赛迪智库
面向政府·服务决策

现状与展望-浏览器支持中国商用密码与应用

Status and Expectation–Browser supports China Commercial Cryptographic Algorithm - SM2

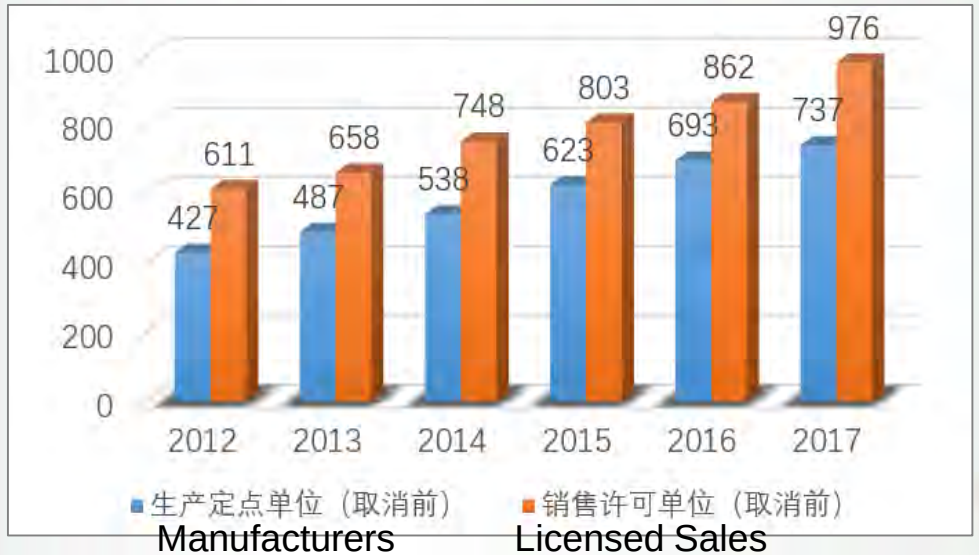
Dr. Liu Quan 刘权 Researcher
Director of Cyberspace Security Institute of China
Secretary General, China CA Industry Alliance

October 17, 2018

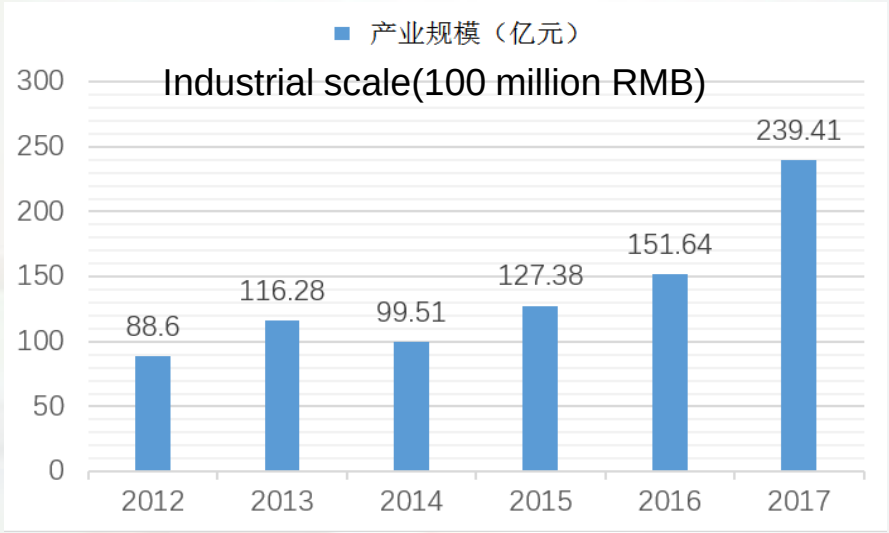
CONTENTS

(1) Status of Commercial Cipher Application in China
中国商用密码应用现状

By the end of 2017,the quantity of commercial cipher sales companies and manufacturers have reached 976 and 737 respectively in China. The industrial scale has reached 23.941 billion which has increase 57.9% compared with 2016. In the past 3 years, the average growth rate of industrial scale was 35%, and the industrial scale of 2018 is expected to exceed 32 billion.



