Let’s encrypt! Certificati SSL per tutti!

Nicola Corti

Gruppo Utenti Linux Pisa

02 Febbraio 2016

Cosa è Let's encrypt?

Let's encrypt è una **Certification Authority (CA)** che rilascia certificati SSL/TLS a titolo **gratuito**.

- Dal 5 Dicembre 2015 si trova in **Public Beta**.
- Ad oggi ha rilasciato più di **480 k** certificati.
- Fa dell'**automazione** il suo punto di forza.
- https://letsencrypt.org/

Cosa è Let's encrypt?

Let's encrypt è una **Certification Authority (CA)** che rilascia certificati SSL/TLS a titolo **gratuito**.

- Dal 5 Dicembre 2015 si trova in **Public Beta**.
- Ad oggi ha rilasciato più di **480 k** certificati.
- Fa dell'**automazione** il suo punto di forza.
- https://letsencrypt.org/

Cosa è Let's encrypt?

Let's encrypt è una **Certification Authority (CA)** che rilascia certificati SSL/TLS a titolo **gratuito**.

- Dal 5 Dicembre 2015 si trova in **Public Beta**.
- Ad oggi ha rilasciato più di **480 k** certificati.
- Fa dell'**automazione** il suo punto di forza.
- https://letsencrypt.org/

Cosa è Let's encrypt?

Let's encrypt è una **Certification Authority (CA)** che rilascia certificati SSL/TLS a titolo **gratuito**.

- Dal 5 Dicembre 2015 si trova in **Public Beta**.
- Ad oggi ha rilasciato più di **480 k** certificati.
- Fa dell'**automazione** il suo punto di forza.
- https://letsencrypt.org/

Cosa è Let's encrypt?

Let's encrypt è una **Certification Authority (CA)** che rilascia certificati SSL/TLS a titolo **gratuito**.

- Dal 5 Dicembre 2015 si trova in **Public Beta**.
- Ad oggi ha rilasciato più di **480 k** certificati.
- Fa dell'**automazione** il suo punto di forza.
- https://letsencrypt.org/

Sponsors

Chi sta supportando il progetto?

Platinum

Gold

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

History

2012 Iniziato il progetto dentro **Mozilla**

11-2014 Let's Encrypt **annunciato pubblicamente**

01-2015 Protocollo **ACME** sottoposto all'**IETF** per essere standardizzato.

04-2015 **ISRG** (Internet Security Research Group) e la **Linux Foundation** si uniscono al progetto

09-2015 Rilasciato il primo certificato per **helloworld.letsencrypt.org**

10-2015 Il certificato intermedio di L.E. diventa ***cross-signed*** grazie a IdenTrust. (*Let's Encrypt is trusted!*)

12-2015 **Public beta!**

Why?

- **Free**
- **Automatico**
- **Open**
- **Sicuro**
- **Trasparente**

Boulder

Architettura

Il sistema di Let's Encrypt si basa su **3 Componenti**: un **server**, un **client** e il **protocollo** che permette a server e client di comunicare.

Il server si chiama **Boulder** ed è scritto interamente in **Go**. Si occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

https://github.com/letsencrypt/boulder

Boulder

Architettura

Il sistema di Let's Encrypt si basa su **3 Componenti**: un **server**, un **client** e il **protocollo** che permette a server e client di comunicare.

Il server si chiama **Boulder** ed è scritto interamente in **Go**. Si occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

https://github.com/letsencrypt/boulder

Boulder

Architettura

Il sistema di Let's Encrypt si basa su **3 Componenti**: un **server**, un **client** e il **protocollo** che permette a server e client di comunicare.

Il server si chiama **Boulder** ed è scritto interamente in **Go**. Si occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

https://github.com/letsencrypt/boulder

Domande...?

Slides realizzate da:
Nicola Corti - corti.nico [at] gmail [dot] com

Slides realizzate con LaTeX Beamer.