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

Challennee

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

.....

History

Server

lient

rotocol

310001

The protocol

Cert revocation

erts

Cross Signing

Setup

Requirements

Run

riugins Revoke

Update

creens

onclusions

esources

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

v	٠	÷	ř	į
	u		ш	

History

2012 Iniziato il progetto dentro Mozilla

11-2014 Let's Encrypt annunciato pubblicamente

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

III ICI

History

Why?

....

Jilent

rotocol

Challenges

Cert revocatio

erts

Cross Signing

setup

Requirements

Download

Plugins

riugins Revoke

Update

Screens

onclusions

Resources

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**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

Spons

Histor

Server

Client

rotocol

Challenges
The protocol

Cert revocatio

erts

Cross Signing

Setup

Requirements

Run

Plugins Revoke

Renewal

Update

Conclusions

Prawbacks Resources

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

History

/vny?

Minus.

Drotopol

- "

The protocol

erts

Cross Signing

etup

Requirements

Run Pluains

Plugins Revoke

Renewal

Update

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 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

	ı	

2012	Iniziato il	nrogetto	dentro	Mozilla
2012	II IIZIatu II	progetto	uentio	IVIUZIIIC

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

ı	r	ľ	t	r	(

History

Server

Client

rotocol

Challenges The protocol

Certs

DV Cross Signing

Cross Signing

Requirements

Run Plugins

Revoke Renewal

Update

onclusion:

rawbacks

- 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.

Let's encrypt! Certificati SSL per tuttil

Nicola Corti

Server

Architettura

Il sistema di Let's Encrypt si basa su **3 Componenti**: un **server**, un **client** e il **protocollo** che permette a server e client di comunicare.

Il server si chiama **Boulder** ed è scritto interamente in **Go**. Si occupa di gestire tutte le procedure per il **rilascio** e **revoca** dei certificati.

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

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

Run

Plugins

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 HTTP che espone un'interfaccia **RESTful**

https://github.com/letsencrypt/boulder

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

History

Server

Client

Protoco

Popurity

The protocol

Cert revocatio

erts

Cross Signing

etup Requirements

Requirements

Run

Plugins

enewal

Update

.....

Conclusions

awbacks 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

.

10t0col

The protocol

Cert revocation

OV

Cross Signing

Requirements

Requirements Download

Run

Plugins

enewal

Screens

Conclusions

awbacks esources



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

Server

Client

Protocol

Security

The protocol

rts

ss Signing

etup

Requirements

Run

Plugins Revoke

Henewal Update

Screens

Conclusions

sources

Plugins

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

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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histor Why?

.

Client

Client

rotocol

Security

The protocol

Cert revocation

erts

ross Signing

Cross Signing

equirements

Requirements

Download

Plugins

Revoke

Update

Screens

Conclusions

Drawback 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 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

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson

Why?

. . . .

Cileiii

Protocol

Protocol

Challennes

The protocol

Cert revocation

Certs

DV

Cross Signin

etup

Requirements

Download

Run

Plugins

levoke

Update

Greens

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 o **HTTPS**.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

Clien

Olici

Protocol

Challenges The protocol

Cert revocation

erts

Cross Signing

Requirements

Requirements Download

Run

Plugins

enewal

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

Histor Why?

Clie

One

Protocol

Security

The protocol

Cert revocation

/

oss Signing

etup

Requirements Download

Run

Plugins

newal

Update Screens

Conclusions

awbacks sources

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

Nicola Corti

Sponsor

Why?

Client

Protocol

1 1010001

The protocol

Cert revocation

verts DV

Cross Signing

Requirements

Download

Plugins Revoke

Renewal Update

aeens

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

Sponsors

Histo Why

Serve

Clier

. .

Protoco

Challenges

Cert revocatio

Certs

Cross Signing

Setup

Requirements

Download

Run

Run Plugins

Revoke

enewal Ipdate

Screens

onclusions

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 Why

Clien

Protocol

The protocol

Cert revocati

Certs

Cross Signin

Potun

Requirements

Requirements

Run

Plugins

evoke

Update

onclusions

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

Sponsors

Hist Why

Ciler

Protoco

Protocol

Challenges

Cert revocati

Cert revocat

Certs

Cross Signing

Setup

Requirements

Download

Run

Plugins Revoke

Update

Screens

Conclusions

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

Server

Clien

. .

Protoco

Security

The protoco

Cert revoca

Certs

/ Cinni

etup

Requirements

Download

Plugins

Revoke Renewal

Update

Conclusions

rawbacks 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 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

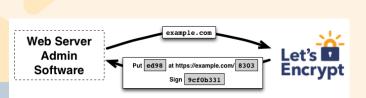
evoke enewal

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

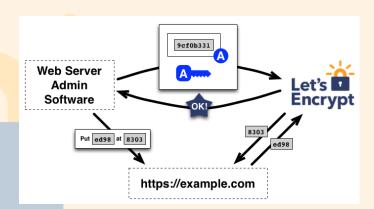
Update

Screens

Conclusions

Resources

Domain Validation



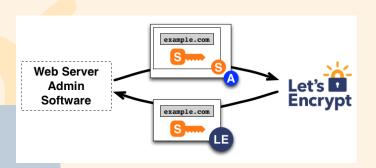
Let's encrypt! Certificati SSL per tutti!

