**Suspect Code:** Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user’s consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.

**4.9.1.3 Revocation Based on Reported or Detected Compromise or Use in Malware**

For all incidents involving malware, CAs SHALL revoke the Code Signing Certificate in accordance with and within the following maximum timeframes. Nothing herein prohibits a CA from revoking a Code Signing Certificate prior to these timeframes.

1. The CA MUST contact the software publisher within one (1) business day after the CA is made aware of the incident.
2. The CA MUST determine the volume of relying parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
3. The CA MUST request the software publisher send an acknowledgement to the CA within 72 hours of receipt of the request.
	1. If the publisher responds within 72 hours, the CA and publisher MUST determine a “reasonable date” to revoke the certificate based on discussions with the CA.
	2. If CA does not receive a response, the CA must notify the publisher that the CA will revoke in 7 days if no further response is received.
		1. If the publisher responds within 7 days, the CA and the publisher will determine a “reasonable date” to revoke the certificate based on discussion with the CA.
		2. If no response is received after 7 days, the CA must revoke the certificate except if the CA has documented proof (e.g., OCSP logs) that the revocation will cause significant impact to the general public.

A CA revoking a Certificate because the Certificate was associated with signed Suspect Code or other fraudulent or illegal conduct SHOULD provide all relevant information and risk indicators to other CAs or industry groups. The CA SHOULD indicate whether its investigation found that the Suspect Code was a false positive or an inadvertent signing.