HTTPS e siti P.A. locali: *matrimonio impossibile*?

Antonio Giovanni Schiavone

Chi sono?

Antonio Giovanni Schiavone

Dottore in Informatica

Esperienze professionali in:

- Consiglio Nazionale delle Ricerche (Pisa / Roma)
- Agenzia per l'Italia Digitale
- Agenzia Nazionale per i Servizi Sanitari Regionali
- Commissione di Vigilanza sui Fondi Pensione

Mi sono occupato di:

- Accessibilità & Usabilità Web
- Semantic Web & Data Visualization
- Identità Digitali & Sicurezza

Di cosa parleremo oggi

Discuteremo dei risultati del progetto Municipality2Https, un progetto di ricerca volto a:

- Effettuare l'analisi della sicurezza delle comunicazioni da/verso i siti web dei circa 8000 Comuni italiani.
- Fornire una valutazione complessiva delle sicurezza di tali comunicazioni per ogni singolo comune.
- Aggregare i dati raccolti su scale geografiche di varia grandezza.
- Offrire un quadro esaustivo dello stato della sicurezza dei siti web dei Comuni Italiani
- Proporre spunti per un irrobustimento della sicurezza digitale delle Pubbliche amministrazioni locali.

Comunicazioni sicure sul Web

Cos’è l’HTTP

L’Hyper Text Transfer Protocol (HTTP) è un protocollo di comunicazione generalmente utilizzato per il trasferimento delle pagine web in internet.

- I dati che passano tramite HTTP non sono criptati (detti anche «in chiaro»)
- Le comunicazioni sono intercettabili da parte di chiunque.
- Non vi è certezza sull’identità delle parti, e quindi i dati sono alterabili da parte di chiunque.

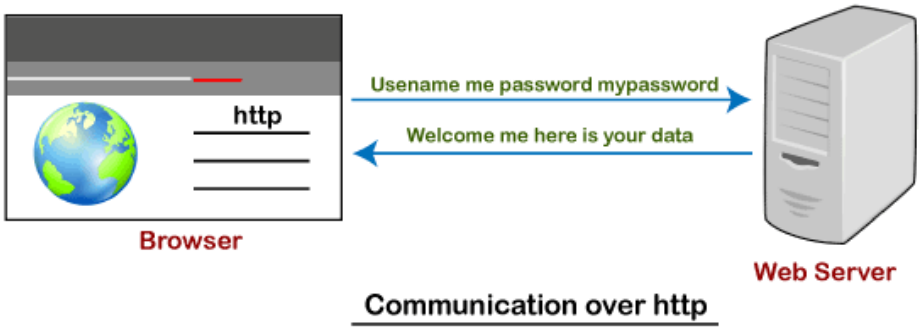
Cos'è l'HTTPS?

L'HTTPS (HTTP Secured) è una variante protocollo HTTP.

- Prima di effettuare lo scambio di dati, viene creato un canale di comunicazione criptato attraverso lo scambio di certificati.
- E' garantita l'identità delle parti e la riservatezza dei dati.

L'uso dell'HTTPS è vitale in tutte quelle situazioni in cui è richiesto un certo grado di sicurezza e privacy (e-commerce, e-mail, home banking, identità digitali), ma oggigiorno ha ricadute positive anche in altri ambiti (ad es. Search Engine Optimization).

