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! 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

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

rawback lesources



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

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

Sponsor History

Server

Clien

Protocol

Challenges The protocol

The protocol

Cert revocatio

Certs

Cross Signing

etup

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions

awbacks esources

Sponsors

Chi sta supportando il progetto?

Platinum













Gold





facebook

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

2012 Iniziato il progetto dentro Mozilla

11/201/ 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

IIIII

History

O a a a

Jient

otocol

ecurity

The protocol

Zert revocatio

erts

Cross Signing

Setup

Requirements

un

Plugins

Renewal

Update

nnelusions

Prawbacks Resources

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

History

Server

Client

rotocol

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Run

Plugins

Revoke

Update

Screens

onclusions

rawbacks

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!)

<mark>12-20</mark>15 Public beta!

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

History

erver

Client

rotocol

Challenges

Cert revocatio

erts

Cross Signing

Poquiromento

Requirements

Download

Plugins

Revoke

Update

Screens

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 tutti!

Nicola Corti

....

Histor

Server

Client

rotocol

Challenges

The protocol

Cert revocatio

erts

Cross Signing

Requirements

Requirements

Run

Plugins Revoke

Renewal 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

	ı	ú	ı	١

History

vvily?

..

Olicile

TOLOCOI

Challenges The protocol

Cert revocation

erts

Cross Signing

Requirements

Requirements Download

Run Plugins

Plugins Revoke

Renewal Update

Screens

Conclusions

rawbacks

2012	Iniziato il	nrogetto	dentro	Mozil	la
2012	II II Ziato II	progetto	uentio	IVIUZII	Ia

- 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

r	ı	ä	+	v	
L					

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!)

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

lr	ï	t	r	Ċ

History

Server

Client

rotocol

Challenges The protocol

Certs

Cross Signing

Setup

Requirements

Run

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!

- Free
- Automatico
- Open
- Sicuro
- ▶ Trasparente

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Why?



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 certificati

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

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor

Server

Clien

TOLOCOL

Security

The protocol

Cert revocation

) - ---k --

Certs

Cross Signing

Setun

Requirements

December

Run

Plugins

Revoke

Renewal

Update

naluaiana

_ . .

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

Security

The protocol

Cert revocatio

erts

Cross Signing

etup

Requirements

Download

Plugins

Plugins

Renewal

Screens

Conclusions

esources

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 Why?

Server

Client

rotocol

Security

The protocol

Jert revocati

erts v

Cross Signing

etup

Requirements

Download

Plugins

riugins Revoke

Renewal Update

Screens

Conclusions

esources

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

History Why?

Server

Client

.

Protocol Security

The protocol

Cert revocatio

erts v

Cross Signing

Requirements

Requirements Download

Run

Plugins

enewal

Screens

Conclusions

awbacks sources



Client

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

History Why?

Server

Client

Protocol

1010001

Challenges

The protocol

Cert revocation

Certs

Ornee Sinnin

etup

equirements

ownload

ownload

ugins

Revoke

enewal

Update

Screens

onclusions

Drawback

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.

Let's encrypt! Certificati SSL per tuttil

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/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

awbacks 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.

Ohttps://github.com/letsencrypt/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Caniar

Client

Protocol

Challenges
The protocol

Cert revocation

v v

ss Signing

etup

Requirements

Run

Plugins

Renewal Update

Screens

Conclusions

awbacks esources

Plugins

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





Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Client

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

ilent

Protocol

The protocol

Cert revocation

erts v

Cross Signing

Requirements

Download

Plugins

Renewal Update

Screens

Conclusions

awbacks sources



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Protocol

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

Sponsor

Histo

Server

Clien

Protocol

Protoco

Challenges

Cert revocation

Corto

Certs

Cross Signin

Catum

Roquiromonto

Daniellenis

Run

Plugins

Revoke

enewal

Update

nclusions

Drawback

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 Sponsor

Histor Why?

Clien

Olici

Protocol

Challenges
The protocol

Cert revocation

erts

Cross Signing

Setup

Requirements

Run

Plugins

enewal

Update Screens

Conclusions

awbacks esources

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.

O https://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

Orawbacks Resources

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
- 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

Sponsors

His

Clien

Protoco

1101000

Challenges
The protocol

Cert revocati

Certs

Cross Signing

etun.

