

TrustAsia SSL White Paper



www.trustasia.com



01 | BACKGROUND

In the era of network information, the security of data is related to the future development of enterprises. With the rapid development of Internet technology, events caused by security problems are more and more frequent. Enterprise websites, especially those involving user privacy information, face the potential risk of being attacked by the network at all times. Website disclosure and fraud events are growing up and cause bad impact, which has serious harm to the interests of the owner and its customers.

The American "prism"-hacking program monitors the public's network activity since 2007.

The Law of the people's Republic of China on Network Security shall be implemented to clearly strengthen the protection of personal information.

2013

2016

Time Warner was phishing and more than 300,000 customer data leaked.

2017

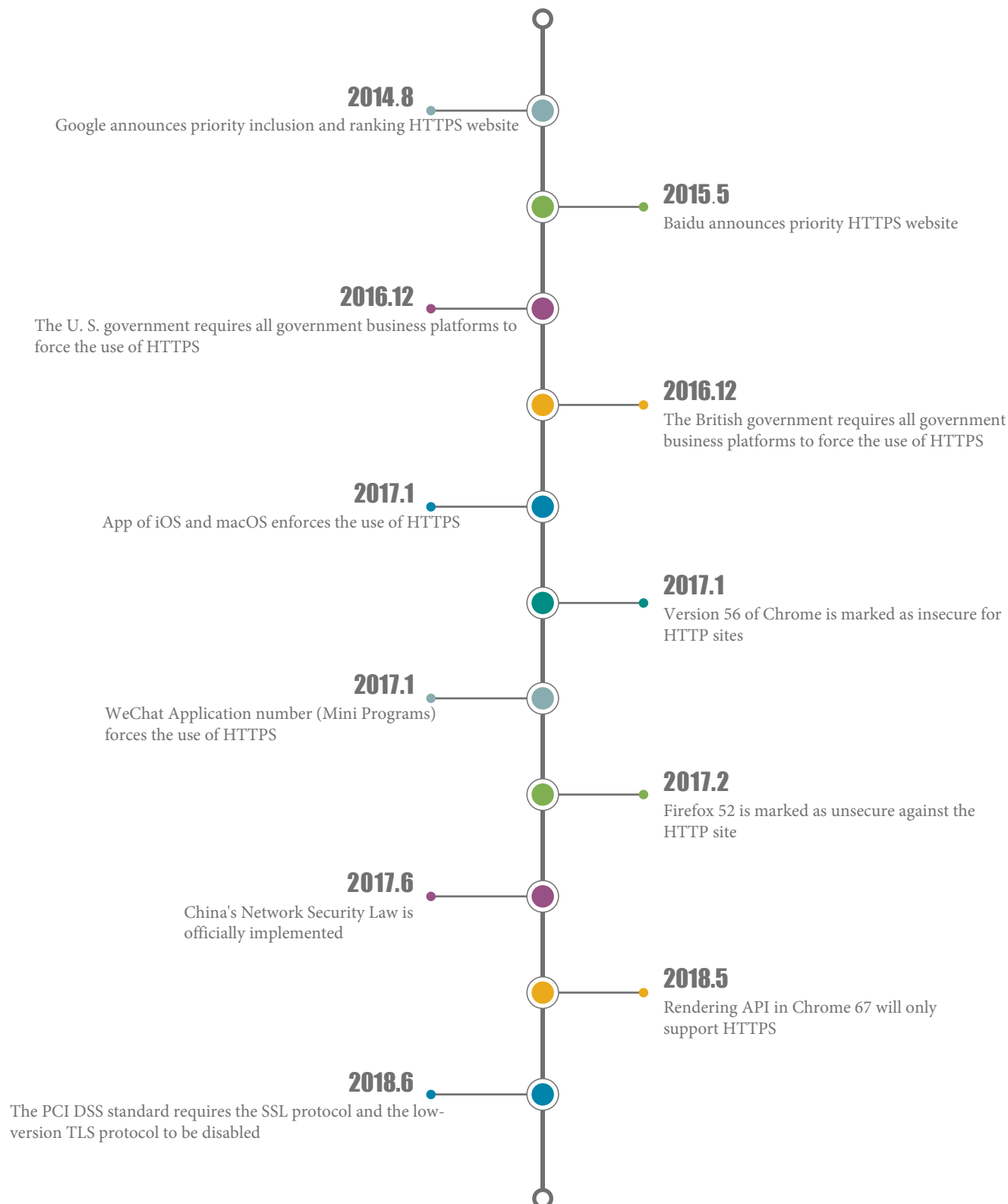
2018

A total of 3 billion user data has been hijacked by traffic, with an illegal profit of over 30 million/ year.

The security of data is related to the future development of the enterprise. The necessary condition for the survival of the enterprise is to make the customer have a sense of trust in the product and establish a trust bridge with the customer. Using SSL certificate is one of the effective methods to improve the security of website, prevent information from being stolen or tampered, hijacked by operator traffic, phishing website and protecting data security.

02 | INDUSTRY TRENDS

The global HTTPS encryption traffic is growing, and HTTPS encryption is listed as a mandatory standard in the requirements of data security in all areas of the world. It can be seen that the installation of SSL certificate is an important step in the safe operation of the future website, regardless of the importance of the development of the SSL certificate industry at home and abroad. Therefore, the enterprise site should install the SSL certificate in time to comply with the development, and select an authoritative trusted CA to apply for SSL certificate.





03 | PRODUCT INTRODUCTION

TrustAsia SSL certificate is a local brand SSL certificate established by TrustAsia Technologies, Inc. which combines the network environment and usage habits of domestic enterprises and enterprises. It provides enterprises and individuals with secure and reliable encrypted data transmission and authentication services.

