What kind of SM2 browser is needed for the cryptography reconstruction?

The cryptography compliance reconstruction is a big thing that must be done in China, and it is a big thing related to national security. One of the important products needed for the cryptography reconstruction is the SM2 browser, so what kind of SM2 browser do users need? What is the difference between the SM2 browser and the commonly used browser? The author wrote an article to clarify these questions today when ZT Browser released a kernel update version.

Everyone can't do their work online without a browser. The top five browsers commonly used by Internet users around the world are Google Chrome, Apple Safari, Microsoft Edge, Opera and Firefox, with market shares of 62.55%, 20.50%, 5.28%, 3.22% and 2.80% respectively, among which Google Chrome, Microsoft Edge and Opera are all developed based on Google's open source Chromium, with a total market share of 71.05%, accounting for an absolute market share, which is why ZT Browser choose the Chromium as kernel.

The author is unable to verify when the product name "SM2 Browser" appeared. Since people call it too much, it becomes a product name. Today I give " SM2 Browser" a formal definition. What is SM2 Browser? The SM2 browser refers to the browser that supports the SM2 algorithm and the SM2 SSL certificate and uses the SM2 algorithm to realize https encryption.

In order to distinguish the top five commonly used browsers in the world, the author suggests that these browsers be collectively referred to as "RSA browsers" to distinguish them from "SM2 browsers". This is the same naming as the name of RSA SSL certificates and SM2 SSL certificates. The RSA SSL certificate refers to the SSL certificate issued by the international algorithm RSA, and the RSA browser is a browser that supports the international algorithm RSA and uses the RSA SSL certificate to realize https encryption. Correspondingly, the SM2 SSL certificate refers to the SSL certificate issued by the SM2 algorithm, and the SM2 browser is a browser that supports the SM2 algorithm and uses the SM2 SSL certificate to realize https encryption. Please note that the RSA algorithm here refers to the general term for implementing the international algorithm https encryption related algorithms, and the SM2

algorithm refers to the general term for implementing the SM2 algorithm https encryption related algorithms, mainly including SM2, SM3 and SM4 algorithm.

To realize the SM2 https encryption, of course, the SM2 browser is inseparable. So, what kind of SM2 browser do users need? What features should a SM2 browser have at least to be called a SM2 browser? To answer these questions, we should refer to international browsers. Since the development of a browser is a huge system project, involving too many international standards and specifications, and considering the compatibility of the HTML specification and the HTTP/HTTPS protocol since the birth of the browser 30 years ago. We must recognize this reality, the only choice to develop a SM2 browser is to develop it based on a mature open-source code. Of course, the first choice is Chromium, because its global market share has reached 71.05%, add the market share of domestic brand browsers, the estimated market share is up to more than 90%.

Back to the question: what kind of SM2 browser do users need? First, what users need is a browser, so of course users should have the latest and most secure browser, which is the SM2 browser developed based on the latest version of the Chromium. Now, the Google Chrome is version 115, but the SM2 browsers currently on the market are based on version 66, version 83, version 86, version 97, version 108, and version 110. According to the Chromium high-risk vulnerability CVE-2023-2033 information released by Google on April 14, the high-performance JavaScript engine V8 that has been widely used in various versions has a Type Confusion vulnerability, and all Chromium lower than version 112.0.5615.121 have this vulnerability and are insecure that it must be upgraded as soon as possible. This is the main reason why ZoTrus Technology decided to upgrade the current browser based on version 97 to version 114. After learning about the CVE-2023-2033 high-risk vulnerability information, we decided to upgrade our browser base on the latest version 114.0.5735.91 at that time. Today, we released a new ZT Browser version V114.0.5735.2241 based on Chromium 114 version, 2241 is the number continued from all versions released by ZT Browser.

That is to say, first of all, what users need is a browser for surfing the Internet, which is the **basic** function. In order to meet this basic function, the SM2 browser should upgrade the Chromium version in time to provide users with a secure kernel.

What about the second requirement? Of course, it is necessary to support the SM2 algorithm and the SM2 SSL certificate, which is the **core** functional requirement. Without this core function, it cannot be called a SM2 browser. Without this function, it is an ordinary browser with basic functions. However, how to support the SM2 algorithm and the SM2 SSL certificate? Of course, we must add the SM2 algorithm to the cipher suite of browser to realize that the cipher suite supports RSA/ECC/SM2 three algorithms, adaptive encryption algorithm, and the SM2 algorithm can be preferentially used to implement https encryption when shaking hands with the web server. Instead of using "two skins" like some so-called SM2 browsers, without changing the core of the cipher suite, a SM2 algorithm module is plugged in, requiring users to check the " SM2 encryption" button to realize the SM2 https encryption, which not only greatly reduces the user's online experience, but also often leads to the inability to seamlessly switch the cipher algorithm, which caused by not knowing which algorithm to be used to implement https encryption, and interrupts the connection with the Web server, thereby affecting the normal browsing.

