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

Histo Why?

Server

Client

......

Challenges

Cert revocation

Certs

Cross Signin

Setup

Requirements

Run

Plugins

Revoke

Update

Screens

Conclusions

rawback: Resources



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro



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

Spons

History

Server

Clien

Protocol

Challenges

The protocol

Cert revocati

Certs

Cross Signing

Setup

Requirements

Download

Plugins

Revoke

Renewal

Update

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**.
- 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

Sponsors

vviiy:

Olion

......

rotocol

Challenges
The protocol

Cert revocati

Certs

Cross Signing

etup

Requirements

Run

Plugins

Revoke

Update

Screens

onclusions

rawback: Resources



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

Sponsors History

Server

Clien

Protocol

Challenges

The protocol

Certs

Cross Signing

etup

Requirements

Run

Plugins

Renewal

Screens

Conclusions

awbacks 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

Intr

Sponsors

Server

Client

Protocol

Challenges

The protocol

Cert revocation

Certs

Cross Signing

Setup

Requirements

Run

Plugins

Renewal

Screens

Conclusions

awbacks 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

Intr

Sponson History

Server

Client

rotocol

Challenges The protocol

Cert revocatio

erts ov

Cross Signing

Setup

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions

esources

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

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

Intr

IIILIU

History

.

. .

lient

otocol

Security

The protocol

erts

Cross Signing

etup

Requirements

lun taataa

lugins evoke

Renewal

Update

nelusions

rawbacks

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

History

Server

Client

rotocol

1010001

Challenges
The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Download

Plugins

Revoke

Update

icreens

onclusions

esources

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

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 II 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

- In	tr	

History

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

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

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

....

Histor

Server

Client

rotocol

Security

The protocol

erts

Cross Signing

Requirements

Requirements

Run

Plugins Revoke

Renewal

Screens

Conclusions

awbacks

	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 II 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

History

en/er

Client

rotocol

Challenges

The protocol

Cert revocation

erts v

Cross Signing

Requirements

Requirements Download

Run Plugins

Plugins Revoke

Renewal Update

Screens

Conclusions

rawbacks

2012	Iniziato il	progetto	dentro	Mozil	la
2012	II II Ziato II	progetto	uentio	WIOZII	ıa

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

ı		+	ú	
	ı			
		۰		

History

Server

Client

rotocol

Challenges The protocol

Certs

Cross Signing

Setup

Requirements

Run Plugins

Revoke

Update

Screens

Conclusions

rawbacks

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

i	ĺ	ı	ú	
	ſ			

History

Server

Client

rotocol

Challenges The protocol

Certs

DV Cross Signing

Setup

Requirements

Run Plugins

Revoke Renewal

Update

creens

onclusions

awbacks

2012	Iniziato il	progetto	dentro	Mozilla
_0.2	111121460 11	progetto	acritio	

- 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

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

- ► Free
- Automatico

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

- ► Free
- Automatico
- Open

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

- ► Free
- Automatico
- Open
- Sicuro

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

- ► Free
- Automatico
- Open
- Sicuro
- Trasparente

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro



Server

Let's Encrypt! Certificati SSL per tutti!

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

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

https://github.com/letsencrypt/boulder

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson

History Why?

Server

Clien

TOLOCOL

Security

The protocol

Cert revocation

Certs

Cross Signing

etup

Requirements

Download

Run

Plugins

Renewal

Update

Screens

onclusions

Jrawbacks 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 HTTPS che espone un'interfaccia RESTful

https://github.com/letsencrypt/boulder

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

Server

Client

rotocol

Security

The protocol

Cert revocatio

Certs

Cross Signing

etup

Requirements

Download

Run Pluains

Plugins Revoke

Renewal

Screens

Conclusions

rawback: 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 HTTPS che espone un'interfaccia **RESTful**

https://github.com/letsencrypt/boulder

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History Why?

Server

Client

rotocol

Security

The protocol

Cert revocation

erts

Cross Signing

etup Requirements

Requirements

Run

Plugins

Renewal

Update

onclusions

)rawbacks

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 HTTPS che espone un'interfaccia **RESTful**

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

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History Why?

Server

Client

Protocol

Security

The protocol

Cert revocation

DV

Cross Signing

Requirements

Requirements Download

Run

Plugins Rovoko

Renewal

Screens

Conclusions

awbacks esources



Client

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Client

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

Sponsor

Sanyar

Client

Client

Protocol

Security

The protocol

Cert revocation

Certs

Cross Signi

etun

Requirements

Requirements

Run

Plugins

evoke enewal

Update

onclusions

rawback: Resources

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

History Why?