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

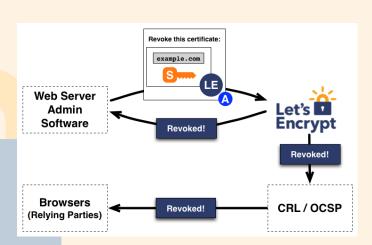
evoke enewal

Update

noluciono

Drawbacks

Certificate Revocation



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

Server

llent

rotocol

Challenges

Cert revocation

erts

OV Oross Signing

Setup

Requirements

Run

Plugins

Renewal Update

acens

Conclusions

esources



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Certs

DV Certificates

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.

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

Why?

erver

Client

Protocol

The protocol

Cert revocation

Cert revocation

Certs

Cross Signin

Setup

Requirements

ownload

un

Plugins

Revoke

lpdate

Screens

Conclusions

Jrawbacks Resources

DV Certificates

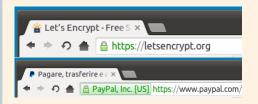
Certificati SSL per tuttil Nicola Corti

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

Sponsors

Why

Client

Protocol

ecurity

The protocol

Certs

OV

Cross Signing

Setup

Requirements

Download

Plugins

Revoke

Update

Screens

Conclusions

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.

In questo modo possiamo evitare errori quali:



Let's encrypt! Certificati SSL per

Nicola Corti

Intro

Hist

Server

Client

Protocol

Challenges The protocol

Cert revocation

Certs

DV Cross Signing

Setup

Requirements

Run

Revoke

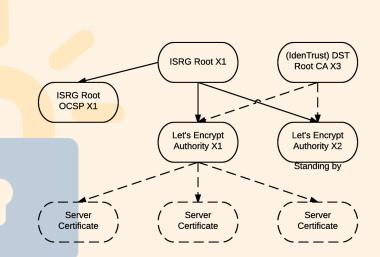
Renewal

Screens

Conclusions

Drawback Resource

Cross Signing



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro Sponsors

Why?

.

JIICHE

rotocol

Challenges The protocol

Cert revocation

Certs

Cross Signing

etup

Requirements

un Iugins

Plugins Revoke

Update

Conclusions

Drawbacks

Validity

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histo Why?

Server

Client

Protocol

Camaita

The protocol

Cert revocati

Certs

Cross Signing

Setup

Requirements

Download

lun

lugins

Update

onclusions

rawbacks esources

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

90-days validity

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

È possibil

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

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

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 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.

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 tuttil

Nicola Corti

Setup

Download

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

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

Histor Why?

Server

Client

Protocol

Challenges
The protocol

Cert revocation

erts

Cross Signing

Setup

Requiremen

Download

Run Plugins

Plugins Revoke

Update

onclusion

rawbacks

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

Cert revocation

erts

Cross Signing

Setup

Requiremen

Download Run

Plugins

Revoke Renewal

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

sei vei

Client

Protocol

Security

The protocol

Cert revocation

erts

Cross Signing

Setup

Requirement

lownload

Run Plugins

Plugins

Renewal

Update

onclusions

rawback: Resources

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)
Sta ndalon	e 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

rotocol

Challenges The protocol

ert revocation

DV

Cross Signing

Setup

ownload un

Plugins

enewal

onclusions

awbacks

certonly

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histo

vvny?

...

JIEHL

rotocol

ecurity

The protocol

erts

erts

DV Cross Signing

Cross Signing

Setup

Requirement

lownload

Plugins

Revok

Renewal

Update

onclusions

esources

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

certonly

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

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

Standalone example

Ad esempio tramite il comando

effettuare l'installazione degli stessi.

\$./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 tuttil

Nicola Corti

Setup

Plugins

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

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 Why

erver

Client

Drotoo

Security

Challenges

Cert revocation

erts

Cross Signing

Setup

octup

Requirements

Run

Plugins

Revoke

Renewal Update

Screens

Conclusions

rawbacks Resources

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

Intro

Sponsors

vviiye

Client

. .

otoco:

ecurity

The protocol

Cert revocati

erts

erts

Cross Signing

Setup

Requiremen

ownload

Run

Plugins Revoke

Revoke

Update

Conclusions

esources

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

Per Debian sid/stretch:

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

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

\$ cd letsencryp

\$ git pul.

Update

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

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

Per Debian sid/stretch:

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

Per tutti gli altri:

\$ cd letsencrypt

\$ git pull

Setup

Update

General usage

Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Histo

Server

Client

rotocol

Security

The protocol

Cert revoca

Certs

Cross Signing

Setup

Requiremen

Run

Plugins

levoke

Update

Conclusions

esources

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

Let's Encrypt ci seguirà 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

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

wny?

Niont

HEHL

rotocol

Security

The protocol

erts

Certs

Cross Signing

Setup

Requiremen

Run

Plugins

enewal

Update

Conclusions

awbacks 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

History Why?