Daminomento

Requirements

Run

Plugins

Revoke

Update

Screens

Conclusions

Orawbacks 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

Sponson

vvily?

01:---

Cileii

Protoco

Challenges
The protoco

Cert revocati

orto

Certs

Cross Signing

Setup

Requirements

Download

Run

Plugins

Renewal Undate

Screens

Conclusions

rawback Jesources

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

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 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.

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.

Security

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

erver

lient

Protocol

nourity

Challenges

ert revocation

Jert revocation

DV

Cross Signing

---i-----

Requirements

ownload

Plugins

newal

Jpdate

nclusions

Resources

Il server può, 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).

Sponsors

wny? Server

Protocol Security

Challenges The protocol

Cert revocation

DV Cross Signing

Setup Requirements

Run Plugins

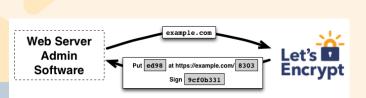
evoke enewal

Renewal Update

Conclusions

awbacks esources

Domain Validation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Hist

Server

Client

Protoco

Security

The protocol

Cert revocation

Certs

Cross Signin

Setup

Requirements

wnload

Plugins

Revoke

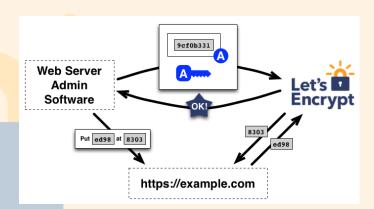
Update

Screens

Conclusions

Resources

Domain Validation



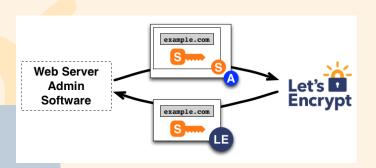
Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Protocol

The protocol

Certificate Issuance



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Histor Why?

Server

lient

Protocol

ecurity

The protocol

Cert revocation

Certs

ross Signing

etup

Requirements

Run

Plugins

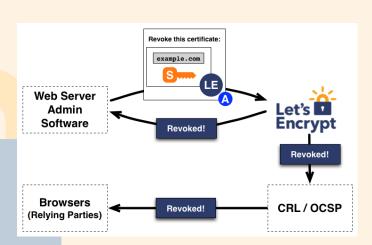
evoke enewal

Update

noluciono

Drawbacks

Certificate Revocation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why?

Server

llent

Protocol

Security

The protoco

Cert revocation

erts

V Cross Signing

etup

Requirements

un

Plugins Revoke

Renewal Update

acens

Conclusions

esources



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

HISTO

Server

lient

lient

rotocol

hallenges

The protocol

Cert revocation

Certs

ov Oross Signi

etup

Roquiromonte

Requirements

ownload

lugins

Revoke

Renewal

Update

nclusions

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

Let's encrypt! Certificati SSL per tutti!

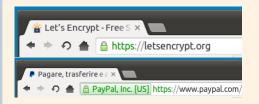
Nicola Corti

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

rotocol

The protocol

Cert revocation

Certs

DV

Cross S

Requirements

Requirements Download

Run Plugins

> evoke enewal

Update

Conclusions

awbacks sources

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

Client

rotocol

curity

The protocol

Cert revocation

Certs

Cross Signing

. .

Requirements

Download

Run

Plugins

Revoke

Update

Screens

Jonelusions

Resource

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

rotocol

ecurity

The protocol

Cert revocatio

Certs

Cross Signing

Setup

Requirements

Nownload Run

Plugins

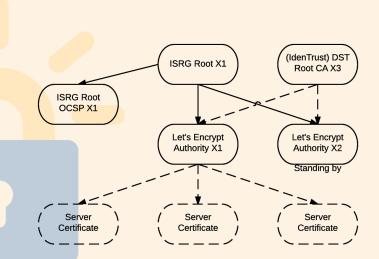
Renewal

Screens

Conclusions

Drawback Resource:

Cross Signing



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Histor Why?

server

Jilent

rotocol

Challenges The protocol

Cert revocation

Certs

Cross Signing

tup

Requirements

lun

Plugins Revoke

Renewal Jpdate

Screens

Conclusions

awbacks sources

Validity

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History Why?

Server

Client

rotocol

.....

Challenges
The protocol

Cert revocati

Certs

Cross Signing

Gross digrilling

setup

Requirements

lownload

un

lugins Revoke

Update

onclusions

awbacks sources

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.