Client

Protoco

Security

The protocol

ert revocatio

/

oss Signing

Requirements

Requirements

Run

Plugins

enewal

Update

Conclusions

sources

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 Sponsor

Server

Client

Protocol

- "

The protocol

erts '

ss Signing

tup

Requirements

Run

Plugins

Renewal 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 server: apache ed nginx.

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Why

Server

Client

0110111

rotocoi

Security

The protocol

Cert revocati

erts

OV ___

Cross Signing

etup

Requirements

Download

Plunins

Plugins

Renewal

Screens

Conclusions

Resource

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 server: apache ed nginx.





Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Server

Client

rataaa

Protocol

The protocol

Cert revocation

erts v

Cross Signing

Requirements

Download

Plugins

Renewal Update

Screens

Drawbacks

sources



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Protocol

Certificati SSL per tutti! Nicola Corti

Let's Encrypt!

otro

Sponsor

Sarvar

Clien

CHEIL

Protocol

PIOLOCOI

Security

The protocol

Cert revocation

Certs

DV

Cross Signii

etup

Requirements

Download

Run

Plugins

levoke

Update

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.

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

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 necessariamente HTTPS.

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Server

Clien

Protocol

Consumbs

The protocol

Cert revocation

OV

Cross Signing

Requirements

Requirements Download

Run

Plugins

enewal pdate

Screens

Conclusions

awbacks esources

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

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 necessariamente attraverso **HTTPS**.

Sponsors History

Histor Why?

Clie

Protocol

Security

The protocol

erts

V

ss Signing

etup eauirements

Requirements Download

> Run Plugins

> Plugins Revoke

Renewal

Screens

Conclusions

awbacks esources

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

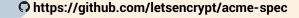
R. Barnes Mozilla J. Hoffman-Andrews EFF J. Kasten University of Michigan July 21, 2015

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.



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Why?

Client

Protocol

The protocol

Cert revocatio

DV

Cross Signing

Requirements

Download Run

Plugins

Renewal Undate

Screens

Conclusions

Orawbacks Resources

Il protocollo ACME ci permette di eseguire tre operazioni:

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

Sponsor

Why

Serve

Clier

D.-+--

Protocol

Security

The protocol

Cert revocatio

Certs

Cross Signing

Setup

Requirements

Download

Run

Plugins

Revoke

pdate

onolugion

_ . .

rawback: Resources

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. Revocare o Rinnovare un certificato per il dominio example.com

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Hist

Serve

Clien

Protoco

1 101000

Challenges

Cert revocation

Certs

Cross Signing

Potun

Requirements

Requirements

Run

Plugins

Revoke

Update

nolucion

onclusions

rawback: Resources

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

Wh

Clien

Protoco

1 101000

The protoco

Cert revocati

erts

ov Oross Signin

Cross Signing

Setup

Requirements

Download Run

Plugins

Revoke

Update

icreens

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 tutti!

Nicola Corti

Intro

Histo Why?

Protoco

Security

The protoco

Cert revoca

Certs

V rnee Sinnii

etup

Requirements

Run

Plugins

enewal

Update Screens

Conclusions

esources

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.

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

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.

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Security

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?

Protocol Security

Challenges The protoo

Cert revocat

V ...

V ross Sianina

oss Signing

etup

Requirements

Run

Plugins

enewal

Update

Conclusions

awbacks esources

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

History Why?

erver

llent

Protocol

ecurity

Challenges

Cost rouncation

Jert revocation

DV

Cross Signing

---i-----

Requirements

lownload

Nuri Plugins

evoke

enewal ndate

reens

onclusions

Orawbacks Resources

Challenges

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

	<u> </u>
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).

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Server

D---4---

Protocol Security

Challenges The protocol

erts

DV Cross Signing

etup Requirements

Run Plugins

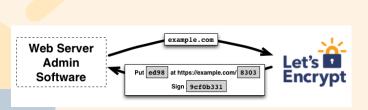
evoke

Update Screens

Conclusions

awbacks esources

Domain Validation

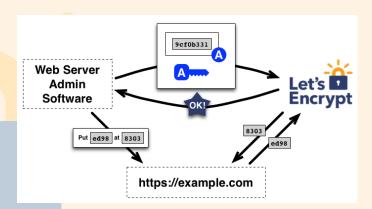


Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

The protocol

Domain Validation



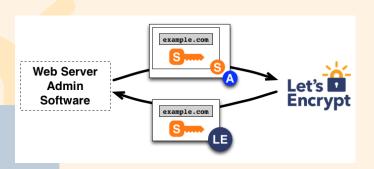
Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Protocol

The protocol

Certificate Issuance



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor Why?

