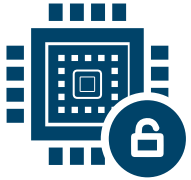
We need a Let's Encrypt movement for Confidential Computing

The importance of protecting data in use

States of Data Protection

Protection at rest
Securing data being stored by encrypting it before storing it or encrypting the device itself

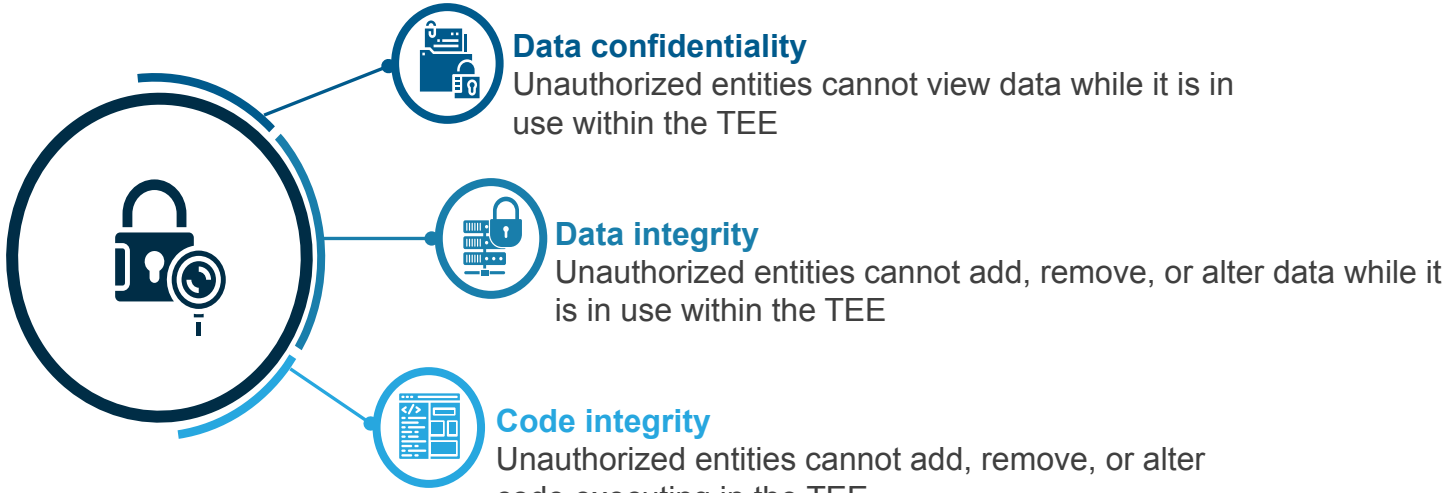
Protection in transit
Securing data transmitted between networks using end-to-end encryption or by using encrypted connections



Protection in use
Protecting data by encrypting it while it is being used in the RAM or processor for computation

CONFIDENTIAL COMPUTING CONSORTIUM

Data/Code Confidentiality/Integrity



Data confidentiality
Unauthorized entities cannot view data while it is in use within the TEE

Data integrity
Unauthorized entities cannot add, remove, or alter data while it is in use within the TEE

Code integrity
Unauthorized entities cannot add, remove, or alter code executing in the TEE

Confidential Computing

Confidential Computing protects data in use by performing computation in a hardware-based, attested Trusted Execution Environment. These secure and isolated environments prevent unauthorized access or modification of applications and data while in use, thereby increasing the security assurances for organizations that manage sensitive and regulated data.

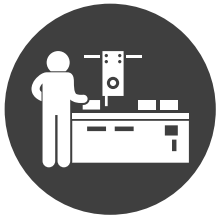
CONFIDENTIAL COMPUTING
CONSORTIUM

Applications of Confidential Computing

Banking, financial services & insurance

Healthcare & life sciences

Telecom, Edge & IoT



Manufacturing

Gov. & public sector

Retail

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing Consortium

The Confidential Computing Consortium is a community focused on projects securing data in use and accelerating the adoption of confidential computing through open collaboration.

It’s a Linux Foundation community composed by:

- Hardware vendors
- Cloud service providers
- Software developers

Members

THE LINUX FOUNDATION

Premier Members

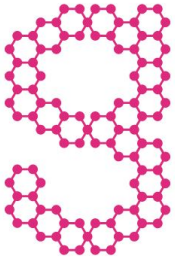
accenture
蚂蚁集团 ANT GROUP
arm
Google
HUAWEI
intel
Meta
Microsoft
Red Hat

General Members

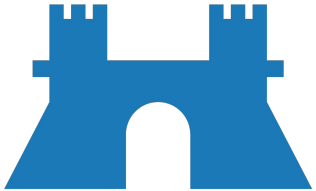
AMD
AMPERE.
anjuna
Anqlave
appliedblockchain
ByteDance
cisco
cosmian
CRUST
CYSEC
DECENTRIQ
EDGELESS SYSTEMS
ENVEIL ENCRYPTED VEIL
Ethernity CLOUD
Fortanix
iExec
MADANA
NVIDIA.
PHALA NETWORK
Profian
r3.
swisscom
vmware
Western Digital.
XILINX
CANONICAL

CONFIDENTIAL COMPUTING CONSORTIUM

Projects





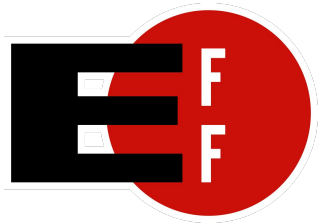

Let’s Encrypt

- The mission for the organization is to create a more secure and privacy-respecting World-Wide Web by promoting the widespread adoption of HTTPS.
- The Let's Encrypt project started in 2012 by two Mozilla employees, Josh Aas and Eric Rescorla, together with Peter Eckersley at the Electronic Frontier Foundation and J. Alex Halderman at the University of Michigan.
- World's largest certificate authority, used by more than 300 million websites
- Provides X.509 certificates for TLS encryption at no charge.

