

# Heartbleed

OpenSSL används i många system som är anslutna till SWAMID. Detta är SWAMID operations rekommendation av hur heartbleed skall hanteras i SWAMID:

Det finns normalt 2 nycklar i en SP eller IdP: en nyckel för den webserver som utgör användargränssnittet för tjänsten eller IdPn och en nyckel som används mellan IdPer eller SPer. Denna andra nyckel (federationsnyckeln) är den som finns i federationsmetadata. SWAMIDs rekommendation är att dessa nycklar bör vara olika: federationsnyckeln kan med fördel associeras med ett sk självsignerat certifikat som inkluderas i metadata. De som satt upp sin SP eller IdP enligt denna rekommendation behöver normalt inte byta federations-nyckeln utom i följande två fall:

1. En shibboleth idp som uppsatt så att apache hanterar SSL för port 8443 \*och\* om apache använder en sårbar openssl så bör IdPns federationsnyckel bytas. Förklaringen är att port 8443 använder federationsnyckeln för TLS och om man konfigurerat sin apache att hantera denna port och (tex via ajp) skicka vidare trafiken till shibboleth IdPn så kommer federationsnyckeln att vara tillgänglig för apache-processen och alltså potentiellt blivit exponerad i en heartbleed-attack. Denna port används för SOAP-bindings för AttributeResponse.
2. En simplesamlphp som kör i mod\_php så ska den nycklas om oavsett om det är en SP eller IdP om openssl-versionen är sårbar.

Kontrollera på din OS-distributionsleverantörs hemsida om din installerade version av openssl är sårbar. Har du byggt och kompilerat openssl får du själv kontrollera sårbarheten. De versioner av openssl som levererats av openssl är sårbara i version 1.0.1- 1.0.1f och 1.0.2beta