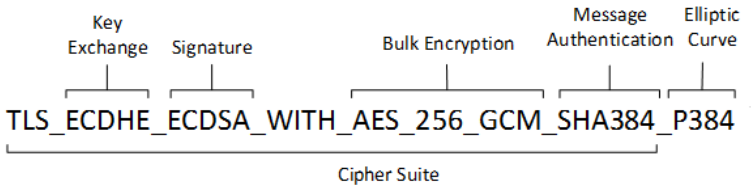
HTTP vs HTTPS



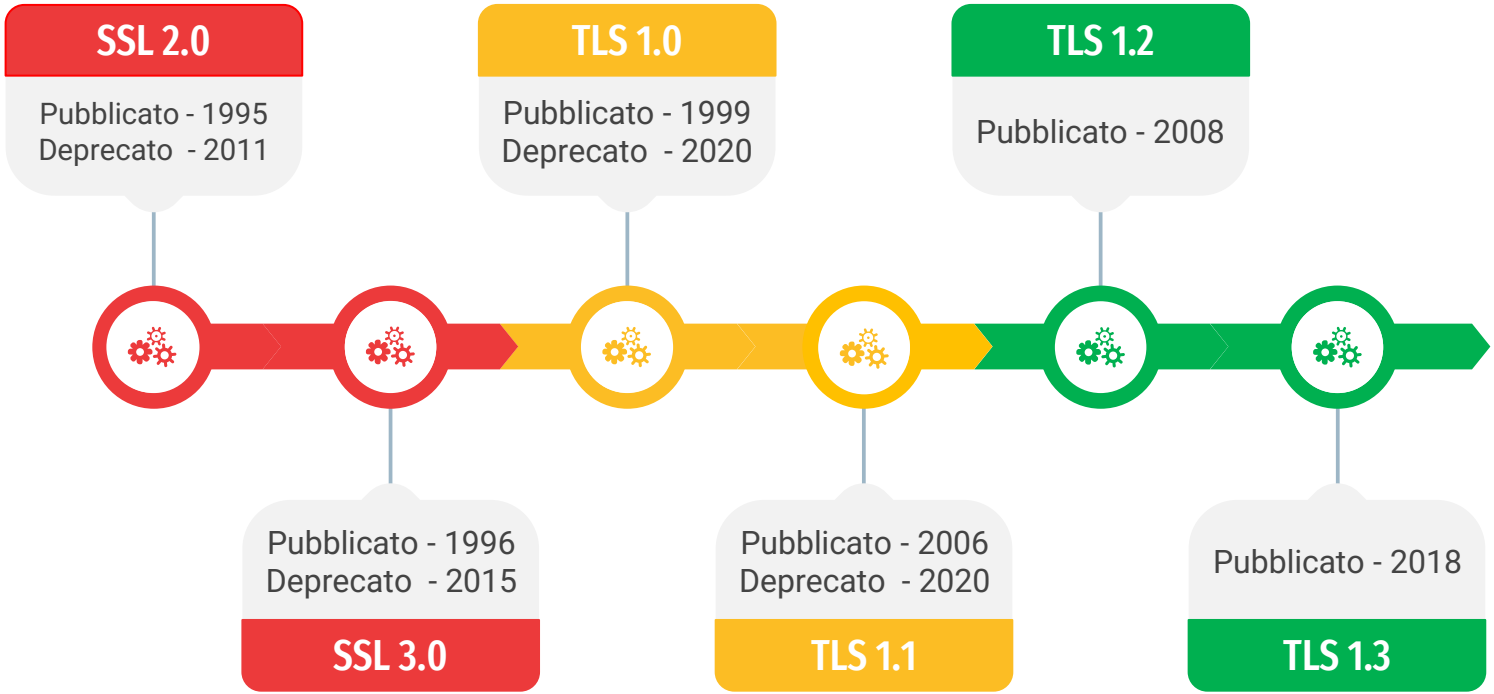
HTTPS, Protocolli crittografici e Cipher Suites

Per instaurare un canale criptato, l'HTTPS utilizza a sua volta:

- Protocolli crittografici (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3)
- Suite di cifratura (Cipher Suites), ovvero insiemi di algoritmi utilizzati per implementare i protocolli crittografici. L'insieme di algoritmi che costituisce una suite comprende tipicamente:
  - un algoritmo per lo scambio delle chiavi crittografiche,
  - un algoritmo di crittografia
  - un algoritmo di message authentication code



Evoluzione degli algoritmi crittografici



Le Raccomandazioni AgID

Le “Raccomandazioni AgID”

Contrariamente ad altri ambiti (ad es. la «Legge Stanca» per l’accessibilità dei siti web), non esiste una legge che obblighi le Pubbliche Amministrazioni all’uso del protocollo HTTPS.

L’unico documento ufficiale su tale tema sono le «Raccomandazioni AgiD in merito allo standard Transport Layer Security (TLS)» pubblicate nel Novembre 2020 dall’Agenzia per l’Italia Digitale e dal Ministero per l'Innovazione tecnologica e la Digitalizzazione (MID).

Tale documento fornisce un insieme di «best practices» in merito ai protocolli di sicurezza e alle Cipher Suite da utilizzare, definendo tre distinte configurazioni del protocollo HTTPS.