04 | PRODUCT FUNCTION



Confirm the authenticity of the website

Help confirm the true identity of the site, like the identity card of the website in the Internet world.



improve search engine ranking

Well-known search engines have given priority to sites that support HTTPS to quickly improve the ranking of websites.



improve that access speed of the Web site

Fully compatible with HTTP2.0 protocol, fast and dynamic loading of web content, for the website service speed.



International Trust and Signature

Place an international trusted signature in the website, visitors can use the signature link to learn about the security and trusted status of your site.



Transmission Security protects user Privacy

Establish a secure information transmission encryption channel between the website and the client to protect the user's privacy data.



Ensure data integrity

HTTPS is used to encrypt communication to prevent data from being stolen and tampered with in the process of transmission to ensure data integrity.



Prevent traffic hijacking

Effectively prevent Internet service provider traffic hijacking, insert advertising.



Improve the brand image and credibility of the company.

The browser address bar displays the HTTPS security lock, indicating that the security of the site is reliable, and the brand image and credibility of the company are enhanced.

More effects

- Apple developer ATS standard. From January 1, 2017, Apple announced that all applications on the AppStore must be enabled with App Transport Security (ATS) secure communications technology.
- The WeChat applet requires HTTPS encryption and must use the SSL certificate.
- It is applied to the security communication design of Information system Security level Protection.

SSL Certificate

Digital Certificate is the cornerstone of Internet Security



05 | WHY CHOOSE TRUSTASIA

Compared with the common brand SSL certificate, TrustAsia brand SSL certificate has many advantages, such as ECC and RSA double encryption algorithm support, enterprise security evaluation, certificate management system, certificate fast issuance, good compatibility and high performance-price ratio.