Server

lient

Protocol

Security

The protocol

Cert revocation

Certs

ross Signing

etup

Requirements

Download

Run

Plugins Revoke

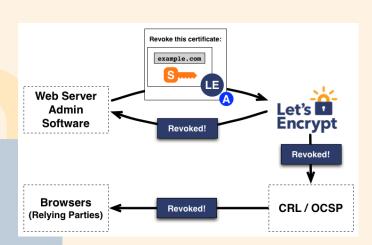
Renewal

Update Scroons

onclusions

Drawback

Certificate Revocation



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Server

llent

Protocol

Security

The protocol

Cert revocation

erts

V Pross Signing

etup

Requirements

Run

Plugins

Renewal Update

. . .

Conclusions

esources



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson

Why?

Server

lient

MEHL

rotocol

San and a side of

Challenges

The protocol

Cert revocation

Certs

DV Canan Cinni

Oross Signi

etup

Requirements

Download

Zun

Plugins

Revoke

Renewal

Update

nelucione

Drawbacks

Resources

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

Certs DV/

DV Certificates

Certificati SSL per tuttil Nicola Corti

Let's Encrypt!

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.



Certs DW

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.

In questo modo possiamo evitare errori quali:

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

Why

liont

Client

rotocol

nallenges

Cert revocati

Certs

Cross Signing

Setup

Requirement

Download

Run

Plugins Revoke

Renewal

Update

onelucion

Drawbacks

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.

In questo modo possiamo evitare errori quali:



Let's Encrypt! Certificati SSL per

Nicola Corti

Intro

Histo

Sanyai

Client

Protoco

Security

The protocol

Cert revocatio

Certs

Cross Signing

Setup

Requirements

Run Plugins

Revoke

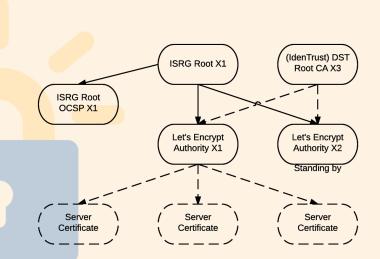
Update

Screens

Conclusions

Drawback Resource:

Cross Signing



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

Differre

rotocol

Challenges

Cert revocation

Certs

DV Cross Signing

tup

Requirements

un funine

Plugins Revoke

Update

Screens

Conclusions

awbacks sources

Validity

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Certs

Cross Signing

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

Validity

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Certs

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 tutti!

Nicola Corti

I certificati <mark>h</mark>anno 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**.

Sponsors

History Why?

01.

Client

Protocol

The protocol

Cert revocati

Certs

DV Cross Siani

Cross Signing

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions

sources



Setup

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Setup

Requirements

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

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.

Requirements

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Server

Client

).........

.....

The protocol

Cert revocation

erts

DV

Cross Signing

Setup

Requirements

Requiremen

Download Run

Plugins

Revoke

Update

onclusions

awbacks sources

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 OS Debian based: **Ubuntu 12.04+** e **Debian 7+**

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Server

lient

rotocol

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Download

DOWING

Plugins

Revoke

Update

Update Screens

onclusions

Resources

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** assumenco che si scelga di clonare il repository.

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

Nicola Corti

Setup

Download

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

ntro

Sponsors

Why?

erver

Client

Protocol

Security

The protocol

Cert revocation

Certs

DV DV

Cross Signing

Setup

Download

Download

Run

Plugins

Revoke

Update

onclusions

rawbacks

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.

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

ro

Sponsors History

Server

lient

rotocol

1010COI

Challenges The protocol

Cert revocation

erts

DV Cross Signing

Cross Signing

Setup

Download

Run

Run

Revoke

Renewal Update

Conclusions

rawbacks

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

Sponsors

Histo Why!

JEI VEI

Client

Protoco

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Requiremen

Download

Run Plugins

Plugins Revoke

Renewal Update

Screens

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

Histor Why?

Server

Client

Protocol

Challenges
The protocol

Cert revocation

erts

Cross Signing

Setup

Requiremen

Download

Run Plugins

kevoke Kenewal

Update Screens

Conclusions

awbacks 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**.

<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?

