Business Needs for Cryptographic Technology in Japan's Financial Industry[1]

Naoyuki Iwashita
Institute for Monetary and Economic Studies
Bank of Japan

Cryptography and the banking industry

The banking industry, as well as the military, has been the largest market for cryptography. It is well known that modern cryptography began with the development of the Data Encryption Standard (DES), which was ignited by the strong business needs for secure communication by banks in the United States. In the 1960s, US commercial banks were competing with each other to build a computer network for financial transactions between their headquarters and branches. Banks have to be able to ensure that information within the banking network, such as payment instructions and private information, remains secure. American banks therefore requested that the US government set a standard for a reliable cryptographic algorithm. IBM developed the algorithm and the National Bureau of Standards (NBS, now the National Institute of Standards and Technology, NIST) approved the DES as FIPS (Federal Information Processing Standards) in the mid-1970s. The DES is known as FIPS 46-1 and 46-2, but among banks it is more frequently referred to as ANSI X9.32, one of the US national banking standards. After the standardization, DES was widely used by commercial banks in the United States and European countries and throughout the rest of the world. Banks have used DES in many applications, such as message authentication code (MAC) and key agreements in wholesale banking, and for the encipherment of personal identification numbers (PINs) in retail banking. The global financial industry has relied heavily on DES for many years.

Migration from DES to triple DES and public key cryptography

This situation changed in the 1990s, when advances in technology and computing performance weakened the security of DES.

The developers originally designed DES with a 56-bit key after considering its strength against an exhaustive key search[2] based on the computer technology of the 1970s. In those days, people believed that an exhaustive key search of DES was so expensive that nobody could attack DES in practice. But, as the performance of microprocessors has advanced and their cost has been reduced, an exhaustive 56-bit key search is no longer unrealistic in the 1990s. In 1994, Michael Wiener estimated that it would cost one million dollars to develop a specialized computer to perform an exhaustive key search of DES that would take 3.5 hours on average. In 1998, a DES cracking machine was actually built and used to recover a DES key in 56 hours at RSA's DES Challenge[3].

---

[1] This paper was prepared for the 1999 International Workshop on Practice and Theory in Public Key Cryptography (PKC'99), held by the Imai Laboratory, Institute of Industrial Science, the University of Tokyo on March 1-3, 1999. Views expressed in this paper are those of author and do not necessarily reflect those of the Bank of Japan or the Institute for Monetary and Economic Studies.

[2] Exhaustive Key Search: the basic technique to attack common key cipher by trying every possible key in turn until the correct key is identified

[3] RSA's DES Challenge: a public contest to evaluate the strength of DES sponsored by the RSA Laboratories

In the light of these developments, US and European banks realize that they need a more secure cryptographic algorithm, so they are now migrating from DES to triple DES[4] and public key cryptography. In 1998, triple DES was standardized by the American banking standardization committee X9F as ANSI X9.52. FIPS 46-2 (DES) has expired and FIPS 46-3 (triple DES) is about to be published. RSA Digital Signature was also standardized by X9F as ANSI X9.31. The U.S. Department of Commerce has approved it as a Federal Standard and RSA has been added to FIPS 186-1. These standardization activities show that US banks are aggressively utilizing more secure cryptographic technology than DES.

The Japanese financial industry seldom uses cryptography

Unlike in the US, the Japanese financial industry is not so actively utilizing cryptographic technology. No national standard has been established by the banking community in Japan, where the market for business applications involving cryptography is very small.

Japan has no regulations covering the use of cryptography, with the exception of export controls on cryptographic products in line with the Wassenaar Arrangement[5]. This lack of regulation reflects the limited use of cryptographic technology in Japan. Even though high-value payment instructions are transmitted in Japanese inter-bank and intra-bank computer networks, cryptographic technologies are seldom used there. We can find only two financial computer networks that incorporate cryptography to achieve information security in Japan. They are BOJ-NET and CAFIS. BOJ-NET is a wholesale settlement system provided by the Bank of Japan. DES and triple DES are used to achieve confidentiality and user authentication in BOJ-NET. CAFIS is a settlement system for credit card transactions provided by a subsidiary company of NTT. FEAL[6] is implemented in CAFIS.

Japanese banks have been seeing that there is very little risk in computer network in so far as they use leased lines for telecommunication. In Japan, telecommunication business was managed by the public sector until the mid-1980s. Banks and bank customers trust that leased lines are never wiretapped and that transmitted data is never tampered with. In fact, there have been very few crimes against bank computer networks and so banks have not realized the importance of cryptography. Bank customers have rarely paid attention to the information security precautions taken by their banks. Japan has therefore been a nation lacking a strong interest in cryptography.