① ECC/RSA Algorithm Supported

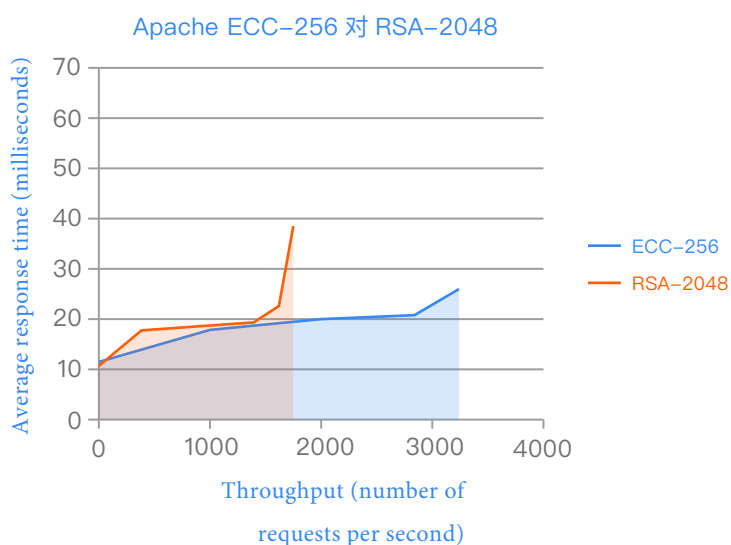
TrustAsia SSL certificate fully supports international ECC and RSA standard encryption algorithm, suitable for user key encryption length.



RSA algorithm: the international standard algorithm, the compatibility is good, the encryption length of 2048 bits is generally adopted, and the performance of the server is high.



ECC algorithm: the Chinese name is elliptic encryption algorithm, the new generation algorithm trend is mainstream, generally using 256-bit encryption length, low consumption for server resources, higher efficiency.



MPKI Certificate Management System



- ✓ Cross-sectoral and regional certificate management
- ✓ Telescopic centralized solution
- ✓ Simplify SSL certificate management throughout the enterprise
- ✓ A better platform for enterprise-class customization



- ✓ Flexible SSL Certificate Management and risk
- ✓ Control Reduced SSL certificate management costs and complexity of SSL certificate management
- ✓ what the heart wishes one's hands accomplish
- ✓ Sub-authority management to eliminate the leakage of certificate information

MySQL Enterprise Edition is a system that can meet the security detection, certificate validity and alarm of multiple HTTPS sites, provide visual rating chart and interactive cross-brand certificate management dashboard, support HTTPS security rating, certificate brand, certificate validity, SSL vulnerability, PCI DSS & ATS compliance monitoring and centralized management, abnormal situations can be alerted by mail, WeChat and telephone. Purchase TrustAsia SSL certificate to provide enterprise version MySQL monitoring service, provide real-time HTTPS monitoring and protection for the website.



Overview of security ratings

The nine ratings of A +, A, A-, B, C, D, E, F, and T are given according to the safety risk



Certificate brand management

Support globally trusted SSL certificate brands, such as DigiCert/Symantec, TrustAsia, Let's Encrypt, etc.



Certificate validity management

The validity period of the certificate shall be subject to hierarchical management, including more than 3 months, 3 months, 2 months and 1 month after expiration.



Certificate Type Management

Classification management is carried out according to the audit type, mainly including EV, OV, DV and unknown.



SSL vulnerability distribution

The monitoring and statistics of related vulnerabilities revealed in SSL protocol, at present, there are 8 related middle and high risk vulnerabilities.



Compliance monitoring

PCI DSS third party payment industry data security standard; ATS application transmission security specification, but also by Mini Programs, Android and other ecological reference









Great Compatibility

Compatibility is related to whether the browser will correctly give web security tips when the user accesses. The TrustAsia root certificate issued by the international top CA organization DigiCert/Symantec supports all the mainstream browsers and mobile devices at present.