Le Configurazioni AgID

Modern

TLS 1.3
Durata del certificato: 90 gg

CipherSuite:
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Certificato:
- ECDSA (P-256)

Curva TLS:
- X25519
- prime256v1
- secp384r1

Intermediate

TLS 1.3 o TLS 1.2
Durata del certificato: 90 - 366gg

CipherSuite:
- Come configurazione Modern
- Altre 8 suite specifiche per TLS 1.2

Certificato:
- ECDSA (P-256)
- RSA 2048 bit

Curva TLS:
- X25519
- prime256v1
- secp384r1

Old

Tutto ciò che non rientra nella configurazioni Modern o Intermediate

Altri aspetti dell'HTTPS

Vi sono altri aspetti di una implementazione HTTPS che le Raccomandazioni AgID non prendono in considerazione o danno per scontato:

- Il certificato deve essere valido (non scaduto, né revocato).
- Il certificato deve essere intestato al dominio del sito che lo utilizza.
- Non devono essere presenti vulnerabilità note (ad es. POODLE, DROWN, etc).
- E' consigliabile la redirezione automatica da HTTP a HTTPS.

Il progetto Municipality2Https

La piattaforma di analisi

Al fine di effettuare l'analisi dei siti dei Comuni italiani, è stata sviluppata la piattaforma di analisi, denominata MunicipalityEvaluator, aventi le seguenti caratteristiche tecniche:

- Sviluppata in Java
- Elaborazione MultiThread per miglioramento performance di analisi
- Dati di input e risultati di anali memorizzati su database relazionale Postgresql
- Parte dell'analisi svolta tramite API di un servizio esterno gratuito (SSL Labs di Qualsys)

Sistema di valutazione

Per consentire il confronto fra comuni diversi e l'aggregazione dei dati su base geografica, la piattaforma applica un sistema di valutazione per la generazione di un indice sintetico numerico, basato sulla dei punteggi con l'aggiunta di alcuni bonus/malus.

Esito	Punteggio
Soddisfacimento della configurazione "Modern"	90
Soddisfacimento della configurazione "Intermediate"	65
Soddisfacimento della configurazione "Old"	40
Assenza di implementazione protocollo HTTPS	0

Sistema di valutazione

Per consentire il confronto fra comuni diversi e l'aggregazione dei dati su base geografica, la piattaforma applica un sistema di valutazione per la generazione di un indice sintetico numerico, basato sulla dei punteggi con l'aggiunta di alcuni bonus/malus.

Casistica	Bonus/Malus
Presenza di redirect da HTTP a HTTPS	+10
Presenza di un Certificate Name Mismatch	-10
Utilizzo di un certificato scaduto	-10
Supporto ad un protocollo vecchio (TLS 1.0 e/o 1.1)	-5 per ogni protocollo
Supporto ad un protocollo obsoleto (SSL 2.0 e/o 3.0)	-10 per ogni protocollo
Presenza di una vulnerabilità SSL/TLS nota	-10 per ogni vulnerabilità

Risultati della valutazione

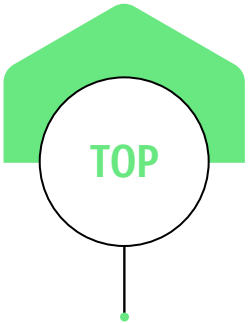
Risultati generali

- Nessun comune rispetta i criteri delle configurazioni Modern o Intermediate
- 791 comuni (10% circa) NON hanno implementato il protocollo HTTPS
- 2610 comuni (37% circa) NON hanno implementato il redirect da HTTP a HTTPS
- 1.916 comuni (27% circa) hanno un Certificate Name Mismatch
- 308 comuni (4% circa) utilizzano un certificato scaduto

Risultati generali

- 3.231 comuni (45% circa) supportano ancora almeno uno protocollo “vecchio” (TLS 1.0 e/o TLS 1.1).
- 280 comuni (4% circa) supportano uno o più protocolli obsoleto (SSL 2.0 e/o SSL 3.0).
- 343 comuni (5% circa) sono affetti da almeno una vulnerabilità nota.