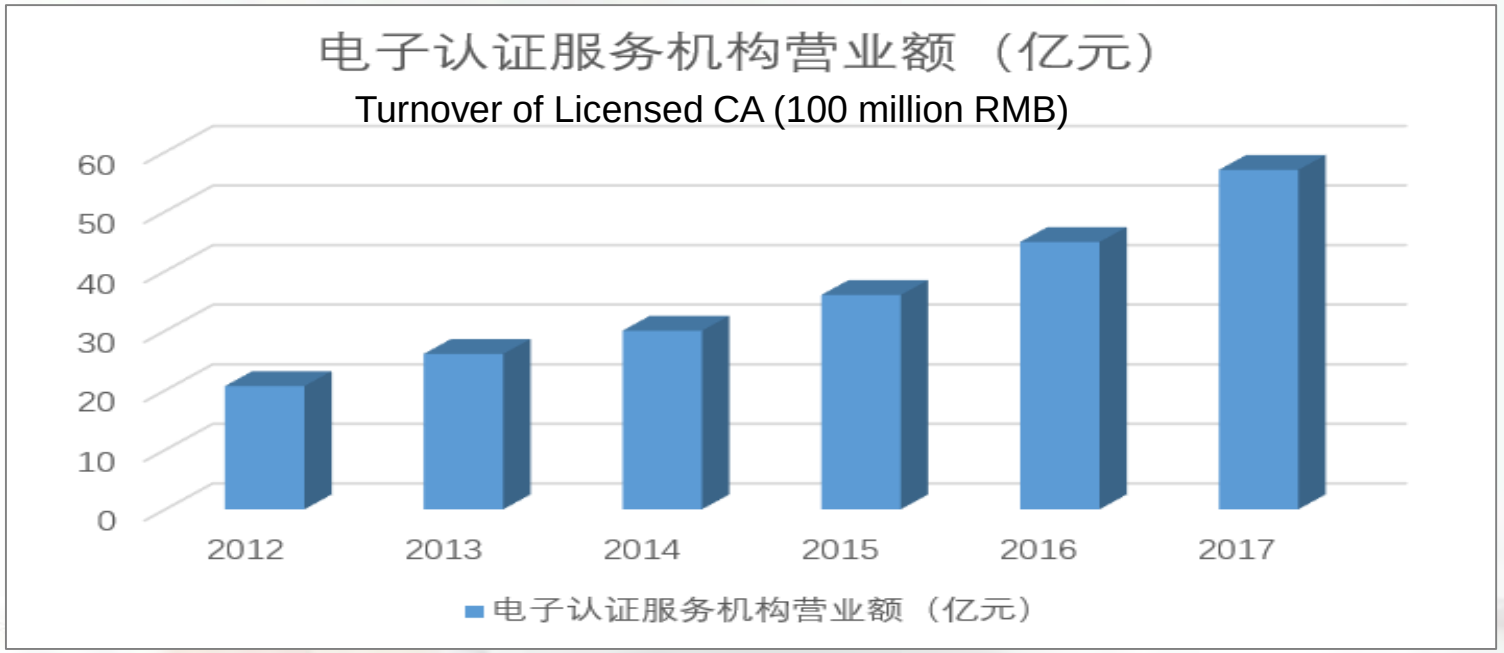
The growth of commercial cipher enterprises in 2012-2017



The industrial scale of commercial cipher in 2012-2017

(1) Status of Commercial Cipher Application in China
中国商用密码应用现状

- 45 companies have obtained the “CA License Using Commercial Cryptographic Algorithm” issued by SCA, 44 companies are listed in the “Catalogue of CAs for Electronic Government Affairs”
- 43 companies have obtained “CA License” issued by MIIT
- The number of issued digital certificates (Client Certificate) reaches 341 million, which can provide electronic authentication services for government to carry out social management, public services and other government activities.
- In 2017, the industrial scale of electronic authentication service reached 5.7 billion.



(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

◆ ”Cyber Security Law” which is formal implemented in June 2017 set that ”Network and critical information infrastructure operators shall fulfill security protection duties, adopt measures such as data classification, backup of important data, and encryption to ensure the network avoids interference, damage or unauthorized visits, and to guard against network data leaks, theft or falsification. Network operators shall safeguarding the integrity, secrecy and usability of online data”.

