Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Gruppo Utenti Linux Pisa



03 Febbraio 2016

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Client

TOTOCOL

Challennes

The protocol

Carta

Certs

Cross Signin

etup

Requirements

Run

Plugins

Revoke

Update

Screens

Conclusions

esources



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

Inti

Spor

History

Server

Client

Protoco

Challenges

Cert revocation

Certs

Cross Signing

Gross digrilling

Danvisamenta

Requirements

Download

Plugins

Revoke

Update

Screens

onclusions

Drawbacks



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**

Let's encrypt! Certificati SSL per tuttil

Nicola Corti



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

Sponso

History Why?

Server

Clien

Protocol

Challenges

The protocol

Certs

Cross Signin

otup

Requirements

Requirements

Run

Plugins

Revoke

Update

creens

Conclusions



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

Inti

Sponsors History

Server

Clien

Protocol

Challenges

The protocol

Certs

Cross Signing

Setup

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions



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

Sponsor History

Server

Clien

Protocol

Challenges The protocol

The protocol

Cert revocatio

Certs

Cross Signing

etup

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions

Sponsors

Chi sta supportando il progetto?















Gold





facebook

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

2012 Iniziato il progetto dentro **Mozilla**

11/2014 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

Sponsors

History

Why?

CIVCI

Client

rotocol

Otocoi

The protocol

Cert revocation

erts

Cross Signing

Setup

Requirements

un

Plugins

Renewal

Update

naluaiana

onclusions

esources

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

History Why?

liont

.....

1010001

Challenges The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Download

Plugins

Revoke

Undate

Screens

onclusions

esources

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

2015 Protocollo **ACME** sottoposto all'**IETF** per essero standardizzato.

04-2**015 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

Sponsors

Histo Why?

anvar

Client

Protocol

-

Challenges
The protocol

Cert revocatio

erts

Cross Signing

Setup

Requirements

Run

Plugins

Revoke

Update

creens

onclusions

esources

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

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

04-2**016 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 tuttil

Nicola Corti

2012	Iniziato	il	progetto	dentro	Mozilla
2012	IIIIZIALO	ш	progetto	ucritio	IVIOZIIIC

- 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

History Why?

Server

Client

Protocol

Challenges
The protocol

Cert revocatio

DV

Cross Signing

Requirements

Requirements Download

Run

Revoke

Update

Screens

Conclusions Drawbacks

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Why?

Client

Protocol

Challenges The protocol

Certs

DV Cross Signing

Cross Signing

Requirements

Run Plunins

Revoke Renewal

Update

maluaian

Conclusions Drawbacks

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

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

100

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!

- Free
- Automatico
- Open
- Sicuro
- ▶ Trasparente

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Why?

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

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

History

Server

Clien

OLOCOI

Security

The protocol

Cert revocation

Certs

Cross Signing

etup

Requirements

Run

Plunins

Revoke

Renewal

Update

onclusions

Resources

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

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

Server

Clien

rotocol

Paramita.

Challenges
The protocol

Cert revocatio

erts

Cross Signing

etup

Requirements

Download

Run

Plugins

revoke Renewal

Update

creens

Conclusions

Resources

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**

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

Server

Client

rotocol

1010001

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Download

Plugins

Revoke

Update

Screens

Conclusions

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**

O https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsor

History Why?

Server

Client

Orotooo

1010COI

The protocol

Cert revocation

OV

Cross Signing

Requirements

Requirements Download

Run

Plugins

Renewal

Screens

Conclusions

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/letsencryp

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

Server

Client

Protocol

FIULUCU

Challenges
The protocol

Cert revocatio

Certs

Cross Signii

CIOSS SIGIII

equirements

Requirements

Run

Plugins

Revoke

Update

creens

onclusions

esources

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

Intro

Why?

00.70

Client

Protocol

PIOLOCO

The protocol

Cert revocation

rts

/ oss Signing

etup

Requirements

Run

Plugins

enewal

Screens

Conclusions

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.

Ohttps://github.com/letsencrypt/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Server

Client

Protocol

Security

The protocol

rts

ss Signing

etup

Requirements

Run

Plugins Revoke

Henewal Update

Screens

Conclusions

sources

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

ntro

Histor

_

Client

Clien

Protocol

Challennee

The protocol

Cert revocation

erts

erts

Cross Signing

Requirements

Download

Run

Plugins Revoke

Update

Screens

Conclusions

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

Sponsors

Why?

