

Providing Secure Banking and E-Commerce via Server Gated Cryptography

Published: February 1999

ASB Bank, one of New Zealand's leading banks, has long earned a reputation for leading the pack when it comes to using technology to respond to customers' needs. So when customers wanted secure, convenient banking via the Internet, ASB Bank responded by launching the Fastnet online banking system, one of the first in the world to use Microsoft's Server Gated Cryptography, a technology that for the first time makes strong cryptography available to worldwide banking customers. ASB Bank is now deploying Access On-line, an online merchant and e-commerce service that also is backed by SGC.

Solution Overview

Industry

Financial

Company Profile

ASB Bank, one of the oldest and largest banks in New Zealand.

Situation

Customers need convenient, secure online banking.

E-merchants need secure credit card authorization

Solution

- **Products**

Windows NT Server 4.0

Internet Information Server 4.0

Server Gated Cryptography

- **Scenarios**

Online banking

Online credit card authorization

- **Services**

- **Partners**

- **Benefits**

Convenient, secure online banking for customers

Fast, secure credit card authorization for e-merchants

ASB Bank is one of New Zealand's oldest banks, having been in operation for over 150 years. But that hasn't stopped it from being at the cutting edge of banking technology. In the 1960s, it was one of the first banks in New Zealand to install a computer system linking its branch offices to its main office. In the early 1980s, it was among the first to deploy point-of-sale banking machines that allowed customers to pay for goods and services using a bank card and have the funds electronically deducted from their checking accounts. In 1988, it was the first bank in New Zealand to introduce banking by telephone.

When the Internet explosion occurred in the mid-1990s, ASB Bank saw an opportunity to make banking more convenient than ever for its customers. "We realized the need to embrace online services in October 1995 to protect our position as a technology leader," says Jeremy Dean, Chief Manager, Electronic Banking. The bank therefore established its Internet Banking Services (IBS) Programme, with the aim of providing information, banking services, product access and transactional utility via the Internet to both retail and commercial customers.

New Opportunities on the Web

Because the World Wide Web was a relatively new technology, it was important for the bank to cut its teeth in the new medium. As its first Internet-based offering, it developed a corporate web site, <http://www.asbbank.co.nz/>, that profiled the bank and its customers. The site was a broad reach site that allowed the bank to learn how to manage Internet development, maintain ongoing programs to update content and functionality and keep the lid on internal support costs. "Working on the corporate web site, we learned how to present to, and interact with, customers on-line. We learned how to express our brand and how to manage a dialogue in that environment," says Dean. "Some of that dialogue can be quite robust."

With that success under its belt, ASB Bank moved on to Fastnet, an Internet banking service that allows retail customers to check balances and statements, transfer funds and make bill payments – from anywhere in the world. It chose to deploy the service on Microsoft® Windows NT® Server 4.0, using its Internet Information Server to provide web hosting services. "We wanted to build on a strong, secure, reliable platform," says Dean

The Bank started testing Fastnet internally and officially launched the service in April 1996. It was the first online banking service in New Zealand. "As a result of that we discovered that our intuitions about the value of on line business services were correct," says Dean. "We flushed out the challenges and

changed technologies. We then committed to launching a full Internet based Service, and did so in mid 1997, providing a customers with a facility that was not only truly useful, but also far in advance of what other New Zealand banks were then able to offer."

Security a Paramount Issue

But security was just as important a consideration to the bank's customers as convenience was, and ASB Bank recognized from the first that Fastnet would need to provide the strongest protection possible for their online transactions. "We established early on that 128-bit cryptography was the minimum level of security that we were comfortable with," says Dean, referring to the length of the encryption keys that are used to protect Fastnet sessions. The more digits in the key, the harder it is for an attacker to decrypt someone else's information. With keys of 128 bits, it has been estimated that it would take a supercomputer thousands of years to decrypt a single message.

The problem was that Microsoft, as a US company, is bound by US export laws concerning cryptography. Until recently, US export laws allowed export of cryptography with no more than 40-bit keys. The 128-bit cryptography that ASB wanted to deploy is immensely more secure. How much more secure? Multiply seventeen billion by seventeen billion, and that's how many times more secure 128-bit cryptography is than 40-bit cryptography. The US Government's concern was that such strong cryptography, if freely exported worldwide, might be used by rogue nations to conceal weapons programs and the like.

Fortunately, a new Microsoft technology called Server Gated Cryptography (SGC) allowed ASB Bank to satisfy its customers' need for secure transactions and the US Government's export laws. US export law does allow strong cryptography to be exported if it can be controlled so that it can only be used for legitimate purposes, like online banking. SGC does just that. The SGC software is included in every current copy of Internet Information Server, Internet Explorer, and Money, and also interoperates with other vendors' Internet browsers. Despite the widespread availability of the software, though, a server needs one pivotal piece of data – a so-called digital certificate – before it can actually begin providing strong cryptographic protection. The companies that provide these certificates are legally responsible for verifying that they're issued only to legitimate companies, like banks.

The end result is that everyone's happy. Customers are happy because they get the security they need, already included in the software they have. The bank is happy to be able to provide a valuable service to its customers, and the US Government is happy because strong cryptography is only being used for legitimate business. "We trailed alternate security technologies, but customer feedback showed that these approaches were cumbersome. We then searched far and wide for the best security we could find

and finally settled on Microsoft's Server Gated Cryptography with 128-bit security," says Dean.

Looking Toward the Future

With the success of Fastnet assured, ASB Bank is looking to expand its online offerings even further. The next service, due to launch in 1999, is called 'Access On-line', and, like Fastnet, uses Server Gated Cryptography to provide 128-bit security, this time for merchant and e.commerce transaction applications. "Where Fastnet adds value to our relationship with traditional retail customers, Access On-Line adds value to our relationship with merchants," explains Dean.

Access On-line allows online merchants to quickly and securely process customers' credit card charges when they make a purchase. "We recognized that merchants and commercial organizations wished to collect, process and have credit card transactions authorized securely over the Internet and we felt that there was a role for the bank to play in that area," says Dean.

Access On-line acts as a broker between the merchant and the card issuer. When the customer hits the "pay" button at an Internet commerce site and provides his credit card number, the merchant establishes a secure session with the bank, using SGC. Access On-line then gets the card number and expiration date, and presents them to the card issuer via a separate SGC session. The issuer provides an authorization number to the Access On-line server, which relays it to the merchant. The end result is fast e-commerce transactions for the customer, with complete security for the customer, the merchant and the card issuer.

"We now better understand how business-to-business and business-to-consumer transactions will be conducted on the Web," says Dean. "You might say that our early incumbency of the position of as technology leader has presented us with a number of learning opportunities."