Why

lient

SHELL

rotocol

Challenges

Cert revocatio

Certs

Cross Signing

Setup

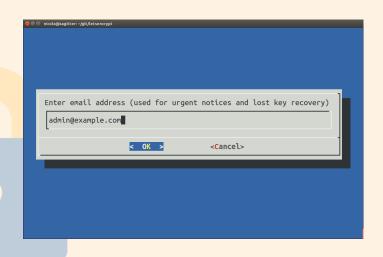
Requireme

Run

Plugins Revoke

Update

Screens



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsor

nisu

Wh

lient

rotocol

ecurity

The protocol

Cert revocation

Certs

Cross Signing

Setup

Requirement

wnload

lun

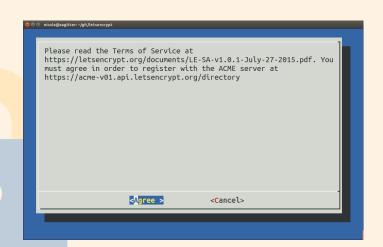
augins Revoke

Henewal Update

Screens

onclusions

Drawbacks Recourses



Let's encrypt! Certificati SSL per

Nicola Corti

Intr

Sponso

HISTOI

Server

Client

100000

hallennes

The protocol

Cert revocati

erts

Cross Signing

Setup

Requiremen

Download

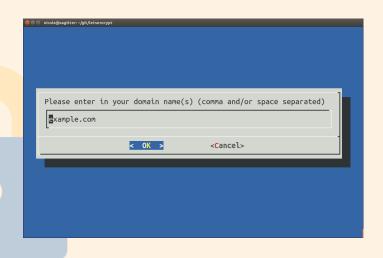
Plugins

Revoke

Update

Screens

onclusions



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponsor

HISU

Wh

liont

.....

Ofocol

curity

The protocol

Cert revocation

Certs

Cross Signing

Setup

equirement:

wnload

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

History Why?

Ment

POTOCOL Security

Challenges
The protocol

Cert revocatio

Cert revocation

OV

Cross Signing

Setup

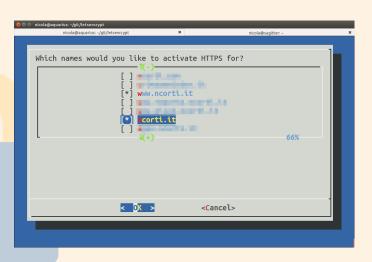
Requireme

Run

Plugins Revoke

Update

Screens



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intr

Sponsor

HISTO

Why?

llient

Protocol

Security

The protocol

Cert revocation

Certs

Cross Signing

Setup

Jetup

Requiremen

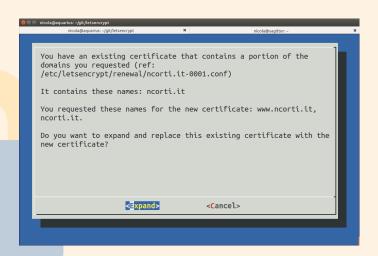
Run

Plugins Revoke

Henewal 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

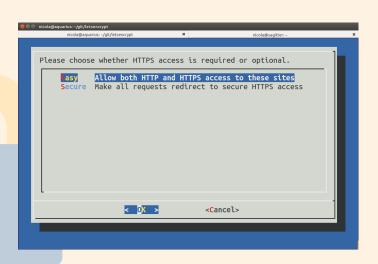
Plugins

Revoke

Update Screens

. .

- . .



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

HISTOI

Sanyar

Client

Protoci

. 101000

The protocol

Cert revocation

erts

Cross Signing

Setup

Requireme

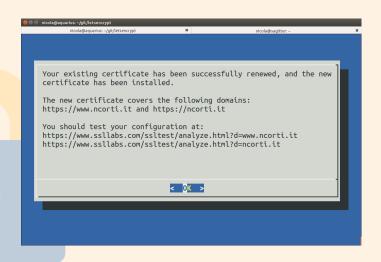
Run Plugins

Revoke

Update

Screens

onclusions



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponson

Histor

DE 1

SHELLE

Protoco

Security

The protocol

Cert revocatio

Certs

Cross Signing

Setup

Danisana

Download

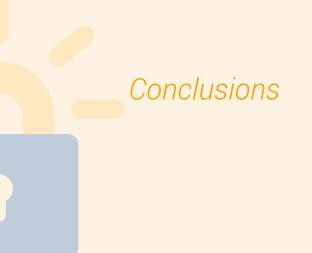
Plugins

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.

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

Why?

NI - - 4

JIICHE

Security

The protocol

Cert revocation

erts v

/ oss Signin

tup

Requirements

Run

Plugins

enewal

Update Screens

Conclusions

Server

Client

Security

The protocol

Cert revocation

V

Cross Signing

etup

ownload

un Iugins

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...?

- ø ncorti.com
 // lipital l
- o @cortinico
- ດ @cortinico

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

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



Let's encrypt! Certificati SSL per tutti!

Nicola Corti

Intro

Sponsors

Why

lient

rotocol

Security

The protocol

Cert revocation

erts

Cross Signing

etup

Requirements

Run

Plugins

Renewal

Update

Conclusions