Client

iciit

rotocol

The protocol

Cert revocation

DV DV

Cross Signing

Requirements

Run

Plugins Revoke

Renewal Update

Screens

Conclusions

Drawbacks

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 scamb o di questi documenti deve avvenire attraverso

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor Why?

Serve

Clien

Protocol

Protoco

Challenges

Cert revocation

Certs

Cross Signin

Cross Signii

etup

Requirements

Run

Plugins

Revoke

Renewal

Update

ومونورياهم

onclusions

Resources

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histor Why?

Clien

Onci

Protocol

Challenges
The protocol

Cert revocation

erts

Cross Signing

Requirements

Requirements

Run

Plugins

enewal

Screens

Conclusions

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**.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Serve

Cilei

Protocol

Challenges The protocol

Cert revocation

erts v

V ross Signing

etup

Requirements

Run

Plugins

enewal ndate

Screens

Conclusions

sources

Network Working Group Internet-Draft Intended status: Standards Track Expires: Innuary 22, 2016

Mozilla J. Hoffman-Andrews EFF J. Kasten University of Michigan July 21, 2015

R Barnes

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.

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Why?

Client

Protocol

Challenges
The protocol

Cert revocatio

Certs

Cross Signing

Requirements

Download Run

Plugins

Renewal

Screens

Conclusions

Il protocollo ACME ci permette di eseguire tre operazioni:

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Il protocollo ACME ci permette di eseguire tre operazioni:

- 1. Provare che noi siamo i responsabili del dominio example.com

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

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

Sponsors

Why

Clien

Protoco

Challenges
The protoco

Cert revoca

Certs

Cross Signing

Requirements

Requirements

Run

Plugins

enewal

Update

Conclusions

rawback: Resources

Il protocollo 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 tuttil

Nicola Corti

Security

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

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.

Security

Security

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**.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Histi Why

0---

Client

Protoco

Security

Challenge

The protoco

Jert revoca

V .

Cross Signing

etup

Requirements

Nownload Run

Plugins

Revoke

Update

onclusions

rawbacks

Security

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

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**.

Sponsors

Why

Serve

Cilent

PIOLOCO

Security

The protoco

Cert revocat

v

oss Signing

etup

Requirements

Run

Plugins Romke

enewal

Update

Conclusions

Challenges

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

Tipo	Descrizione
DNS	Si chiede di inserire un record TXT all'interno

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor

erver

Client

otocol

Security Challenges

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

ownload

Run Plunins

Plugins Revoke

Renewal Indate

Jpdate

onclusions

Il server <mark>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 record TXT all'interno	
	del proprio DNS.	
Proof of possession	Si chiede di firmare un documento utilizzando una chi-	
	ave che il server può ricondurre al client.	
Domain Validation with	Si chiede di configurare un server TLS ad uno specifico	
Server Name Indication	indirizzo IP (tramite un record A nel DNS).	

Intro Sponsors History

History Why?

Client

Protocol
Security
Challenges

The protocol

Certs

Setup Requirements

Run Mugins

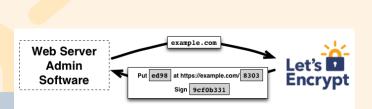
evoke

Update Screens

Conclusions

awbacks esources

Domain Validation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Hist

Server

Client

010001

Challenges

The protocol

Certs

Oross Signin

etup

Requirements

ownload

Plugins

Revoke

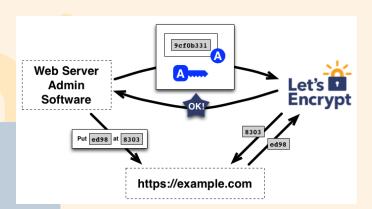
Renewal Update

Screens

Conclusions

Resource

Domain Validation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

Server

Client

ecurity

The protocol

Cert revocatio

erts

DV

Cross Signing

Setup

Requirements

Run

Plugins

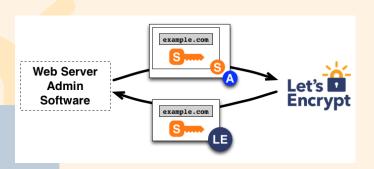
Renewal

Update

Conclusions

rawback: Resources

Certificate Issuance



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

Server

lient

JUCOI

Challenges
The protocol

Cert revocation

Certs

--Cross Signing

etup

Requirements

Download Run

Plugins

Plugins Revoke

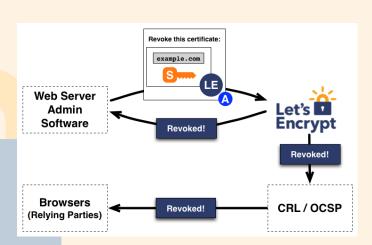
Update

Screens

Conclusions

Resource

Certificate Revocation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Server

