REGIONE TOSCANA

Giunta Regionale

Direzione Generale Organizzazione

Settore Ufficio per la Transizione al Digitale

Infrastrutture e Tecnologie per lo Sviluppo

della Societa' dell'Informazione

Rilascio certificati ad uso applicativo

DOCUMENTO: **P*rocedure operative per le richieste di certificati ad uso applicativo -- Public Key Infra*structure - PKI**	

EMISSIONE - VERIFICA - APPROVAZIONE			
	Funzione	Nome	firma
Emissione	Direttore Esecuzione Contratto	Grazia Ugolini	
Emissione	Funzionario Collaboratore su Contratto	Andrea Panichi	
Verifica	Funzionario	Alessandro Tarchi	
Verifica	Funzionario	Vincenzo Martiello	
Verifica			
Approvazione	Dirigente Responsabile Contratto UTD - ITSSI)		

LISTA DI DISTRIBUZIONE : ad uso interno di Regione Toscana

AGGIORNAMENTI

Versione	Data	Paragrafi Modificati	Motivo Modifica
1.0	19/09/2018		Prima stesura
1.1	26-09-2018	-	Rivista formattazione
1.2	21/06/2019		Modifica relativa al dirigente responsabile e relativa anonimizzazione

1 Premessa

Regione Toscana , attraverso un contratto di fornitura , fornisce certificati ad uso *server* di varia tipologia.

Lo scopo del presente documento è rendere noto le specifiche e le procedure per una corretta gestione del ciclo di vita dei suddetti certificati .

La struttura indicata nella sezione “versioning” sul rigo “Approvazione”, opera in qualità di RA (Registration Autority) nei confronti del fornitore di servizi contrattualizzato.

2 Tipologia dei certificati

- **OV** : Autenticazione Server (Single-SAN Organization Validated (OV)) (comunemente indicati nelle procedure attuali come certificati server della CA pubblica)
  - Scadenza : 1 o 2 anni
- **CA privata RT** : Certificati ad uso universale emessi su CA privata di RT . (vengono utilizzati ad esempio in scenari di mutua autenticazione machine to machine)
  - scadenza: 1 o 3 o 5 anni

3 Modalità di richiesta

3.1 Chi può richiedere certificati

Le richieste devono essere fatte dal capo progetto RT responsabile della componente applicativa o del sistema che necessita del certificato o dal suo supporto tecnico, su sua esplicita autorizzazione e per ogni certificato richiesto.

E' responsabilità del richiedente tenere traccia o monitorare la scadenza del certificato.

La RA non è tenuta ad avvertire il richiedente dell'approssimarsi della scadenza.

Di buona regola la RA inoltra email di avviso scadenza certificato alla **email di riferimento** solo per i certificati OV.

3.1.1 Sistemi al TIX

Il supporto tecnico, che può effettuare le richieste su autorizzazione del capo progetto RT, si differenzia a seconda della tipologia dell’asset su cui deve essere installato il certificato:

- tipologia IAAS: è il supporto tecnico della componente applicativa o del sistema che necessita del certificato;
- tipologia PAAS o SAAS: il supporto tecnico è il presidio del Centro Servizio TIX, che si occuperà di tutti i relativi aspetti (richiesta, installazione, monitoraggio, ecc.)

In ogni caso è consentito chiedere supporto al Centro Servizi TIX per l’inserimento del controllo “scadenza certificato” nel sistema di monitoraggio TIX nella sezione della componente o servizio

relativo.

3.2 Come si richiedono i certificati

Le richieste devono a essere inoltrate all'indirizzo email ra.pki@regione.toscana.it

L'oggetto del messaggio deve contenere la label [RA] CN=<nome a dominio>

Nel corpo del messaggio devono essere indicati :

- La modalità di richiesta (default o chiave) – vedasi punti 3.2.1 e 3.2.2
- Il tipo di certificato richiesto (OV o CA privata RT)
- Le informazioni per la generazione del certificato :
  - **OU=< Unità Organizzativa**> (se non specificato verrà inserito dalla RA : **Regione Toscana)**
  - **CN=<nome a dominio>** (ad esempio: **www.regione.toscana.it**; per certificati della CA privata RT non e' necessario che sia un effettivo nome a dominio, ad esempio e' corretto anche un nome come **NAL-R-Toscana**.
  - **email=<email di riferimento> (**Si veda la relativa sezione note).

