## 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

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

### 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

Di fatto si tratta di un server HTTP che espone un'interfaccia
RESTful

https://github.com/letsencrypt/boulder

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Client

. . . . . . . .

Certs

### 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.

Di fatto si tratta di un server HTTP che espone un'interfaccia

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Client

Protoc

CELLS

### 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.

Di fatto si tratta di un server HTTP che espone un'interfaccia RESTful

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.

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.

Di fatto si tratta di un server HTTP che espone un'interfaccia **RESTful** 

Ohttps://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

IIIIIO

Server

Client

Protoco

00.00

## letsencrypt

Il client si chiama (semplicemente) letsencrypt ed è scritto interamente in Python. Si occupa di farvi interagire con il server remoto e gestisce i vostri certificati.

Installabile tramite il pacchetto letsencrypt (solo debian sid/stretch).

labile tramite **clone** del repository.

https://github.com/letsencrypt/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Client

Protoco

0 - 4. ...

## letsencrypt

Il client si chiama (semplicemente) letsencrypt ed è scritto interamente in Python. Si occupa di farvi interagire con il server remoto e gestisce i vostri certificati.

- Installabile tramite il pacchetto letsencrypt (solo debian sid/stretch).
- ► Installabile tramite clone del repository.

https://github.com/letsencrypt/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

Client

Protoc

JEI LS

## letsencrypt

Certificati SSL per tutti!

Nicola Corti

Intro Serve

Client

Protoc

Satur

Il client si chiama (semplicemente) letsencrypt ed è scritto interamente in **Python**. Si occupa di farvi interagire con il server remoto e **gestisce i vostri certificati**.

- Installabile tramite il pacchetto letsencrypt (solo debian sid/stretch).
- ► Installabile tramite **clone** del repository.
  - Ohttps://github.com/letsencrypt/letsencrypt

## **Plugins**

Lo scopo principale del client è quello di **semplificare e automatizzare** tutto il processo di autenticazione e di creazione del certificato.

Per questo motivo sono stati sviluppati dei plugin per il setup automatico dei certificati ottenuti sui principali web browser: apache ed nginx.



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Serve

Client

Protoco

Certs

etup

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

Client

Protoco

erts

Lo scopo principale del client è quello di **semplificare e automatizzare** tutto il processo di autenticazione e di creazione del certificato.

Per questo motivo sono stati sviluppati dei plugin per il setup automatico dei certificati ottenuti sui principali web browser: apache ed nginx.





Il protocollo che utilizzano client e server per interagire si chiama **Automated Certificate Management Environment (ACME)**.

ACME si base sullo scambio di file **JSON** firmati (anche detti JWS, **Json Web Signature**). Questi documenti contengono le richieste inviate dal client e le risposte ottenute dal server.

Lo scambio di questi documenti deve avvenire attraverso

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Client

Protoco

\_ \_ \_ \_

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro Serve

Cilent

1 101000

2atun

Il protocollo che utilizzano client e server per interagire si chiama **Automated Certificate Management Environment (ACME)**.

ACME si base sullo scambio di file **JSON** firmati (anche detti **JWS, Json Web Signature**). Questi documenti contengono le richieste inviate dal client e le risposte ottenute dal server.

o di questi documenti deve avvenire attraverso

HTTPS

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro Serve

- Ciletit

.....

Il protocollo che utilizzano client e server per interagire si chiama **Automated Certificate Management Environment (ACME)**.

ACME si base sullo scambio di file **JSON** firmati (anche detti **JWS, Json Web Signature**). Questi documenti contengono le richieste inviate dal client e le risposte ottenute dal server.

Lo scambio di questi documenti deve avvenire attraverso **HTTPS**.