lient

rotocol

ecurity

Challenges

Cert revocation

erts

V

Setup

Requirements

lun

Plugins

Renewal Update

Screens

Conclusions

esources

DV Certificates

DV

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

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

DW

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.



Sponsor

Why?

....

Client

Protocol

Challenges
The protocol

Cert revocation

DV

Cross S

etup

Requirements Download

Run Plugins

Revoke Renewal

Update

onclusions

awbacks

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

Sponsor

Wh

Server

lient

Protocol

Security

The protoco

Certs

DV Cross Signine

Cross Signing

Setup

Requirements

Run

Plugins

Revoke

Update

Screens

Conclusions

Resources

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

Sponsor

His

Server

lient

otocol

ecurity

The protocol

Certievocat

DV

Cross Signing

Requirements

Download

Plugins

Revoke

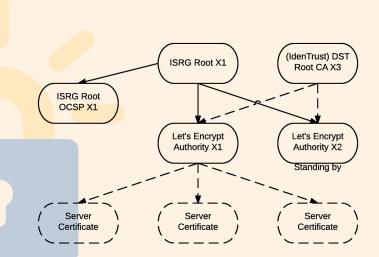
Update

screens

Conclusions

rawback: Resources

Cross Signing



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

Differit

Protocol

Challenges The protocol

Cert revocation

DV Cross Signing

Setup

Requirements

un Iugins

evoke enewal

Screens

Conclusions

awbacks sources

Validity

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histor Why?

erver

Client

Protocol

1010001

Challenges
The protocol

Cert revocati

Certs DV

Cross Signing

Setup

Requirements

ownload

un lugins

lugins Revoke

Update

onclusions

rawbacks esources

I certificati hanno una validità di **90 giorni** dopo i quali scadono, e non sono considerati 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.

È possibile di **cron**

no delle mail di *remind* che ci ricordano della scadenza. Le automatizzare il processo di rinnovo tramite dei task

Validity

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Cross Signing

I certificati hanno una validità di **90 giorni** dopo i quali scadono, e non sono considerati più validi dai browser.

90-days validity

Ouesta 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.

Validity

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

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

Ouesta 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**.

Cross Signing

Requirements

Per eseguire il client è necessario:

- Essere su un sistema Unix like.
- Avere Python 2.6 o 2.7.
- Avere accesso di root sul proprio sistema.

Inoltre, il plugin di autoconfigurazione di **apache**, funziona solamente con sistemi Debian based: **Ubuntu 12.04+** e **Debian 7+**

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor Why?

Server

Client

Protocol

Security

The protocol

Cert revocatio

erts v

DV Cross Signing

Cross aigning

etup

Requirements

Download

Run

Plugins

Renewal

Update

Conclusions

rawback: Resources

Requirements

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Why?

. . . .

rotocol

Challenges
The protocol

Cert revocation

erts w

Cross Signing

Setup

Requirements

Davidand

Download

Plugins

Revoke Renewal

Update

Conclusions

rawbacks esources

Per eseguire il client è necessario:

- Essere su un sistema Unix like.
- Avere Python 2.6 o 2.7.
- Avere accesso di root sul proprio sistema.

Inoltre, il plugin di autoconfigurazione di **apache**, funziona solamente con sistemi Debian based: **Ubuntu 12.04+** e **Debian 7+**

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Server

Client

Protocol

Security

The protocol

Cert revocatio

Certs

Cross Signin

Setup

Requirements

Download

Run

Plugins

Revoke Renewal

Update

Screens

Conclusions

esources

Per prima cosa è necessario scaricare il client letsencrypt.

Per Debian sid/stretch:

```
$ sudo apt-get install letsencrypt
$ letsencrypt --help
```

Per tutti gli altri

```
$ git clone https://github.com/letsencrypt/letsencrypt
$ cd letsencrypt
```

\$./letsencrypt-auto --help

Da ora in poi ci riferiremo ai comandi con **letsencrypt-auto** assumendo che si scelga di clonare il repository.