List of compatibility of TrustAsia SSL certificates in major browser versions

年

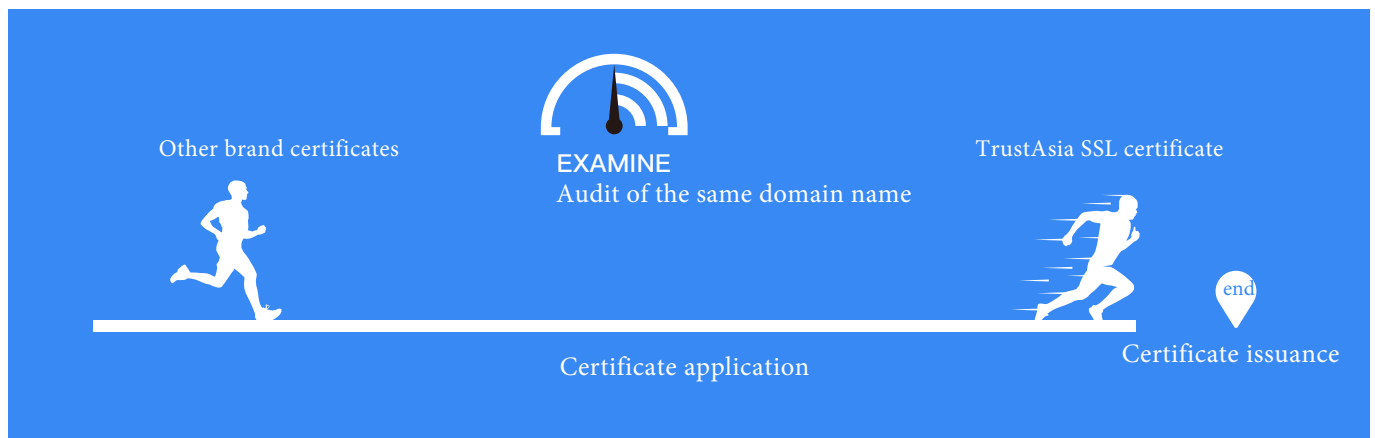
2018.10 以后
2018	17	58-62	64-69	11.1-12	50-55	11.4	9
2017	15-16	51-57	56-63	10.1-11	43-49	10.3-11.2	8
2016	14	44-50	48-55	9.1-10	35-42	9.3-10.2	7
2011-2015	9-11	12-13	4-43	9-47	5.1-9	11.5-34	4.3-9.2
2006-2010	7-8		2-3.6	4-8	3.1-5	10.1	3.2-4.1
2001-2005	6						

IE
Edge
Firefox
Chrome
Safari
Opera
iOS
Android

5 Fastly Issue Certificate

TrustAsia brand for certified domain name certificate application, can be issued in real time.



6 More Services



01 TrustAsia OV SSL Certificate

TrustAsia OrganizationValidation(OV)SSL Certificate, Asian Integrity Enterprise SSL Certificate, or Asian Integrity Organization Verification SSL Certificate. It can provide the maximum SHA256-bit encryption algorithm to ensure the security of online transaction and online shopping of your users. It can not only play the role of website information encryption, but also prove the real identity of the website to the user, so that the user can fully trust your website. . TrustAsiaOVSSL supports single domain name, multi-domain name, and multiple versions of wildcard characters.

Features



Strict enterprise identity information authentication



ECC and RSA dual algorithm support



Whole process technical support service



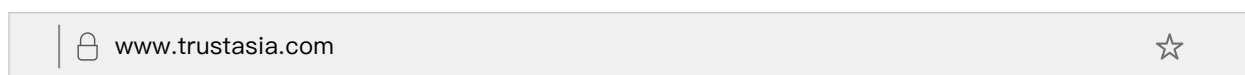
Asian Integrity Certificate Security Program

Applicable object

Enterprise sites, e-commerce sites, electronic post office servers, APP distribution downloads that also meet the requirements of iOS, Google and so on must use HTTPS secure connections.

Browser display

The browser displays a green 'lock' type security message. When you click the Lock icon, you will see the name of the certificate issuing authority.



Internet Explorer



Chrome



Firefox



Safari



Opera

TrustAsia Extended Validation (EV) SSL certificate, Chinese for Asian integrity enhanced SSL certificate, or Asian integrity enhanced organization certification SSL certificate, is issued according to a series of specific standards of X. 509e-certificate. TrustAsia EV SSL is the highest end SSL certificate of the global unified identity authentication standard. It automatically activates the green address bar of the browser and displays the enterprise name of the website operator in the address bar. It is easier for users to identify the real identity of the real website operator and fully trust your website, thus bringing more orders. TrustAsia EV SSL supports single domain name, multi-domain name version.

