Gatekeeper Public Key Infrastructure Framework

A whole-of-government suite of policies, standards and procedures that governs the use of digital keys and certificates in Government.

The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that govern the use of digital keys and certificates in Government for the authentication of individuals, organisations and non-person entities - such as devices, applications and computing components. Organisations that that do not provide digital certificate services to government can also undergo the Gatekeeper accreditation process if they so wish.

Gatekeeper accreditation supports PKI hierarchies which issue digital keys and certificates to subscribers whom:

* interact in open environments (e.g. the Internet);
* participate in closed environments (e.g. communities of interest); and,
* interact in both open and closed environments (e.g. hybrid communities).

The Gatekeeper Framework has been developed in consultation with Agencies, lawyers, ICT security auditors, PKI subject matter experts and commercial service providers.

**Print formatted version of the Gatekeeper PKI Framework – PDF (415 kb)**

Why is this important?

The Framework is mandatory for agencies using PKI to authenticate their clients through the use of digital keys and certificates issued by Gatekeeper accredited Service providers. It ensures a whole-of-government outcome that delivers integrity, interoperability, authenticity and trust for Service Providers and their Subscribers that aligns the application of PKI to the way government agencies interact with external stakeholders.

## How do I?

* Apply for Accreditation
* Engage a Service Provider
* See who is Accredited
* See who is undergoing accreditation