Nicola Corti

Per prima cosa è necessario scaricare il client **letsencrypt**.

Per Debian sid/stretch:

```
sudo apt-get install letsencrypt
$ letsencrypt --help
```

Let's encrypt! Certificati SSL per tuttil

Download

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Download

Per prima cosa è necessario scaricare il client **letsencrypt**.

Per Debian sid/stretch:

```
sudo apt-get install letsencrypt
$ letsencrypt --help
```

Per tutti gli altri:

```
$ git clone https://github.com/letsencrypt/letsencrypt
$ cd letsencrypt
$ ./letsencrypt-auto --help
```

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

ro

Sponsors

Server

lient

)rotooo

Protocol

Challenges The protocol

Cert revocation

erts

OV OV

Cross Signing

Setup

Download

Download

Run

Plugins

Renewal

Screens

Drawbacks

Per prima cosa è necessario scaricare il client letsencrypt.

Per Debian sid/stretch:

```
$ sudo apt-get install letsencrypt
$ letsencrypt --help
```

Per tutti gli altri:

```
$ git clone https://github.com/letsencrypt/letsencrypt
$ cd letsencrypt
$ ./letsencrypt-auto --help
```

Da ora in poi ci riferiremo ai comandi con **letsencrypt-auto** assumendo che si scelga di clonare il repository.

Run

Eseguire il client è molto semplice. È sufficiente invocare il comando:

\$./letsencrypt-auto

E verremo guidati durante il processo di issuing dei certificati.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

erver

Client

Security

The protocol

Cert revocation

erts

oss Signing

otuo

Requirements

ownload

Run

Plugin

Renewal

Update

Conclusions

awbacks esources

Apache

Se si vuole configurare **Apache** per utilizzare i certificati che vengono generati, è possibile utilizzare il comando

```
$ ./letsencrypt-auto --apache -d example.com -d www.example.com
```

Indicando con --apache che si vuole configurare Apache e con -d i vari domini per cui si sta richiedendo un certificato.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Server

Client

Protocol

Challenges

Cert revocation

erts ov

Cross Signing

Setup

Requirements Download

Run

Plugins

Renewal Undate

Screens

Conclusions

awbacks sources

Contacts

Durante la prima interazione ci verrà chiesta la nostra **email** per i contatti e ci verrà chiesto di accettare i **Terms of service**.

<mark>È poss</mark>ibil<mark>e saltare</mark> questi passaggi tramite i seguenti flag

\$./letsencrypt-auto --email admin@example.com --agree-tos

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

oci vci

Client

Protocol

Security

The protocol

Cert revocation

erts

Cross Signing

Cross Signing

Conviromente

Requirements

Run

Plugin

Plugins

Update

Screens

conclusions

esources

Contacts

Durante la prima interazione ci verrà chiesta la nostra **email** per i contatti e ci verrà chiesto di accettare i **Terms of service**.

È possibile saltare questi passaggi tramite i seguenti flag

\$./letsencrypt-auto --email admin@example.com --agree-tos

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

`on/or

Client

. .

- "

Challenges
The protocol

Cert revocation

erts

V

Cross Signing

etup

Requirements

Run

Plunin

Plugins

Update

Screens

Conclusions

esources

Plugins

Plugin	Α	ı	Descrizione
Apache	Υ	Υ	Richiede ed installa automaticamente i certi-
			ficati su Apache 2.4 (Debian based)
Standalone	e Y	Ν	Avvia un webserver standalone sulla porta
			80/443
Stan dalone	e Y	Ν	Ottiene il certificato andando a scrivere
			all'interno della root di web server già attivo
Manual	Υ	Ν	Fornisce i comandi da eseguire per ottenere
			un certificato su un'altro web server
Nginx	Υ	Υ	Richiede ed installa automaticamente i certi-
			ficati su Nginx (sperimentale)

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

certonly

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Plugins

È possibile utilizzare i plugin con il supporto per l'authentication (Y nella colonna A) per ottenere solamente i certificati senza effettuare l'installazione degli stessi.

certonly

È possibile utilizzare i plugin con il supporto per l'authentication (Y nella colonna A) per ottenere solamente i certificati senza effettuare l'installazione degli stessi.

È sufficiente indicare l'opzione certonly nella linea di comando.