CONFIDENTIAL COMPUTING CONSORTIUM

Sponsors and Partners

- Run by Internet Security Research Group (ISRG).
- Major sponsors: Electronic Frontier Foundation (EFF), the Mozilla Foundation, OVH, Cisco Systems, Facebook, Google Chrome, Internet Society, AWS, NGINX, and Bill and Melinda Gates Foundation.
- Partners: IdenTrust, University of Michigan (U-M), and Linux Foundation.



Software & Protocol

- certbot: Python-based implementation of the client side to manage the certificate using the ACME protocol
- Boulder: Go-based implementation of the server side of the ACME protocol.
- Automatic Certificate Management Environment (ACME).

Let's Encrypt

IMPACT ON THE WEB

As of November 1, 2022, Let's Encrypt provides TLS to over 309 million domains via 239 million active certificates. Let's Encrypt usage grew by more than 33 million domains in 2022.

2022 DAILY ISSUANCE

1.8M	2.5M	3.1M
MIN	AVG	MAX

CERTS ISSUED SINCE 2015

3,078,399,255

ACTIVE CERTIFICATES

239,710,300

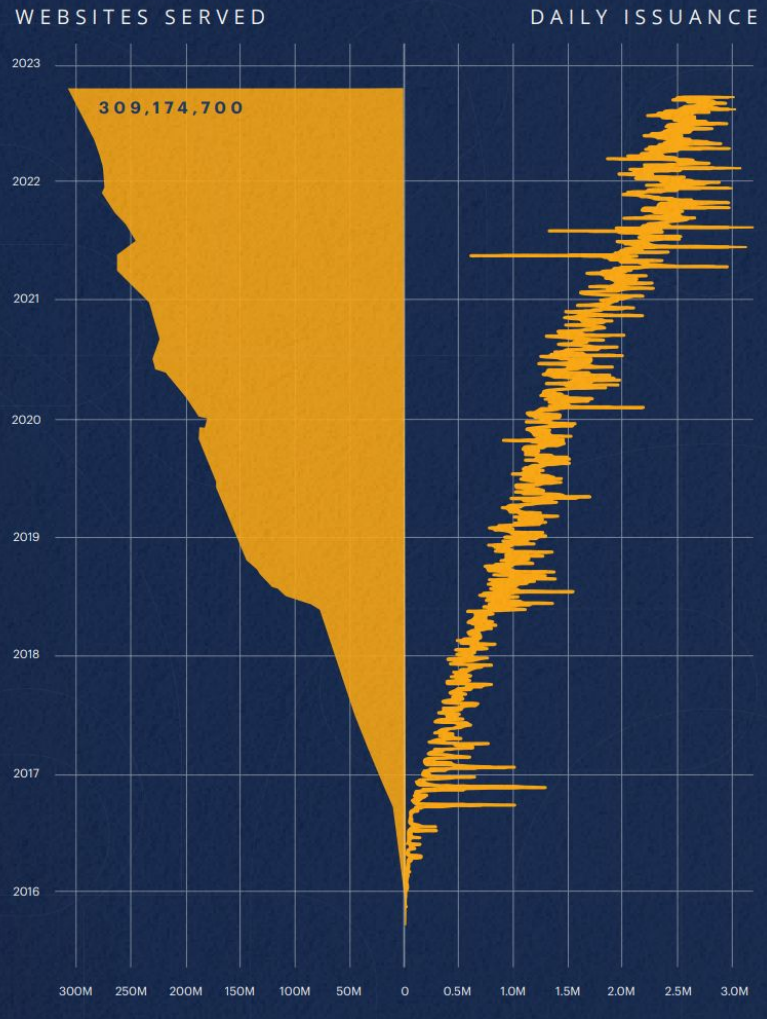
REGISTERED DOMAINS

99,496,600

82% WEB PAGES LOADED BY FIREFOX USING HTTPS, GLOBALLY

30 CERTIFICATES ISSUED PER SECOND ON AVERAGE

> "LET'S ENCRYPT IS A CRITICAL, YET FREQUENTLY UNNOTICED, PART OF THE PUBLIC COMMONS THAT KEEPS THE INTERNET SAFE AND SECURE FOR EVERYONE."
>
> NADIA ASPAROUHOVA
> AUTHOR | WORKING IN PUBLIC



What can CC learn from Let's Encrypt?

- Campaign to bring awareness around the importance of encrypting data in use, like Let's Encrypt brought for data in transit
- Adoption of TEEs by Cloud Service Providers
- Develop software that makes it really easy to deploy Confidential Computing
- Abstract all the complexities
- CSP neutral, Hardware neutral
- Promote open source software
- Make it affordable, even free eventually
- Commoditize Confidential Computing

CONFIDENTIAL COMPUTING CONSORTIUM

Thank you!

Get in touch:
pr@confidentialcomputing.io

Join the Confidential Computing Consortium meetings:
https://confidentialcomputing.io/

Outreach: Every other Wednesday, 5pm CET
https://zoom.us/j/427840416

TAC: Every other Thursday, 4pm CET
https://zoom.us/j/184384055

CONFIDENTIAL COMPUTING CONSORTIUM