Network Working Group R. Barnes
Internet-Draft Mozilla
Intended status: Standards Track J. Hoffman-Andrews
Expires: January 22, 2016 EFF
J. Kasten
University of Michigan
I uly 21, 2015

#### Automatic Certificate Management Environment (ACME)

draft-barnes-acme-04

#### Abstract

Certificates in the Web's X.509 PKI (PKIX) are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certificate authorities in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. Today, this verification is done through a collection of ad hoc mechanisms. This document describes a protocol that a certificate authority (CA) and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

https://github.com/letsencrypt/acme-spec

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Protocol

### Il protocollo ACME ci permette di eseguire tre operazioni:

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Il protocollo ACME ci permette di eseguire tre operazioni:

- 1. **Provare** che noi siamo i responsabili del dominio example.com
- Ottenere un certificato per il dominio example.com
- 3. Revo**care** o **rinnovare** un certificato per il dominio *exam ple.com*

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Clier

Protoco

Satur

Il prot<mark>ocollo</mark> ACME ci permette di eseguire tre operazioni:

- 1. **Provare** che noi siamo i responsabili del dominio example.com
- 2. Ottenere un certificato per il dominio example.com
- 3. Revocare o rinnovare un certificato per il dominio example.com

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Clien

Protoco

Il prot<mark>ocollo</mark> ACME ci permette di eseguire tre operazioni:

- 1. **Provare** che noi siamo i responsabili del dominio example.com
- 2. Ottenere un certificato per il dominio example.com
- 3. **Revocare** o **rinnovare** un certificato per il dominio *example.com*

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

liont

Protoco

Setun

Client

Protoco

0 - 4----

Setup

Le interazioni fra client e server sono cifrate tramite una coppia di **chiavi asimmetriche** (una **privata** ed una **pubblica**) che viene generata durante il primo avvio del client.

Il server ci permette di **provare** che siamo gli amministratori del dominio desirato, inviandoci una o più **challenge** che dobbiamo risolvere.

Ogni interazione con il server è inoltre corredata da un **nonce** che permette di evitare attacchi di tipo **Replay**.

Donton

Certs

Setup

Le interazioni fra client e server sono cifrate tramite una coppia di **chiavi asimmetriche** (una **privata** ed una **pubblica**) che viene generata durante il primo avvio del client.

Il server ci permette di **provare** che siamo gli amministratori del dominio desirato, inviandoci una o più **challenge** che dobbiamo risolvere.

Ogni interazione con il server è inoltre corredata da un **nonce** che permette di evitare attacchi di tipo **Replay**.

Olicile

Certs

Setup

Le interazioni fra client e server sono cifrate tramite una coppia di **chiavi asimmetriche** (una **privata** ed una **pubblica**) che viene generata durante il primo avvio del client.

Il server ci permette di **provare** che siamo gli amministratori del dominio desirato, inviandoci una o più **challenge** che dobbiamo risolvere.

Ogni interazione con il server è inoltre corredata da un **nonce** che permette di evitare attacchi di tipo **Replay**.

## Challenges

Il server può, a sua discrezione, inviare una o più challenges.

Tipo	Descrizione
DNS	Si chiede di inserire un <b>record TXT</b> all'interno

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

IIILIC

Server

lient

Protocol

S -- do . . . . .

Il serv<mark>er pu</mark>ò, a sua discrezione, inviare una o più challenges.

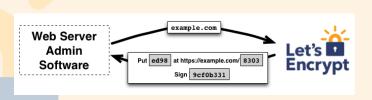
Tipo	Descrizione
Simple HTTP	Si chiede di posizionare un file all'interno
	del proprio webserver contenente un token
	specifico (Accettato sia HTTP che HTTPS).
DNS	Si chiede di inserire un <b>record TXT</b> all'interno
	del proprio DNS.
Proof of possession	Si chiede di <b>firmare un documento</b> utilizzando una chi-
	ave che il server può ricondurre al client.
Domain Validation with	Si chiede di <b>configurare un server TLS</b> ad uno specifico
Server Name Indication	indirizzo IP (tramite un record A nel DNS).