Standalone example

Ad esempio tramite il comando

\$./letsencrypt-auto --standalone-supported-challenges \
http-01 certonly -d example.com

Si avvia un server standalone sulla porta 80 e si otterrà il certificato per il dominio example.com

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

erver

Client

Security

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Plugins

Plugins

Renewal

Screens

Conclusions

awbacks sources

/etc/letsencrypt

/etc/letsencrypt.

Il client andrà a salvare i certificati e le chiavi dentro la cartella

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

/etc/letsencrypt

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Il client andrà a salvare i certificati e le chiavi dentro la cartella /etc/letsencrypt.

Dentro guesta cartella andranno a finire sia i certificati che le chiavi pubbliche/private. È quindi FONDAMENTALE fare un backup della cartella e mantenerla in un luogo sicuro.

I certificati si troveranno dentro la cartella /etc/letsencrypt/live/example.com/, sono link simbolici che verranno aggiornati ad ogni rinnovo dei certificati.

/etc/letsencrypt

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

I file che andremo a trovare sono:

privkey.pem Chiave privata del certificato. Da non condividere ΜΑΙΙ

cert.pem Certificato del server (quello che viene inviato al client).

chain.pem Elenco dei certificati intermedi delle C.A. collegati al certificato.

fullchain.pem Elenco dei certificati intermedi delle C.A. collegati al certificato, più il certificato stesso.

Revoke

Per revocare un certificato è sufficiente invocare l'opzione revoke

\$ / letsencrypt-auto revoke --cert-path example-cert.pem

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Why

Server

Client

Protoco

Conumity

The protocol

Cert revocation

Certs

Cross Signin

Cross Signin

Poquiromonto

Requirements

Download

Plugins

Revoke

Renewal

Update Screens

Conclusions

rawback: Resources

Revoke

Per revocare un certificato è sufficiente invocare l'opzione revoke

\$ /.letsencrypt-auto revoke --cert-path example-cert.pem

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Revoke

Renewal

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

....

01:---

......

Protocol

Security

The protocol

Cert revocati

Certs

Cross Signing

etup

Requirements

Download __

Run Plugins

Revoke

Renewal

Update

analuaian

rawbacks

L'operazione di rinnovo è molto semplice, e può essere effettuata semplicemente invocando il comando **letsencrypt**, senza parametri.

E inoltre possibile impostare flag quali --renew-by-default per effettuare il rinnovo senza nessuna interazione da parte

dell'uten

In questo modo è possibile schedulare un task su **cron** per il rinnovo automatico dei certificati prima dei 90 giorni.

Renewal

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

L'operazione di rinnovo è molto semplice, e può essere effettuata semplicemente invocando il comando **letsencrypt**, senza parametri.

È inoltre possibile impostare flag quali --renew-by-default per effettuare il rinnovo senza nessuna interazione da parte dell'utente.

modo è possibile schedulare un task su **cron** per il tomatico dei certificati prima dei 90 giorni. Intro Sponsors

History

Server

Client

rotocol

Security

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Run

Plugins Revoke

Renewal

Screens

Conclusions

sources

Renewal

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

L'operazione di rinnovo è molto semplice, e può essere effettuata semplicemente invocando il comando letsencrypt, senza parametri.

<u>È inoltre possibile impostare flag quali --renew-by-default per</u> effettuare il rinnovo senza nessuna interazione da parte dell'utente.

In questo modo è possibile schedulare un task su **cron** per il rinnovo automatico dei certificati prima dei 90 giorni.

Renewal

Update

È importante tenere il client aggiornato, in quanto si tratta di una beta pubblica.

Per Debian sid/stretch:

\$ sudo apt-get update && sudo apt-get upgrade

Per tutti gl<mark>i altri:</mark>

\$ cd letsencryp

\$ git pul

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

Server

Client

rataaa

rotocol

ecurity

The protocol

Cert revocatio

erts

er is

Cross Signing

etup

Requirements

Download

Plugins

Revoke

newal

Update

Conclusions

)rawbacks

Update

Let's encrypt! Certificati SSL per tutti! Nicola Corti

Update

È impo<mark>rtante</mark> tenere il client aggiornato, in quanto si tratta di una beta pubblica.

Per Debian sid/stretch:

\$ sudo apt-get update && sudo apt-get upgrade

Update

Certificati SSL per tutti! Nicola Corti

Let's encrypt!

È importante tenere il client aggiornato, in quanto si tratta di una beta pubblica.