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

di cron

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?

Server

Client

Protocol

Security

The protocol

Cert revocatio

Certs

DV

Cross Signing

Setup

Requirements

Run Plugins

Plugins Revoke

Renewal Update

Screens

Conclusions

awbacks sources



Setup

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Why?

en/er

lient

rotocol

Security

The protocol

Cert revocation

Certs

Certs

Cross Signin

Setup

Jetup

ownload

lownload

un

Plugins

Revoke

Jpdate

Screens

onclusions

Drawbacks

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

Why?

Server

lient

rotocol

Challenges

Cert revocation

Cert revocation

erts

Cross Signing

Setup

Requirements

Download

Run

Plugins

Revoke Renewal

Update

onclusions

)rawback: toenumoe

Requirements

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Histo Why?

Serve

JIEHL

Protocol

Security

The protocol

Cert revocati

erts

Cross Signing

Setup

Requirements

Run

Plugins

Renewal Update

screens

Jonciusions

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Sanyar

lient

rotocol

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Download

DOWNIOU

Run

Revoke

Renewal

Update

nolucion

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

To the transfer of the transfe

Da ora in poi ci riferiremo ai comandi con **letsencrypt-au** assumenc<mark>o che si scelga di clonare il repository.</mark>

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 tuttil

Nicola Corti

Setup

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

rn

Sponsors

Why?

Server

Client

Protocol

Security

The protocol

Cert revocation

erts

DV Cross Signing

Setup

Setup

Download

Run

Plugins

Renewal

Update Screens

Conclusions

rawbacks lesources

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

Sponson

Why

Client

Protoco

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Requiremen

Download

Run

Plugins

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

erts

Cross Signing

Setup

Requiremen

Download

Plugins

Revoke

Renewal Update

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**.

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Setup

Run

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

Intro

Sponsors

enver

Client

Protocol

Security

The protocol

Cert revocatio

erts

OV ...

Cross Signing

Setup

Requirement

ownload

Run Download

Plugins

Renewal

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	Υ	Ν	Avvia un webserver standalone sulla porta
			80/443
Stan dalone	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

rotocol

Challenges The protocol

Cert revocation

DV

Cross Signing

Setup

ownload iun

Plugins

evoke enewal

Update Screens

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

/etc/letsencrypt

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

/etc/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

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**.

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

Intro Sponsors

Why?

Server

Client

CHEIL

rotocol

Challenges

The protoco Cert revocat

erts

Cross Signing

Setup

Setup

Download Run

Plugins

Revoke

Renewal Update

Screens

Conclusions

esources

/etc/letsencrypt

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Sponsors

Server

Client

Protocol

Challenges The protocol

The protocol

Cert revocation

Derts DV

Cross Signing

Setup

Requireme Download

Plugins

Renewal

Conclusions

awbacks

I file che andremo 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.

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

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

Setup

Revoke

Renewal

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson History

^ - - · · · · · ·

Client

......

Protocol

Challenges

The protocol

O - ---

Certs

Cross Signing

Setup

Requiremen

Download

Run

Plugins

Renewal

Update

Screens

Joniciusions

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 tuttil

Nicola Corti

Setup

Renewa

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.

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.

Sponsor

Histor Why?

Server

Client

rotocol

Security

The protocol

Certs _{DV}

Cross Signing

Setup

Requiremen

Run

Renewal

Update

Conclusions

awbacks esources

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.

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:

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

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.

Per Debian sid/stretch:

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

Per tutti gli altri:

\$ cd letsencrypt

\$ git pull

General usage

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

INTLO

Why?

Jilent

rotocol

Security

The protoco

Cert revocat

Certs

Cross Signing

Setup

Requiremen

Run

Plugins

levoke

Update

Conclusions

rawbacks 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 dispondere 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

terminale.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

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

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

Setup

Update

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 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**.

Sponsors

Histo Why?

Server

Client

rotocol

Security

The protocol

Cert revocation

OV .