The Internet has stimulated interest in cryptography in Japan

But this is all changing now. A growing interest in cryptographic technology is being witnessed in Japan. The driving force behind this is the rapid growth in Internet use in Japan.

---

[4] Triple DES: a method to strengthen the security of DES by performing DES operations three times in the sequence encrypt-decrypt-encrypt with two or three different keys

[5] Wassenaar Arrangement: an international agreement on export controls for conventional weapons and dual-use goods and technologies

[6] FEAL: a common key cryptographic algorithm developed by NTT in 1988

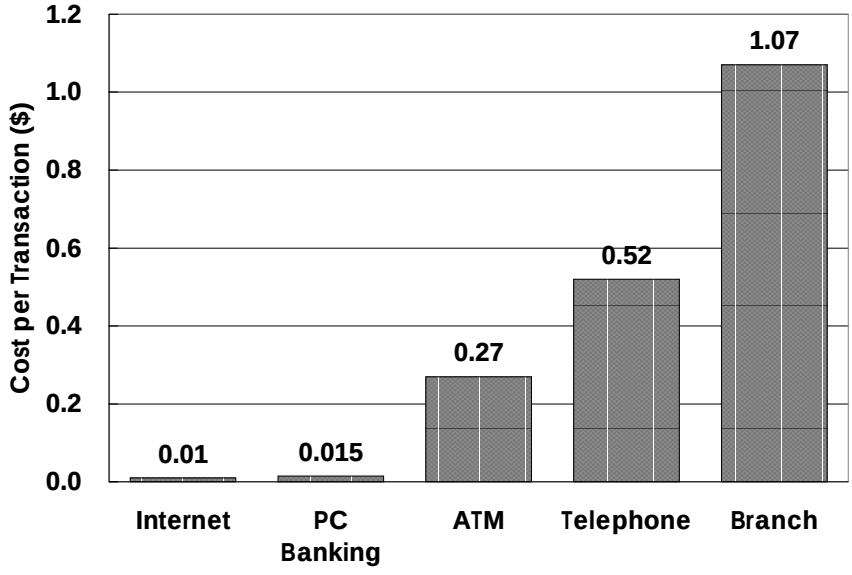
According to the Internet Association of Japan, the population of Internet users in Japan increased to more than ten million by 1998. As in the US, this has stimulated an active discussion on how to protect data transmitted on the Internet in Japan. The evidence of this is that while no books on cryptographic security sold well in Japan a few years ago, books on IT security and electronic money can now be found in the best-seller sections of bookstores, next to popular leisure books.

As interest in cryptography grows, the number of users of cryptography will increase. In fact, a wide variety of security products using cryptographic technology have recently been marketed by many vendors in Japan. Also, projects to test the implementation of cryptographic technology such as electronic money and S.E.T.-based electronic credit cards have been implemented by banks and other financial institutions.

Internet banking is emerging

From the business point of view, US and European banks are actively developing Internet banking. According to a paper by a consulting firm named Booz-Allen and Hamilton, US and European banks rank the Internet as the most important customer interface in 10 years.

Internet banking services are less expensive to offer to customers than other forms of banking. Checking an account balance or transferring funds from a checking account to a savings account can be done in person at a branch bank, over the telephone, with an Automatic Teller Machine (ATM), or at home using a PC on a bank's Web site. A branch bank can serve as many customers as it has staff to handle. Once the investment is made to create a fully functioning Internet site, the bank's Web site can handle one customer inquiry or tens of thousands a day. The consulting firm estimates that it costs about one cent to conduct a banking transaction using the Internet and more than one dollar if handled by a teller at a branch bank. They predict that online retail banking is being driven by lower operating costs, the ability to offer new services, and the ability to do one-to-one marketing.



(Source: Booz-Allen and Hamilton)

The emergence of Internet banking is prompting US and European banks to rethink their customer interface. The Internet enables banks to offer low-cost, high value-added financial services. In addition, it provides customers with better opportunities to compare services and make transactions at home or in the office.

The perception gap on Internet banking between Japan on the one hand and the US and Europe on the other

The Japanese banking industry is far behind in the practical use of cryptographic technology because it has been doing its business over closed networks. Japanese banks need to define a new security policy and utilize cryptographic technology when they provide new services over open networks such as Internet banking and electronic money.