Per Debian sid/stretch:

\$ sudo apt-get update && sudo apt-get upgrade

Per tutti gli altri:

\$ cd letsencrypt

\$ git pull

Update

General usage

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

0....

Histo Why?

Server

Client

rotocol

- ...

Challenges
The protoco

Cert revocat

Certs

DV Cross Signino

Cross Signin

Requirements

Requirements

Run

Plugins

levoke

Update

Conclusions

esources

Nella stragrande maggioranza dei casi, sarà sufficiente invocare il comando **letsencrypt** e farsi guidare dall'interfaccia grafica da terminale

Let's Encrypt ci guiderà durante tutti i processi di generazione/rinnovo di ogni certificato. Sarà sufficiente rispondere alle domande che ci vengono chieste.

Troppi parametri da ricordare renderebbero poco snello il processo automatico di letsencrypt, ma al tempo stesso permettono molta flessibilità e permettono di includere letsencrypt dentro script.

General usage

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

Client

Protocol

Security

The protocol

Cert revocati

erts

Cross Signing

Requirements

Requirements Download

Run

Plugins Revoke

Update

Conclusions

awbacks

Nella stragrande maggioranza dei casi, sarà sufficiente invocare il comando **letsencrypt** e farsi guidare dall'interfaccia grafica da terminale

Let's Encrypt ci guiderà durante tutti i processi di generazione/rinnovo di ogni certificato. Sarà sufficiente rispondere alle domande che ci vengono chieste.

Troppi parametri da ricordare renderebbero poco snello il processo automatico di letsencrypt, ma al tempo stesso permettorio molta flessibilità e permettono di includere letsencrypt dentro script.

General usage

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Spons History Why?

Client

Protocol

Security Challenges

The protocol

Cert revocatio

Cert revocatio

DV

Cross Signing

Requirements

Requirements Download

> Run Plugins

> > enewal

Update

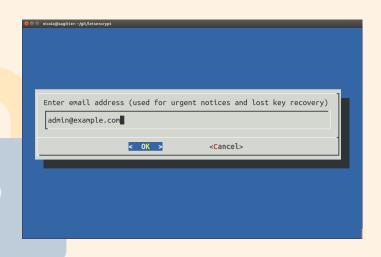
Conclusio

awbacks sources

Nella stragrande maggioranza dei casi, sarà sufficiente invocare il comando **letsencrypt** e farsi guidare dall'interfaccia grafica da terminale.

Let's Encrypt ci guiderà durante tutti i processi di generazione/rinnovo di ogni certificato. Sarà sufficiente rispondere alle domande che ci vengono chieste.

Troppi parametri da ricordare renderebbero poco snello il processo automatico di letsencrypt, ma al tempo stesso permettono molta **flessibilità** e permettono di includere letsencrypt dentro **script**.



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

1110

vviiy

lient

rotocol

ecurity

The protocol

Cert revocation

Certs

Cross Signing

etup

equirements

Download

Run

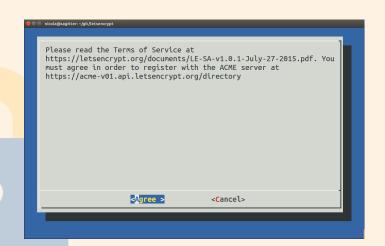
Plugins Rovoko

enewal

Update Screens

an alumian

Drawbacke



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor

Why?

