



# AGID

Agenzia per l'Italia Digitale

# spod

## SPID – SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE

Avviso nr. 33 – Versione 2

11/11/2020

### INFRASTRUTTURA A CHIAVE PUBBLICA AGID DELLA FEDERAZIONE SPID

È istituita presso l'Agenzia per l'Italia Digitale un'infrastruttura a chiave pubblica (PKI) gerarchica, basata su una CA radice (*root CA*) e specifiche CA intermedie (*sub-CA*) utilizzate per fornire ai soggetti partecipanti alla federazione SPID i certificati elettronici per verificare i sigilli elettronici apposti sui messaggi scambiati con la controparte e sui metadata afferenti ai soggetti stessi.

Alla data del presente Avviso, i fornitori di servizi pubblici – così come identificati nell'Avviso SPID №28/2020 e s.m.i. – possono continuare ad utilizzare certificati *self-signed*.

Al fine di verificare l'intera catena dei certificati, il certificato di CA radice e i certificati di CA intermedie sono pubblicati ai seguenti indirizzi:

- *root CA*: [https://eidas.agid.gov.it/certificati/AgID\\_eIDAS\\_Root\\_CA.cer](https://eidas.agid.gov.it/certificati/AgID_eIDAS_Root_CA.cer)
- *sub-CA* per IDP: [https://eidas.agid.gov.it/certificati/Sub\\_CA\\_SPID\\_IdP.cer](https://eidas.agid.gov.it/certificati/Sub_CA_SPID_IdP.cer)
- *sub-CA* per SP pubblici: [https://eidas.agid.gov.it/certificati/Sub\\_CA\\_SPID\\_pubblici.cer](https://eidas.agid.gov.it/certificati/Sub_CA_SPID_pubblici.cer)
- *sub-CA* per SP privati: [https://eidas.agid.gov.it/certificati/Sub\\_CA\\_SPID\\_privati.cer](https://eidas.agid.gov.it/certificati/Sub_CA_SPID_privati.cer)

Il diagramma di flusso della PKI su cui si basa il sistema di fiducia descritto è accessibile al seguente URI: [https://eidas.agid.gov.it/spid/Diagram\\_PKI\\_federazione\\_SPID\\_v1.0.pdf](https://eidas.agid.gov.it/spid/Diagram_PKI_federazione_SPID_v1.0.pdf)

Il Responsabile del progetto SPID