JEI VEI

Client

Protocol

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Requirement

ownload

Run Plugins

Plugins

Renewal

Update Screens

Conclusions

rawback lesources

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 tuttil

Nicola Corti

Setup

Run

Plugins

Plugin	Α	ı	Descrizione
Apa <mark>che</mark>	Υ	Υ	Richiede ed installa automaticamente i certi-
			ficati su Apache 2.4 (Debian based)
Sta ndalo	ne Y	Ν	Avvia un webserver standalone sulla porta
			80/443
Webroot	Υ	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

ntro Sponsors

Server

Client

otocol

Challenges The protocol

ert revocation

DV

Cross Signing

Setup

ownload un

Plugins

Revoke

Update

onclusions

sources

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.

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Plugins

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 tuttil

Nicola Corti

Setup

Plugins

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

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Plugins

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

Dentro questa 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.

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Plugins

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

Dentro questa 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.

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

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Plugins

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

I file che <mark>and</mark>remo a trovare sono:

privkey.pem Chiave privata del certificato. Da non condividere MAI!

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.

Sponsors

History

erver

liont

TOLOCOI

Challenges
The protocol

Cert revocation

OV Proce Signing

Cross Signing

Setup

Download

Plugins

Renewal

Conclusions

awbacks

Revoke

Per revocare un certificato è sufficiente invocare l'opzione revoke

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Setup

Revoke

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

Sponsors

Histo

erver

Client

FIOLOCOI

Challenges

Cert revincation

erts

DV Cross Signing

Cross Signing

Setup

Requirement

Download

Run

Revoke

Renowal

Update

Conclusions

rawback: Resources

Renewal

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson History

^ - - · · · · · ·

Client

Protoco

Protocol

Challenges The protocol

Cert revocati

Certs

DV

Cross Signing

Setup

Requiremen

Download Run

Run Pluains

Renewal

Update

Screens

Lonciusions

esources

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

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

Sponsors

0----

Client

Jilent

rotocol

Security

The protocol

Cert revocation

DV

Cross Signing

Setup

Requiremen

Run

Plugins Revoke

Renewal

Update Screens

Conclusions

sources

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.

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

Sponsors

Histor Why?

Server

Client

Protocol

Challenges

The protocol

Cert revocation

DV

Cross Signing

Setup

Requiremen

Run Plugins

Renewal

Update

Conclusions

awbacks sources

Update

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Setup

Update

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

Update

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

Setup

Update

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

Per Debian sid/stretch:

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

Update

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

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

Per Debian sid/stretch:

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

Per tutti gli altri:

beta pubblica.

\$ cd letsencrypt

\$ git pull

Setup

Update

General usage

Let's Encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Update

Nella stragrande maggioranza dei casi, sarà sufficiente invocare il com<mark>ando letsencrypt</mark> e farsi guidare dall'interfaccia grafica da terminale.

General usage

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

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

Let's Encrypt ci seguirà 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.

Sponsors

Histo

Caniar

Client

rotoco

rotocoi

The protocol

Cert revocati

erts

Cross Signing

Setup

Requiremen

Run

Plugins Revoke

Update

Screens

Conclusions

sources

General usage

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

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

Let's Encrypt ci seguirà 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**.

Sponsors

Histor Why?

Why?

lient

Jlient

Protocol

Challenges

Cert revocatio

erts

Cross Signing

Setup

Requireme

Run

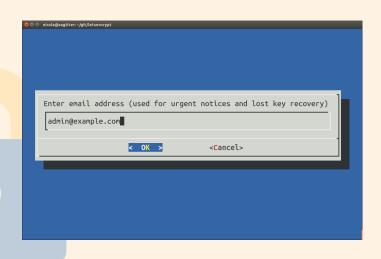
Plugins Revoke

Update

Update Screens

onclusions

awbacks sources



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

HISU

lient

otocol

010001

curity

The protocol

Cert revocation

Certs

Cross Signing

Setup

Requirement

wnload

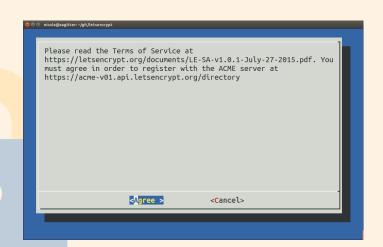
Plugins

Revoke

Update

Screens

onclusions



Let's Encrypt! Certificati SSL per

Nicola Corti

Intr

Sponso

HISTOI

Server

Client

Protoco

curity

The protocol

Cert revocatio

erts

Cross Signing

Setup

Requiremen

Download

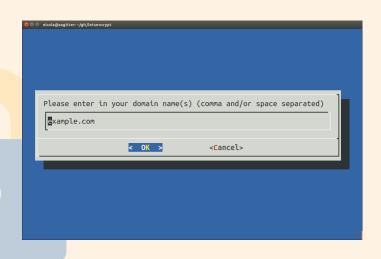
Run Pluains

Revoke

Update

Screens

onclusions



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

HISU

llient

otocol

ecurity

The protocol

Cert revocation

Certs

Cross Signing

Setup

Requirement

wnload

un

riugins Revoke

Renewal

Screens

onclusions

Drawbacks Posouroos

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 Why?