I Comuni Top&Flop

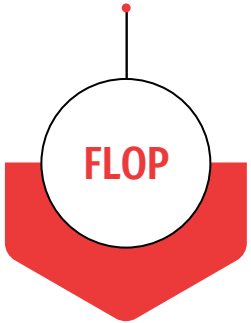


50 Punti

4.494 comuni che implementano il redirect da HTTP a HTTPS, hanno configurazione Old e non hanno malus

Piccolo comune ligure che ha collezionato tutti i malus previsti

-60 Punti



Risultati Nazionali e MacroRegionali

- Il punteggio Medio nazionale è 34,23 punti (SD 17,53)
- Il punteggio per MacroRegioni è il seguente:

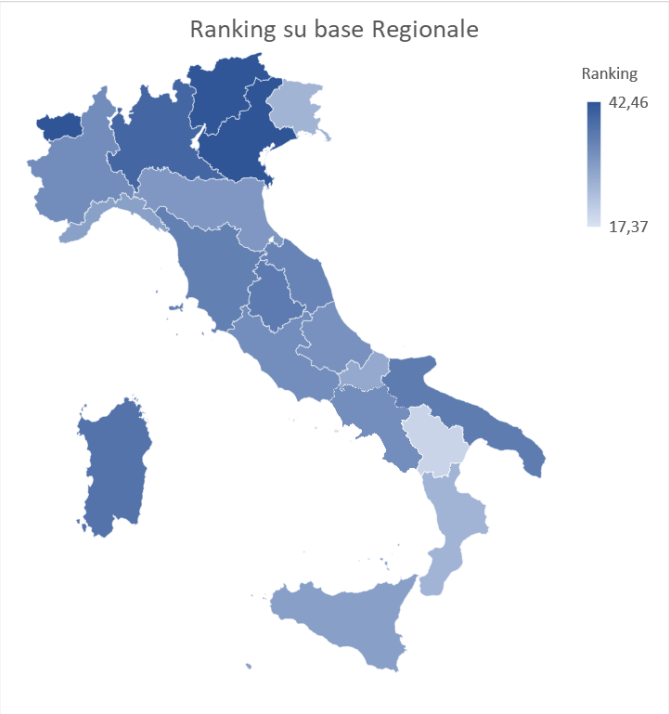
MacroRegione	Punteggio
Nord-Est	38,32
Nord-Ovest	36,22
Isole	33,64
Centro	33,49
Sud	29,23

Risultati Regionali

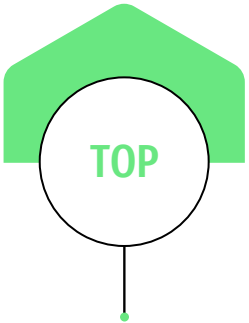
Regione	Punteggio
Veneto	42,46
Valle d'Aosta	42,43
Trentino Alto Adige	42,34
Lombardia	39,42
Sardegna	37,21
Umbria	35,71
Puglia	35,54
Toscana	34,87
Marche	34,14
Piemonte	32,59

Regione	Punteggio
Lazio	32,44
Campania	32,15
Abruzzo	31,78
Emilia Romagna	30,70
Sicilia	29,36
Liguria	29,29
Molise	27,61
Friuli Venezia Giulia	25,72
Calabria	25,68
Basilicata	17,37

Risultati Regionali

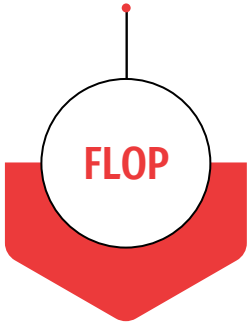


Le Province Top&Flop



Macerata 49,27
Treviso 47,98
Venezia 46,25

Potenza 16,30
Prato 11,43
Ravenna 7,78



Conclusioni

HTTPS e siti P.A. locali

- Quello fra HTTPS e P.A. locali è un «matrimonio» possibile, ma al momento alquanto tormentato.
- Pesano soprattutto il supporto a protocolli vecchi ed il mancato redirect da HTTP a HTTPS.
- Grave anche la presenza di Certificate Name Mismatch, spesso dovuto a fornitori «poco accorti».
- Con qualche notevole eccezione, la «crisi coniugale» colpisce soprattutto nelle regioni del Sud.
- Le «Raccomandazioni AgID» sono lontane dallo status quo.
- Sarebbe auspicabile una legge che imponga requisiti minimi di sicurezza digitale.

Grazie

Per la vostra Attenzione

Web site: www.antoniogiovannischiavone.it - **Email:** antonio.giovanni.schiavone@ieee.org - **Twitter:** @AGSchiavone - **Linkedin:** www.linkedin.com/in/antoniogiovannischiavone