» venafi_certificate

Provides access to TLS key and certificate data enrolled using Venafi. This can be used to define a certificate.

» Example Usage

```
resource "venafi_certificate" "webserver" {
    common_name = "web.venafi.example"
    algorithm = "RSA"
    rsa_bits = "2048"
    san_dns = [
        "web01.venafi.example",
        "web02.venafi.example"
    ]
    key_password = "${var.pk_pass}"
}
```

» Argument Reference

The following arguments are supported:

- `common_name` - (Required, string) The common name of the certificate.
- `algorithm` - (Optional, string) Key encryption algorithm, either RSA or ECDSA. Defaults to "RSA".
- `rsa_bits` - (Optional, integer) Number of bits to use when generating an RSA key. Applies when algorithm=RSA. Defaults to 2048.
- `ecsa_curve` - (Optional, string) Elliptic curve to use when generating an ECDSA key pair. Applies when algorithm=ECDSA. Defaults to "P521".
- `san_dns` - (Optional, set of strings) List of DNS names to use as alternative subjects of the certificate.
- `san_email` - (Optional, set of strings) List of email addresses to use as alternative subjects of the certificate.
- `san_ip` - (Optional, set of strings) List of IP addresses to use as alternative subjects of the certificate.
- `key_password` - (Optional, string) The password used to encrypt the private key.
- `expiration_window` - (Optional, integer) Number of hours before certificate expiry to request a new certificate.

» Attributes Reference

The following attributes are exported:

- `private_key_pem` - The private key in PEM format.
- `chain` - The trust chain of X509 certificate authority certificates in PEM format concatenated together.
- `certificate` - The X509 certificate in PEM format.