JCI VCI

JIEHL

Protocol

Challenges
The protocol

Cert revocatio

- -----

OV

Cross Signing

Setup

Requireme

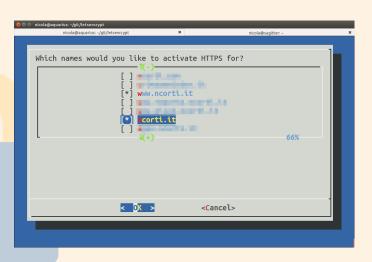
Run

Plugins Revoke

Update

Screens

Drawbacks



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponsor

Histor

Why?

Niont

MEHIL

Protocol

Security

The protocol

Cert revocatio

erts

Cross Signing

Setup

Poguiromon

Requirement

Download

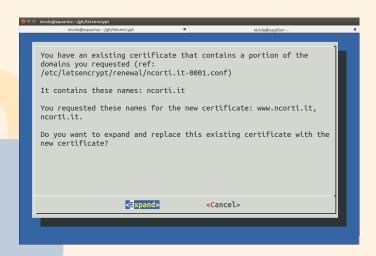
Plugins

Revoke

Update

Screens

onclusions



Let's Encrypt! Certificati SSL per

Nicola Corti

Intro

Sponsors

History

0----

lient

Protoco

Conumity

The protocol

Cert revocation

erts

Cross Signing

Setup

Requireme

Download Run

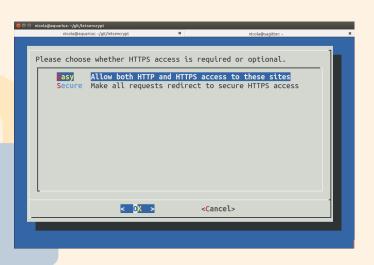
Plugins

Renewal

Update Screens

an alumian

- . .



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

HISTOI

Server

Client

Protoc

1 101000

Security

The protocol

Cert revocation

Certs

Cross Signing

Setup

Setup

Requireme

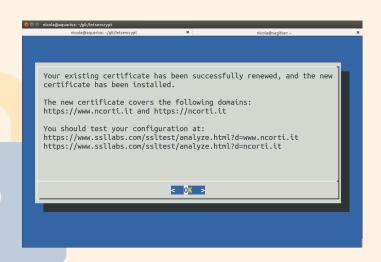
Run

Revoke

Update

Screens

Conclusions



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson

Histor

Client

5110110

Protoco

ecurity

The protocol

Cert revocation

Certs

Ornee Sinning

Gloss algring

Setup

Requiremen

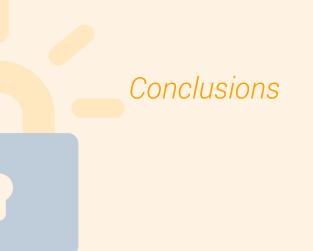
Download Run

Plugins Revoke

Update

Screens

Conclusions



Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Conclusions

Drawbacks

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

Nes<mark>sun supp</mark>orto 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

.....

CHEIL

rotocoi

Security

The protocol

Cert revocatio

erts

Cross Signing

etup

Requirements

wnload

Plugins

Revoke

enewal ndate

Update Screens

Conclusions

Drawbacks Resources

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?

CIVCI

Jilent

rotocol

Challenges The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

lun

Plugins

voke newal

Update

Conclusions

Drawbacks

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 tuttil

Nicola Corti

Conclusions

Drawbacks

Server

Client

POTOCOI Security

The protocol

Cert revocation

v v

Cross Signing

etup

equirements ownload

ın

lugins evoke

Renewal Update

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

Domande...?

- o @cortinico
- റ @cortinico

Slides realizzate con LTEX Beamer.
La seguente presentazione è rilasciata sotto licenza

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



Sorgenti su https://github.com/cortinico/gulp-letsencrypt

Let's Encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

HEHL

rotocol

Security

The protocol

ert revocation

/

Cross Signing

Requirements

Download

Plugins

Plugins

Update

Conclusions