Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Gruppo Utenti Linux Pisa



02 Febbraio 2016

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

HILLIC

Serve

Client

FIULUCU



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 de ll'automazione il suo punto di forza.
- https://letsencrypt.org/

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Jilent

FIULUL

Certs



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/

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Serve

Client

Protoc

Certs



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/

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Serve

Clien

Proto

Certs



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/

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Serve

CITE

Protoc

OCI to

Setur



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/

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Serve

Clier

FIOLO

Certs

Sponsors

Chi sta supportando il progetto?

Platinum













Gold





facebook

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

2012 Iniziato il progetto dentro Mozilla

- 11/201/ Let's Encrypt annunciato pubblicamente
 - 2015 Protocollo ACME sottoposto all'IETF per essere standardizzato.
- 14-2015 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!

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Client

Protocol

erts

Setur

Certificati SSL per tutti!

Nicola Corti

Server

Client

rotocol

Certs

Setu

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

standardizzato.

14-2015 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

Certificati SSL per tuttil

Nicola Corti

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

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

Certificati SSL per tuttil

Nicola Corti

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

	r	r	Ť	'n			
	u	Ц	ι	u	Ц	u	

Server

Client

Setun

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

٠.		٠		
П			r	

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!)

Clien

Certs

Setup

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

SHEIR

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.

ll 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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Client

Protocc

00,00

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.

I<mark>l server si chiama **Boulder** ed è scritto interamente in **Go**. Si</mark> occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

Certificati SSL per tuttil

Nicola Corti

Server

Boulder

Certificati SSL per tuttil

Nicola Corti

Server

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.

I<mark>l server si chiama **Boulder** ed è scritto interamente in **Go**. Si</mark> occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

Ohttps://github.com/letsencrypt/boulder

Domande...?

Slides realizzate da:

Nicola Corti - corti.nico [at] gmail [dot] com

Slides realizzate con La Beamer.

La seguente presentazione è rilasciata sotto licenza

Creative Commons - Attributions, Non Commercial, Share-alike.



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

HILLIC

Serve

Client

.0.000

Certs