So far, Japanese banks have hesitated to change their security policy by opening up their networks to the public in spite of the cost effectiveness of this new channel for delivering banking services to their customers. According to a survey on Internet banking in Japan conducted by the same consulting firm in 1997, there was a huge perception gap between Japanese banks on the one hand and US and European banks on the other regarding the future of Internet banking. The US and European banks expect Internet banking to become the most important retail channel within 10 years, but Japanese banks expect traditional branches to remain the most important channel.

A global survey covering 386 retail and corporate banks in 42 countries to assess the strategic impact of Internet banking on the financial services industry

US and European banks expect ..	Japanese banks expect ..
Within 3 years, 60% of retail and 80% of corporate sites will offer a broad range of interactive, on-line banking services.	Japanese banks consider Internet banking to still be in a test phase.
US and European banks rank the Internet as the most important customer interface in 10 years. There is a possibility that traditional branches will lose their most profitable customers in 3-5 years.	Japanese banks rank traditional branches as the most important channel in 10 years, and rank the Internet as the third most important channel, after the telephone.

(Source: Booz-Allen and Hamilton)

Differences in payment practices between Japan and the US

It is understandable that Japanese banks underestimate the impact of Internet banking and hesitate to change their business style, because their customers' need for the new interface is not so strong as it is in the US and Europe. Japanese banks see that their customers are satisfied with traditional branch banking because Japanese payment practice allows bank customers to enjoy relatively low transaction costs.

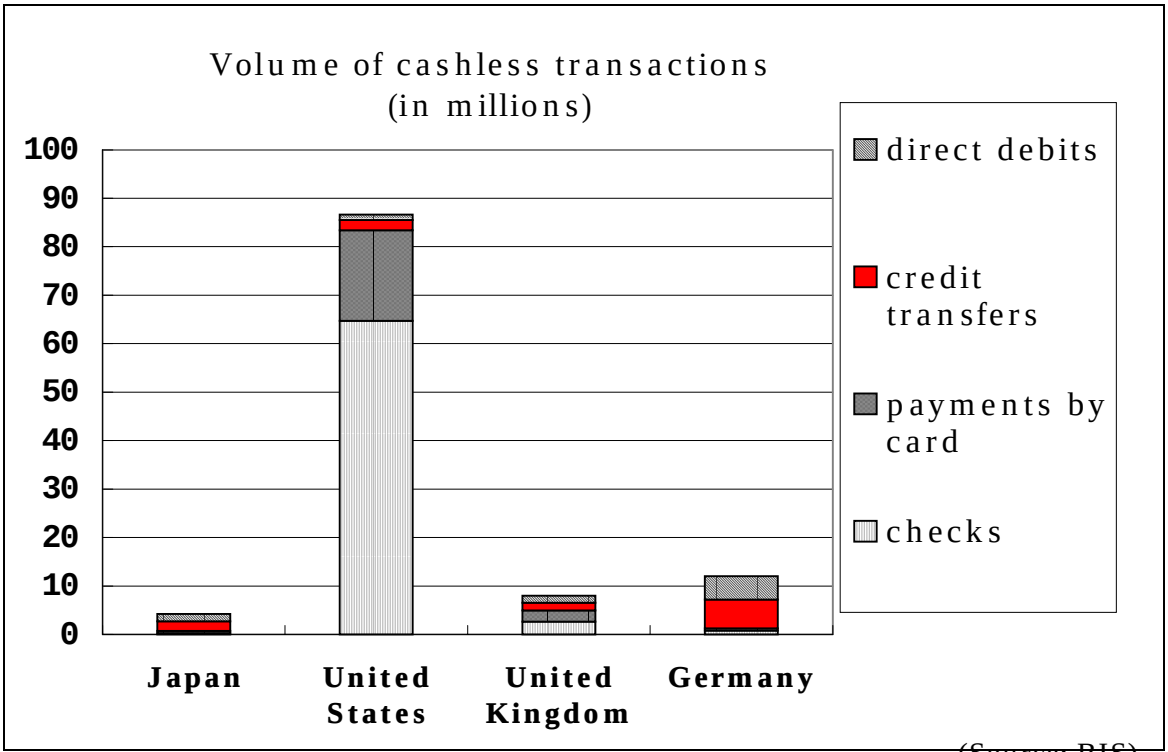
In Japan, cash is dominant in the settlement of transactions between individuals and businesses. Although business firms do write out checks, these are used solely for the settlement of transactions between businesses. Checks are not used for the payment of salaries or for the settlement of small transactions with individuals. For all practical