The third requirement is, of course, **free**. This is what users know about browsers from the first time they go online. The top 5 browsers commonly used by users in the world are all completely free. The SM2 browser should also be completely free, which is a common demand of users. ZT Browser is aware of the simple needs of users, we have insisted on making a completely free SM2 browser since the public beta version was released on June 1 last year, and it must be completely free in all versions, including the Windows version and the made-in-China Operation Systems such as Kylin version and UOS version. This is the open secret why the number of users of ZT Browser has jumped from zero to one million in just one year, and it may already be the SM2 browser with the largest market share in China.

The author believes that only a completely free SM2 browser is available on the market can promote the popularization and application of SM2 SSL certificates and promote SM2 https encryption to ensure the security of China websites. It is no exaggeration to say that providing a completely free SM2 browser should be a browser producer's due awareness for national security, and it is a due social responsibility. The reason why RSA algorithm SSL certificates and RSA algorithms can be widely used in the world, of course, the completely free browser is the first hero, this has to be said that Microsoft IE browser was the first to be completely free and made a great contribution, and we must also praise

Google for making Chromium completely open source, these large companies have made immortal contributions to ensuring global Internet security. If China wants to popularize SM2 SSL certificates and SM2 https encryption, it must also learn from international practices to provide users to use a completely free SM2 browser. Only in this way can commercial cryptography be realized to ensure the security of China cyberspace. ZT Browser decided to insist on providing users with a free SM2 browser based on the latest Chromium, just like Microsoft broke the Netscape browser charging business model in 1995, which is the social responsibility that a SM2 browser producer should have.

The fourth requirement is to be clean and free of advertisements, because the application scenario of the SM2 browser is office, if there is a bunch of messy advertisements on the office computer, of course, this is not the office environment that any organization managers and employees want to see. ZT Browser always value the needs of users, from the first day of product release, it directly stated in Article 16 of the "Terms of Service" that "ZT Browser does not provide advertising services." We have also rejected some ad companies' intention to cooperate in advertising. We always firmly believe that if we focus on users and do everything for the sake of users, everything else will follow.

In addition to 100% meeting the above four real needs from users, ZT Browser also sets up a security bottom line for users, only modifying the code of the cipher suite part of the original Chromium, the code of the algorithm handshake with the web server and The code of UI to support the SM2 algorithm, SM2 SSL certificate and SM2 Certificate Transparency, and other codes are all original, without adding any extra line of code. Therefore, what users get is a browser with 100% the same functions and performance as Google Chrome, plus a completely free, clean, and ad-free SM2 browser that support SM2 algorithm.

ZT Browser does not stop at the above excellent functions. We also innovatively provide four additional functions exclusively in the world, and plan to develop a new cryptography reconstruction solution for zero-installation SM2 browsers.

(1) The address bar displays the SM2 encryption icon and website identity validation level icon: let site visitors know at a glance whether the website adopts the SM2 algorithm to achieve cryptography protection for compliance, and at a glance whether the identity of the website is trusted.

(2) Support SM2 certificate transparency: Not only supports international certificate transparency for RSA SSL certificate like Google Chrome, Apple Safari and Microsoft Edge, but also supports the SM2 certificate transparency for SM2 SSL certificate, which effectively protect the SM2 https encryption security and website security.

(3) EV green address bar: Let EV certification plays an important role in protecting the identity of the website and preventing the identity of the website from being counterfeited, so that website visitors can rest assured to interact with this website and conduct online transactions when they see the green address bar and protect Internet users from fake websites.

(4) Website trusted identity validation service: This is a paid value-added service provided by ZoTrus Technology, which solves the problem of lack of identity for 83% of the websites that have deployed DV SSL certificates, allowing the deployment of free DV SSL certificate websites can also have green address bars with trusted identities like EV SSL certificates deployed. Website security requires https encryption and trusted identity, which can effectively enhance the confidence of website visitors, thereby facilitating more online transactions.

(5) Plan to develop RBI service: This is currently a popular Remote Browser Isolation technology in the world, which can be used for SM2 reconstruction, so that users do not need to change browsers or install SM2 browsers, not only can directly use any existing browser to access the cloud SM2 browser to realize the SM2 https encryption, and can add an extra layer of threat protection and data protection for Internet browsing activities, run webpage code in the cloud SM2 browser, and isolate the local device from malware , to provide users with a more secure browsing experience in compliance with cryptography protection.

Welcome to download and use the completely free full-featured SM2 browser - ZT Browser.

Richard Wang

August 8, 2023
In Shenzhen, China