ATTENZIONE :Nel caso di servizio TIX deve essere data l'indicazione della tipologia dell'asset su cui va installato il certificato (IAAS, PAAS, SAAS).

3.2.1 Modalità default

Si definisce modalità di default la modalità in cui la RA genera la chiave privata del certificato richiesto.

La RA restituisce, in risposta alla email di richiesta, un file in formato P12 contenente anche la chiave privata del certificato richiesto.

3.2.2 Modalità con chiave privata generata dal committente

In questo caso allegato alla mail di richiesta deve essere fornita la CSR a cura del committente.

Si ricorda a tale proposito che i campi

- **C=IT**
- **O=Rete Telematica Regionale Toscana**

sono fissi e non modificabili.

La RA in questo caso **restituisce al richiedente** il certificato in formato PEM.

4 Note

4.1 CN

Per i certificati **OV** (SSL emessi su CA Pubblica) esistono dei regolamenti che esulano i nostri ambiti di competenza.

Regione Toscana deve dimostrare, secondo procedure stabilite dal certificatore responsabile della emissione del certificato, la propria competenza sul dominio sul quale viene registrato il CN richiesto.

Pertanto se vengono richiesti certificati su domini su cui ancora RT non ha mai provveduto a fornire tale evidenze, l'emissione del certificato non può essere immediata.

4.1.1 Domini attualmente autorizzati

Questa la lista (non esaustiva) dei domini su cui RT **è gia autorizzata:**

***.arti.toscana.it**

***.aurit.toscana.it**

***.cittadinoinformato.it**

***.e.toscana.it**

***.giovanisi.it**

***.lavoro.toscana.it**

***.lifeweee.eu**

***.open.toscana.it**

***.piattaformaturismo.toscana.it**

***.prevenzionecollettiva.toscana.it**

***.regione.toscana.it**

***.rete.toscana.it**

***.sanita.toscana.it**

***.servizi.toscana.it**

***.sisac.toscana.it**

***.start.toscana.it**

***.suap.toscana.it**

***.tix.it**

4.2 E-mail di riferimento

Il campo email viene utilizzato per eventuali comunicazioni sullo stato del certificato . Si

suggerisce di utilizzare email **non personali** ma di progetto. Sono consentite, a responsabilità del capoprogetto richiedente il certificato, anche liste di distribuzione che comprendono piu' indirizzi, anche esterni al nome a dominio regione.toscana.it (ad esempio: **staff@tix.it**).

4.3 PEM

Formato più comunemente utilizzato dalle Certification Authorities per emettere i certificati, solitamente utilizzando le estensioni convenzionali .pem, .crt, e .cer. Sono files ASCII con codifica Base64 e contengono "-----BEGIN CERTIFICATE-----" all'inizio e "-----END CERTIFICATE-----" alla fine. Possono essere in formato PEM sia certificati server, che certificati intermedi e chiavi private.

4.4 P12 (o PKCS#12 / PFX)

Il formato PKCS#12 o PFX è un formato binario che permette di salvare in modo criptato sia il certificato server e quelli intermedi, che la chiave privata. L'estensione utilizzata è solitamente .pfx o .p12. I file PFX sono di solito usati su macchine Windows per effettuare backup e migrazioni da un server all'altro di certificati con le loro rispettive chiavi private.

5 Riferimenti

Di seguito i profili attualmente contrattualizzati:

5.1 Profilo dei certificati OV

Attualmente la CA contrattualizzata **root: "Actalis Authentication Root CA** meglio descritta sul sito del certificatore :

https://www.actalis.it/prodotti/certificati-ssl.aspx

5.2 CA privata RTRT

CN = CA Privata RTRT

OU = Regione Toscana

O = Rete Telematica della Regione Toscana

C = IT