purposes, individuals in Japan do not write checks.
The use of pre-arranged direct debits and pre-arranged direct credits through bank accounts is also widespread. With pre-arranged direct debits, the claimant (payee) sends a payment request to the designated financial institution of the payer either through the firm banking network or by providing a magnetic tape. The said financial institution pays out the requested amount of funds from the account of the payer based on the three-party agreement between the payer, the payee, and the bank. About 80% of all households in Japan use pre-arranged direct debits to pay the five major public utility charges, namely, telephone, electricity, gas, water, and the national television service.

With pre-arranged direct credits, the payer directly deposits funds in the bank account of the payee for the periodic payment of salaries, dividends, and pensions. The payer sends instructions to the bank either through the firm's banking network or by providing a magnetic tape. The information and the funds are transmitted to the payee's bank through the inter-bank network. Almost all large firms use pre-arranged direct credits to pay salaries.

These electronic means used in the settlement of funds between individuals and businesses allow a large volume of transactions to be conducted mechanically. As a result, both businesses and individuals save a great amount of labor associated with the settlement of funds.

A comparison of statistics of payment volume in Japan and the United States shows that (1) the share of electronic means in business-to-business payments is higher in Japan than in the United States and (2) the volume of payments in the United States is much larger than in Japan. This shows that payments are made less frequently in Japan than in the United States, with a correspondingly higher value for each payment. This reflects differences in payment practice between Japan and the United



(Source: BIS)

States. In Japan, companies make business-to-business payments only once a month based on the assumption of long-term business relationships. Accounts payable or receivable are not settled as they are incurred during the course of a month. Instead, they are aggregated and settled on a designated day (the 10th, for example) of the following month after the records are confirmed by both parties. This feature can also be supported by macroeconomic data, which show that the size of accounts receivable in corporate balance sheets in Japan is large relative to the size of the economy.

In the United States, companies make payments for each transaction by issuing checks and bills. For a business, preparing and sending paper bills are costly. For a consumer, paying bills by check is time-consuming. For banks, processing paper checks is costly. Because existing payment practice is inefficient, banks, bank customers and the government have a strong need to improve the payment system in the United States.

Will the Japanese Banking Industry expand its use of cryptography?

As Japanese payment systems and practices are well-designed and so far efficient for bank customers, those customers do not request that banks introduce a new interface such as the Internet if it means additional cost. This probably explains why Japanese banks hesitate to revamp existing payment networks, while US and European banks are improving their payment systems to more advanced ones, such as Internet banking.

But when Internet banking becomes widespread throughout the world, it is not likely that Japanese banks alone will continue to rely heavily on expensive branch banking. Even though it is not so profitable, Japanese banks have to change their way of doing business to make themselves compatible with the global standard because the Internet will stimulate global competition between banks. It will be a hard task for Japanese banks to change their existing closed payment networks to open networks, but they will need to introduce new interfaces by using cryptographic technology in order to survive in the 21st century.

Reference

Bank for International Settlements, "Statistics on payment systems in the group of ten countries - figures for 1996," December 1997.

Booz-Allen & Hamilton, Inc., "Internet Banking: A Survey of Current and Future Development," February 1996.

Booz-Allen & Hamilton, Inc., "Booz-Allen's Worldwide Survey Revealed A Huge Perception Gap Between Japanese And American/European Banks Regarding Internet Banking," 1997.

D. Coppersmith, C. Holloway, S. M. Matyas, and N. Zunic, "The Data Encryption Standard," Information Security Technical Report, Vol. 2, No.2, pp. 22-24, ZERGO, 1997.

Electronic Frontier Foundation, "Cracking DES -- Secrets of Encryption Research, Wiretap Politics & Chip Design," O'Reilly & Associates, May 1998.

International Organization for Standardization, "ISO/TC68 Cryptographic Development Policy," April 1995.

K. Kusuda and T. Matsumoto, "A Strength Evaluation of the Data Encryption Standard," Institute for Monetary and Economic Studies, Bank of Japan, DPS No. 97-E-5, July 1997.

RSA Laboratories, "Frequently Asked Questions about Today's Cryptography."

U.S. Department of Commerce, "The Emerging Digital Economy," May 1998.

M.J. Wiener, "Efficient DES key search," Technical Report TR244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994.