

CERT/CC PGP Key

We are moving away from PGP email for coordinated vulnerability disclosure in favor of a web-based platform called VINCE. We encourage you to [read about](#) and [start using](#) VINCE.

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:

```
Key ID: 2294BA7D2B2298B9
Key Type: RSA
Key Size: 4096
Created: 2021-06-16
Expires: 2022-09-30
Key Fingerprint: 7F5F 2679 07B2 C455 9DB3 60DB 2294 BA7D 2B22 98B9
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 to 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.

- [Current Key](#)
- [2021-06-16 2294BA7D2B2298B9](#)
- [2020-09-24 738058A74C4ADC8C](#)
- [2019-07-11 45FD541AB93ED52B](#)
- [2018-09-06 DEE21B6AD59F7366](#)
- [2017-12-01 E3DDDC387B502ECF](#)
- [2017-09-07 69CDF89D591174C3](#)