ntro

Protocol

FIULUCU

### **Domain Validation**

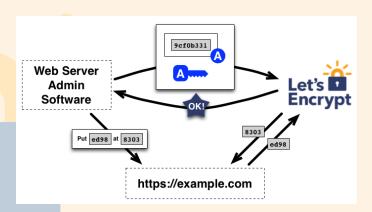


#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Protocol

### **Domain Validation**



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

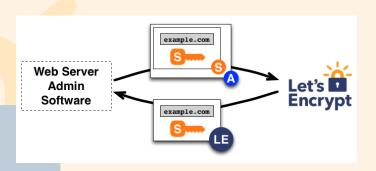
ntro

Server

Client

Protocol

### Certificate Issuance



#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

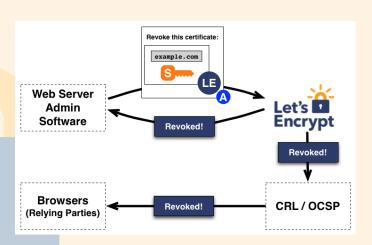
Server

Client

Protocol

Certs

### Certificate Revocation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

Server

CHETTE

Protocol

## **DV** Certificates

#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

DV

I certificati rilasciati sono di tipo **Domain Validated**. Provano cioè che si è effettivamente i proprietari di un determinato dominio.

Certificati di tipo **Organization Validation** oppure **Extended Validation** richiederebbero verifiche esplicite del soggetto che fa richiesta del certificato.

ntro

erve

Client

Protoco

Certs

## **DV** Certificates

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Client

-10100

Certs

DV

I certificati rilasciati sono di tipo **Domain Validated**. Provano cioè che si è effettivamente i proprietari di un determinato dominio.

Certificati di tipo Organization Validation oppure Extended Validation richiederebbero verifiche esplicite del soggetto che fa richiesta del certificato.



## **Cross Signing**

Tutti i certificati rilasciati sono *Cross-signed* da parte di **IdenTrust**. Questo permette ai certificati di L.E. di essere riconosciuti dalla maggioranza dei browser.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Gliei

Certs

## **Cross Signing**

Tutti i certificati rilasciati sono *Cross-signed* da parte di **IdenTrust**. Questo permette ai certificati di L.E. di essere riconosciuti dalla maggioranza dei browser.



#### Let's encrypt! Certificati SSL per tutti!

Nicola Corti

lni

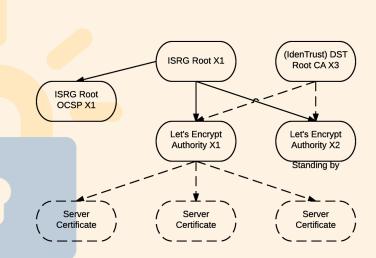
Serve

Olici

Certs

. .

## **Cross Signing**



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Server Client

Protoc

Certs

## Validity

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

Server

Client

Certs

otuun

I certificati hanno una validità di **90 giorni** dopo i quali scadono, e non s<mark>ono c</mark>onsiderati più validi dai browser.

## 90-days validity

Questa non è una novità nel mondo della sicurezza. Rinnovare i certificati frequentemente è una buona abitudine e permette di limitare i danni di eventuali certificati compromessi.

Riceveremo delle mail di *remind* che ci ricordano della scadenza È possibile automatizzare il processo di rinnovo tramite dei task

di cron

## Validity

Certificati SSL per tutti!

Nicola Corti

Intro

Clions

Certs

00,10

Setup

I certificati hanno una validità di **90 giorni** dopo i quali scadono, e non s<mark>ono c</mark>onsiderati più validi dai browser.

## 90-days validity

Questa non è una novità nel mondo della sicurezza. Rinnovare i certificati frequentemente è una buona abitudine e permette di limitare i danni di eventuali certificati compromessi.

o delle mail di *remind* che ci ricordano della scadenza automatizzare il processo di rinnovo tramite dei task

di cron.

Certs

Setup

I certificati hanno una validità di **90 giorni** dopo i quali scadono, e non s<mark>ono c</mark>onsiderati più validi dai browser.

## 90-days validity

Questa non è una novità nel mondo della sicurezza. Rinnovare i certificati frequentemente è una buona abitudine e permette di limitare i danni di eventuali certificati compromessi.

Riceveremo delle mail di *remind* che ci ricordano della scadenza. È possibile automatizzare il processo di rinnovo tramite dei task di **cron**.

# 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

101000