezes it)
- Beta1, 2020-06-02: Code complete (API stable, feature freeze)
- BetaN: Other beta releases TBD
- Final: 2020 early Q4

Progress to date …



Latest Status



12 To do

WIP: Bring EC into FIPS provider
#10250 opened by romen
triaged: feature

Error reporting and reason table generation for providers
#9003 opened by levitte
branch: master | triaged: feature

Restructure library configuration
#8764 opened by levitte
triaged: feature
3.0.0

Library contextify "everything" [master only]
#8760 opened by levitte
triaged: feature
3.0.0

Move X25519 implementation to provider.
#10353 opened by paulidale
help wanted | triaged: feature

Move X448 implementation to provider.
#10354 opened by paulidale
help wanted | triaged: feature

Move SM2 digest signature implementation to provider.
#10357 opened by paulidale
help wanted | triaged: feature

Move SM2 asymmetric cipher implementation to provider.
#10358 opened by paulidale
help wanted | triaged: feature

Set up FIPS provider CI build
#10359 opened by paulidale
help wanted | triaged: feature

FIPS provider TLS tests
#10360 opened by paulidale
help wanted | triaged: feature

Missing null-check after CRYPTO_zalloc
#10612 opened by KihongHeo
branch: master | good first issue | triaged: bug
1 linked pull request

Automated as To do — Manage

16 In progress

Move EC code to provider
#10351 opened by paulidale
help wanted | triaged: feature

Move ECDH implementation to provider.
#10352 opened by paulidale
help wanted | triaged: feature

Move ECDSA implementation to provider.
#10356 opened by paulidale
help wanted | triaged: feature

WIP: OSSL_STORE for providers
#9389 opened by levitte
branch: master
Draft

WIP: FIPS module checksums: add scripts and Makefile rule
#8871 opened by levitte
branch: master
Draft

RSA FIPS test fixes
1 of 2
#8662 opened by slontis
branch: master

FIPS: DSA/DH changes
2 of 2
#8264 opened by slontis
Changes requested

AES CTR-DRGB: use platform specific AES-CTR support
#10457 opened by p-steuer
approval: otc review ... | branch: master

Enforce the order of CMS creating ctrl calls
0 of 2
#10637 opened by beldmit
approval: ready to m... | branch: master | triaged: refactor
Changes approved

EXPERIMENTAL: remove all the legacy bits from a EVP_PKEY
#10797 opened by levitte

Automated as In progress — Manage

8 Needs review

WIP: FIPS self testing
0 of 2
#8646 opened by slontis
branch: master
Changes requested

WIP: Infrastructure for fetchable RAND.
0 of 2
#10144 opened by paulidale
branch: master
Changes requested

[WIP] PROV: add RSA signature implementation
#10557 opened by levitte
branch: master
3.0.0
Changes requested

EVP: Adapt EVP_PKEY checking, comparing and copying for provider keys
#10807 opened by levitte
approval: review pen... | branch: master
Changes requested

Make the RSA ASYM_CIPHER implementation available inside the FIPS module
#10881 opened by mattcaswell
branch: master
Changes requested

[WIP] Move EC & ECDH to providers
9 of 21
#10631 opened by romen
branch: master
Changes requested

Make libssl provider aware
#10854 opened by mattcaswell
approval: done | branch: master
Changes requested

DSA: deprecate the low level functions.
2 of 2
#10977 opened by paulidale
branch: master

Automated as In progress — Manage

4 Reviewer approved

Move X25519/X448 to the default provider
#10964 opened by mattcaswell
branch: master
Changes approved

Params: change UTF8 construct calls to avoid explicit strlen(3) calls.
1 of 2
#11019 opened by paulidale
approval: done | branch: master
Changes approved

Add FFC param/key generation
1 of 2
#10909 opened by slontis
approval: done | branch: master
Changes approved

Redesign the KEYMGMT libcrypto <-> provider interface
#11006 opened by levitte
approval: done | branch: master
Changes approved

Automated as In progress — Manage

301 Done

Decentralize legacy_ctrl_str_to_param()
#10947 opened by levitte
approval: ready to m... | branch: master
Changes requested

EC: deprecate the low level ECDH, ECDSA and EC_KEY_METHOD functions.
2 of 2
#10960 opened by paulidale
approval: ready to m... | branch: master
Changes approved

EVP: Small refactor of keymgmt library code
#10963 opened by levitte
approval: done | branch: master
Changes approved

Add support for DH 'modp' group parameters (RFC 3526)
2 of 2
#10897 opened by slontis
approval: ready to m... | branch: master
Changes approved

Add RSA key validation to default provider
2 of 2
#10780 opened by slontis
approval: ready to m... | branch: master
Changes approved

mac: deprecate low level calls to CMAC and HMAC.
2 of 2
#10836 opened by paulidale
approval: ready to m... | branch: master
Changes requested

Adapt X509_PUBKEY_set() for use with provided implementations
#10851 opened by levitte
approval: done | branch: master
Changes approved

Adapt ASN1_item_sign_ctx() for use with provided keypairs
#10920 opened by levitte
approval: done | branch: master

Automated as Done — Manage

https://github.com/openssl/openssl/projects/2

OpenSSL Cryptography and SSL/TLS Toolkit

intertek acumen security

Latest Status

https://github.com/openssl/openssl/projects/2

- 12 – To do
- 15 – In progress
- 8 – Needs review
- 4 – Reviewer approved
- 301 – Done

Current Status - Development

- Default, Legacy and FIPS provider are present and most of the crypto algorithms have been migrated
- Tremendous work has gone into making OpenSSL 3.0 a reality, however much is to be done
- Code completion: End of Q2 2020
- Final release: End of Q4 2020

Current Status – FIPS Validation

- Acumen has stared developing the ACVP test tool
- In parallel will begin work on the operational test tool
- Goal is to have test tools ready by code complete
- Acumen is working closely with OMC in order to finish testing as close to final release as possible
- Current expectation is validation report submission code complete + 4-6 weeks
- Validation by report submission + 6 months

Post Certification - Rebranding

- Current validation is limited in OEs
- OMC is not going to be involved in rebranding/addition of OEs
- Interested parties are free to rebrand and add OEs
  - Work directly with Acumen
  - Work directly with lab of your choice

Post Certification – Certificate Maintenance

- OMC plans to keep certification current as opposed to point in time
- Re-certification will be driven based on requirements changes and/or addition of functionality
- Will try and leverage 1SUB and 3SUB re-certification scenarios

Important Links

- OpenSSL: https://www.openssl.org/
- OpenSSL Blog: https://www.openssl.org/blog/
- OpenSSL Github: https://github.com/openssl/openssl
- Acumen Security: https://www.acumensecurity.net/

Apply what you have learned today

- Next week you should:
  - Review development on Git
  - Follow OpenSSL blog for latest developments
- End of year:
  - Prepare for final release
  - Ensure your applications work with v1.1.1 and v3.0 (when available)
  - Determine what additional OEs/Rebrands will be required for your business
- Q1-Q2 2021:
  - Execute on plans for additional OEs/Rebrands