Cross Signing

Setup

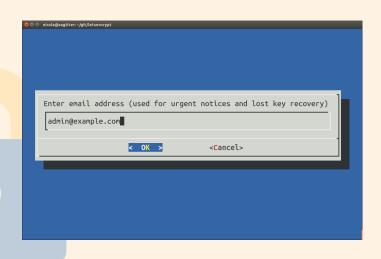
Requireme

Run

Plugins Revoke

Update

Screens



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponso

HIS

Wh

liont

Ofocol

ecurity

Shaheriges The exeternal

Cert revocation

Certs

Cross Signing

Setup

Requirement

wnload

ın

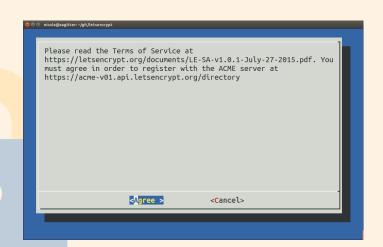
Plugins Rovoko

Renewal

Update Screens

reens

DITCIUSIONS



Let's encrypt! Certificati SSL per

Nicola Corti

Intr

Sponsor

Mhv2

Client

J.11C11C

Protoco

Security

The protocol

Cert revocati

erts

Cross Signing

Setup

Requireme

Download

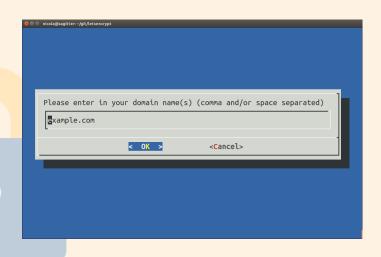
Plugins

Revoke

Update

Screens

conclusions



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponsor

nisu

Wh

Cliont

Ofocol

Challenges

The protocol

Cert revocation

Certs

Cross Signing

Setup

Requirement

wnload

Jn

Plugins

Revoke

Update

Screens

onclusions

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 tutti!

Nicola Corti

Sponsor

Why?

SHELL

rotoco

Security

The protocol

Cert revocatio

v

Cross Signing

Setup

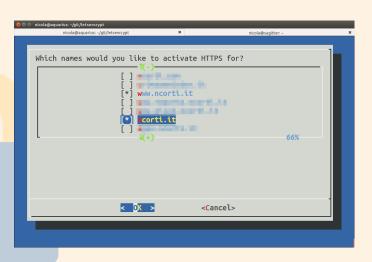
Requireme

Run

Plugins Revoke

Update

Screens



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponsors

Histor

Why?

liont

Protoco

1010001

Challenge

Cert revocatio

erts

Cross Signing

Setup

Poguiromon

Requiremen

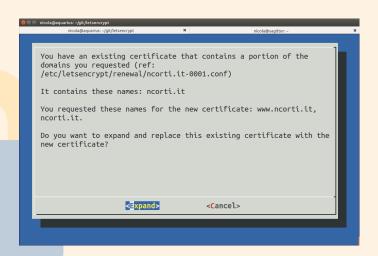
Run

Plugins Revoke

Update

Screens

onclusions



Let's encrypt! Certificati SSL per

Nicola Corti

Intro

Sponsors

HISTOR

Server

lient

rotocol

Conurity

The protoco

Cert revocati

erts

Cross Signing

Setup

Requireme

Download

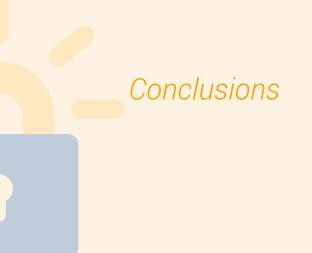
Plugins

Revoke

Update Screens

. .

- . .



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Conclusions

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

Why?

Client

rotocol

Challennes

The protocol

Cert revocation

Cert revocation

Certs

Cross Signing

etup

Requirements

ownload

Run

riugins Revoke

enewal

Update

Conclusions

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?

Jilent

- "

Challenges
The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

ownload un

Plugins

evoke

Update

Conclusions

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

Nhy?

lient

Drotooo

Security

The protocol

erts

rts /

ross Signing

etup

Requirements

Run

Plugins

Renewal Jpdate

Conclusions

Server

Client

Protocol

Challenges

Cert revocation

erts v

Cross Signing

etup

Requirements Download

un fugine

> evoke enewal

Update

Conclusions

Drawbacks 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
- ດ @cortinico

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

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



Let's encrypt! Certificati SSL per

Nicola Corti

Intro

Sponsors

Why

Client

otocol

010001

Challennes

The protocol

errievocauc

erts

oss Signing

equirements

equiternents

Run

Plugins

Revoke

Update

Conclusions