Jilent

Protoco

Consider

The protocol

Cert revocati

Certs

Cross Signing

Cross Signing

octup

Requirements

ownload

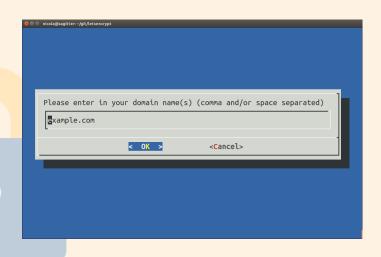
Plugins

Revoke

Update

Screens

Conclusions



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Screens

```
nicola@sagitter: ~/git/letsencrypt
Make sure your web server displays the following content at
http:// /.well-known/acme-challenge/S-phkbW1bo ZS2MDmtZzvPKvOgsDpuGN0DH
9YdSshi0 before continuing:
S-phkbW1bo ZS2MDmtZzyPKvOqsDpuGN0DH9YdSshi0.8K2NX9Rba6j230BnmRz0OsNfrWrBM1Ur8cGV
6aY2IFc
If you don't have HTTP server configured, you can run the following
command on the target server (as root):
mkdir -p /tmp/letsencrypt/public html/.well-known/acme-challenge
cd /tmp/letsencrypt/public html
printf "%s" S-phkbW1bo ZS2MDmtZzvPKvOqsDpuGN0DH9YdSshi0.8K2NX9Rba6i230BnmRz0OsNf
rWrBM1Ur8cGV6aY2IFc > .well-known/acme-challenge/S-phkbW1bo ZS2MDmtZzvPKvOgsDpuG
N0DH9YdSshi0
# run onlv once per server:
$(command -v python2 || command -v python2.7 || command -v python2.6) -c \
'import BaseHTTPServer, SimpleHTTPServer: \
s = BaseHTTPServer.HTTPServer(('', 80), SimpleHTTPServer.SimpleHTTPRequestHandle
r); \
s.serve forever()"
Press ENTER to continue
```

Let's encrypt! Certificati SSL per

Nicola Corti

History

Server

леп

rotocol Recurity

The protocol

Cert revocation

erts

V

Cross Signing

Setup

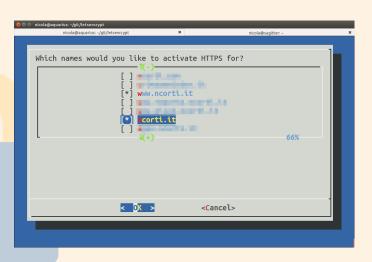
Requirements

Run

Plugins Revoke

Update

Screens



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

HISTOR

Why?

llient

Protocol

Security

Thereses

Cert revocatio

Certs

Cross Signing

Catua

Requirements

Run

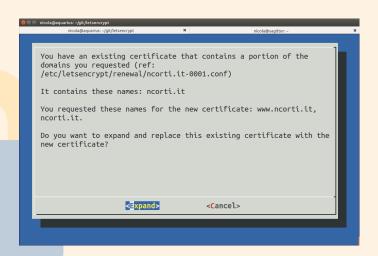
Plugins

Revoke Renewal

Update Screens

1100110

DITCIUSIONS



Let's encrypt! Certificati SSL per

Nicola Corti

Intro

Sponsors

Mbv2

Server

lient

Protocol

Recurity

The protoco

Cert revocat

erts

Cross Signing

etup

Requirements

Run

Yugins Revoke

Update

Screens

Conclusions

Drawbacks

- Nessun supporto per Organization Validation o Extended Validation, troppo complessi da automatizzare.

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Drawbacks

- Nessun supporto per Organization Validation o Extended
 Validation, troppo complessi da automatizzare.
- Nessun supporto per le wildcards (*.example.com), forse in futuro.
- Challenges solo tramite HTTP (public beta), supporto DNS ancora assente.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History Why?

erver

Client

rotocol

Challenges The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

ownload un

Plugins

evoke enewal

Update

onclusions

Drawbacks

- Nessun supporto per Organization Validation o Extended
 Validation, troppo complessi da automatizzare.
- Nessun supporto per le wildcards (*.example.com), forse in futuro.
- Challenges solo tramite HTTP (public beta), supporto DNS ancora assente.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

erver

Client

Protocol

Challenges The protocol

Cert revocation

erts v

/ oss Signino

etup

Requirements

lun

Plugins

Renewal Update

Screens

Conclusions

Resources

- How it works https://letsencrypt.org/howitworks/
- Tech details https://letsencrypt.org/howitworks/technology/
- Read the docs https://letsencrypt.readthedocs.org/
- Community board https://community.letsencrypt.org/
- Code https://github.com/letsencrypt/
- Mailing lists
 - Client https://groups.google.com/a/letsencrypt.org/ forum/#!forum/client-dev
 - Server https://groups.google.com/a/letsencrypt.org/ forum/#!forum/ca-dev
 - ACME (IETF) https://www.ietf.org/mailman/listinfo/acme

Nicola Corti

ntro

Histor Why?

Why?

CHEIIL

otocol

Challenges
The protocol

Cert revocation

erts v

Cross Signing

equirements

ownload

Plugins

Renewal

Screens

Conclusions

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

Intro

History

server

Client

rotocol

Security

The protocol

erts

DV

Gloss aigilii

Requirements

Run

Plugins

Renewal Undate

Screens

Conclusions