Features



Authentication of Enterprise identity Information at the highest level



A browser that supports EV and displays the green address bar and company name



ECC and RSA dual algorithm support



Whole process technical support service



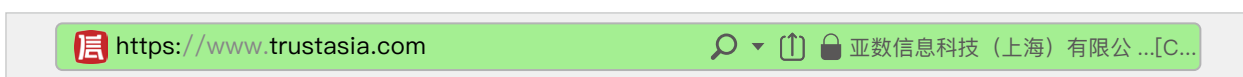
TrustAsia Certificate Security Program

Applicable object

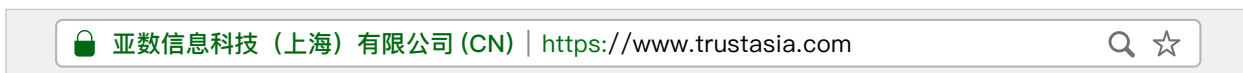
Banks, insurance, financial institutions-related corporate websites, e-commerce sites, APP distribution downloads that also meet the requirements of iOS, Google and so on must use HTTPS secure connections.

Browser display

The browser displays a green address bar, a green lock security flag, and an enterprise name. When you click on the Lock icon, you will see the full company name and the name of the certification authority.



Internet Explorer



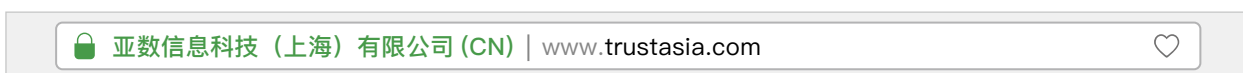
Chrome







Firefox



Safari

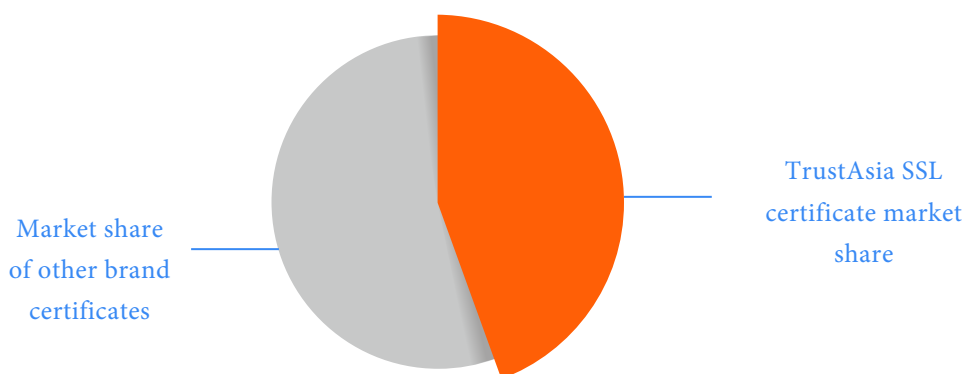


Opera

Certificate type	TrustAsia OV	TrustAsia EV
Trust level		
Security Grade		
SAN (UC) support	✓	✓
Public key algorithm	RSA and ECC	RSA and ECC
encryption strength	Support up to 256 bits.	Support up to 256 bits.
Public key length	RSA (more than 2048)	RSA (more than 2048)
free-to-charge	✓	✓
Installation check	✓	✓
State detection	✓	✓
Supported version	Single domain name, multi-domain name and wild card character	Single and multiple domain names.

TrustAsia SSL certificate market share

According to the scanning report of Netcraft, an internationally renowned SSL market analysis and research platform, the domestic market share of, TrustAsia SSL certificate up to March 2018 is Top1.



07 | SUCCESS CASE

TrustAsia brand SSL certificate has excellent product quality, good after-sales service, loved by users. Hundreds of Chinese enterprises and institutions have applied for TrustAsia SSL certificates, and you are no stranger to the following companies.

well-known enterprise (partial)



电子商务 (部分)



金融支付 (部分)





WeChat public number

Official Website:

www.trustasia.com

Call: 400-880-8600

Customer service email:

support@trustasia.com