

# CERT/CC PGP Key

## Sending Sensitive Information

We recommend that you encrypt sensitive information in email to protect it from being viewed by unintended recipients. We prefer OpenPGP standard cryptography, which usually means Pretty Good Privacy (PGP) or the GNU Privacy Guard (GnuPG or GPG). However, can use S/MIME or other methods on a case-by-case basis.

Those unable to use PGP can contact us at <cert@cert.org> or +1 412-268-5800 to arrange alternative methods.

We also encourage you to check the PGP signature on email and documents to verify the authenticity and integrity of mail from the CERT/CC.

## Download and Verify the Current CERT/CC PGP Key

Our current PGP key is [available below](#) and has the following properties:

```
CERT PGP Key Information
Key ID: 45FD541AB93ED52B
Key Type: RSA
Created: 2019-07-11
Expires: 2020-09-30
Key Size: 4096
Key Fingerprint: 6216 58A6 CE37 C480 E55B F4D9 45FD 541A B93E D52B
UserID: CERT Coordination Center <cert@cert.org>
```

The CERT PGP keys have an operational life span of approximately one year. When we generate a new key, it will be published on this page and updated on public keyservers.

Call us at +1 412-268-5800 to verify the fingerprint.

## CERT/CC PGP Keys (Current and Historical)

Below is a list of keys currently or previously used by CERT/CC. Please use only the most recent key for encrypting new information.

- [2019-07-11 45FD541AB93ED52B](#)
- [2018-09-06 DEE21B6AD59F7366](#)
- [2017-12-01 E3DDDC387B502ECF](#)
- [2017-09-07 69CDF89D591174C3](#)