2017年6月正式实施《中华人民共和国网络安全法》规定：网络运营者和关键信息基础设施的运营者应当履行安全保护义务，采取数据分类、重要数据备份和加密等措施，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；网络运营者应当维护网络数据完整性、保密性和可用性,以及加密措施的实施。

(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

◆ ”Notice on strengthening the commercial cipher application of infrastructure information network” issued by General Office of MIIT ask that ”Establish and improve the commercial cryptographic system in the infrastructure information network, guide and standardize the application of commercial cryptography in the infrastructure information network, and promote the application of commercial cryptography solidly”.

《工业和信息化部办公厅关于加强基础信息网络密码应用工作的通知》要求，建立健全基础信息网络领域密码保障体系，指导并规范基础信息网络领域国产化密码应用，扎实推进国产密码应用工作。

(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

◆ “Notice on promoting the application of SM series cryptographic algorithm in foreign funded banks” announced that “promote the full application of commercial cipher application in foreign investment banks”.

《关于推进外资法人银行SM系列密码算法应用工作的通知》，全面启动外资银行国产密码应用工作。

(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

- “State administration informatization project construction plan during The 13th Five-year” clearly announced that , The construction of government information project should comprehensively promote the application of secure and reliable products and commercial cipher, improve the ability of self-protection, and ensure the security and reliable operation of government information system.

《“十三五”国家政务信息化工程建设规划》，明确要求政务信息化工程建设要全面推进安全可靠产品和密码应用，提高自主保障能力，切实保障政务信息系统的安全可靠运行。

(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

- ”Interim Measures for procurement of government information system” formulate that “the procurement requirements shall implement the requirements of relevant laws, regulations, policies and standards and norms of the SCA. At the same time, relevant organizations should plan, build and operate commercial cipher supported system and evaluate the system periodically”.

《政务信息系统政府采购管理暂行办法》规定：“采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

(2) Requirements of Commercial Cipher Application for Browser 浏览器商用密码应用相关要求

- “Guidelines for government websites” requires relevant organization to classify and manage important and sensitive data, complete encrypted storage and transmission, use cryptographic algorithms and products that conform to SCA policies and standards. Thus, a cryptographic-based trusted network, security support and operation supervision mechanism will be gradually established.

《政府网站发展指引》，明确要求对重要数据、敏感数据信息分类管理，做好加密存储和传输。用符合国家密码管理政策和标准规范的密码算法和产品，逐步建立基于密码的网络信任、安全支撑和运行监管机制。

(3) Future plan for the Commercial Cipher Application in Browser 浏览器商用密码应用下一步设想

- At present, foreign brand SSL certificates have monopoly status in China, and the SSL certificates issued by China CA need to do the WebTrust audit, but the current CAB Forum standard don't support SM2 algorithm.
- According to the relevant requirements of commercial cipher application in China, foreign CA issued SSL certificate will encounter obstacles in government information systems and infrastructure system if it doesn't support China Commercial Cryptography Algorithm – SM2.

目前，国外品牌的服务器SSL证书在我国拥有垄断地位，国内CA签发的SSL证书只有通过WebTrust审计并预置到各个浏览器后才有效。但目前国际标准不支持SM2；而根据中国商用密码应用的相关要求，在党政机关、重要领域等，不支持中国加密算法SM2的SSL证书应用会遇到障碍。

(3) Future plan for the Commercial Cipher Application in Browser 浏览器商用密码应用下一步设想

- To meet the requirements of commercial cipher application in China, the Alliance is taking the lead in formulating browser security standards for SM2 support, and related standard for CA that issue SM2 SSL certificate. On this basis, we are preparing to build a forums for CA, browsers, operating systems (CCABO, **China CA/ Browser/OS Forum**,).

为适应商用密码应用的相关要求，下一步CA联盟牵头制定浏览器安全标准和相关CA标准支持SM2，在此基础上，筹建中国CA机构、浏览器、操作系统论坛(CCABO论坛)

- It is hoped that the relevant organizations will support the CCABO Forum, and CCABO like to cooperate with CA/B Forum.

希望各相关单位能支持CCABO论坛，并为CA/B Forum在中国推进落地事宜做好配合工作。

赛迪智库
面向政府·服务决策

Thanks

www.ccidthinktank.com

Email：liuquan2189@163.com