Case Study

SE*link*™

ATM Security Enhancement and Optimisation

Background

The most commonly used switching platforms, Base24, lacks the flexibility to meet the increasing number of new security standards and the requirements of new payment products. Base24 was never security-by-design to face cyber attacks.
Another consideration is that large financial institutions are increasingly frustrated with the rigidity of Base24 sunset and legacy switching platforms. Financial institutions are charged dearly by service providers for the national private switched network infrastructure since every ATM must be set with fixed IP in order to be reachable by the ATM Host and vice versa.

Challenge

The workarounds needed to secure ATM connections to the Host, like TLS/SSL, to try to address Base24 deficiencies only serve to increase technical complexities and higher costs for greater bandwidth. Implementing cryptographic accelerators on the host and resizing networks bandwidth were not helping but actually compounded the initial issues meant to be resolved.
Financial institutions are gearing themselves for enriched crypto agile cryptographic schemes in order to be ready for quantum era since standard technologies like TLS/SSL are not crypto agile. But can they possibly implement something great but with little or no infrastructural changes to their existing ATM environment ?

Industry

Financial Institutions

Challenge

- ATM needs to be secured
- Reduced bandwidth due to the ATM private infrastructure
- Standard protocol not designed to face new landscapes and trends of cyber attacks
- Quantum Computing era is real

Goals

- New security scheme and technology with low impact on ATM infrastructure
- Reduce bandwidth consumption through low overhead security scheme
- Crypto agility to face the quantum computing-era

Solution

SE*link*™ provides a zero trust security model combined with software-defined network segmentation and whitelisting practices. Delivering Data, Device, Network Security and Control in one single solution

Solution

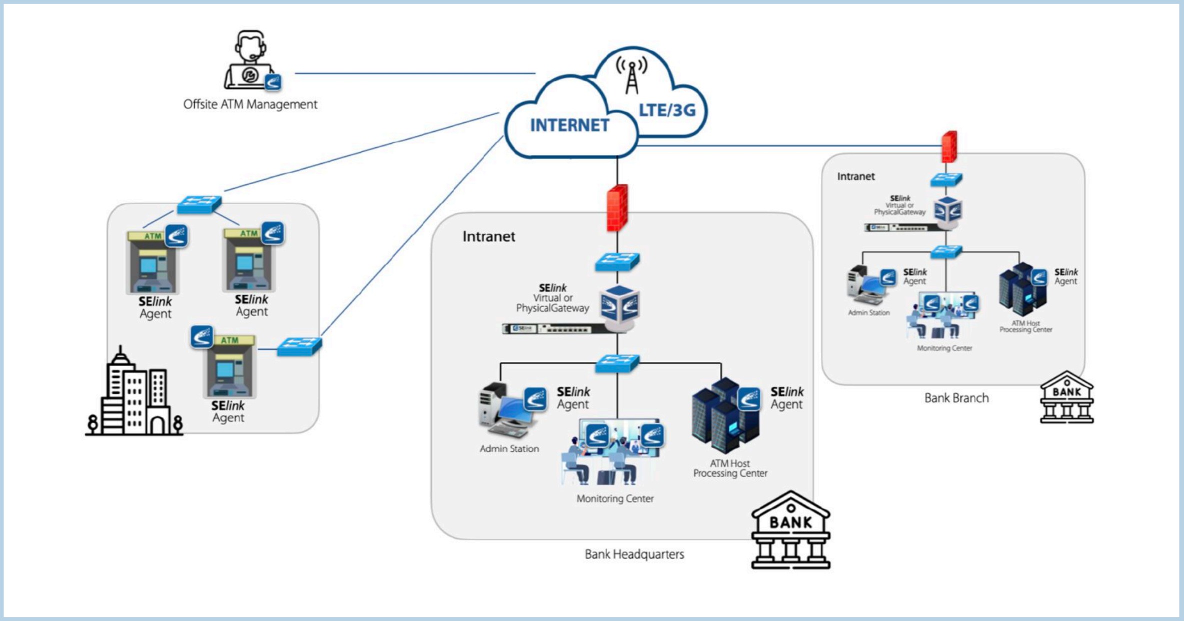
A new generation of payment switching solution is needed to enable businesses to react quickly to customer demands, supports multi vendor software, new security requirements and payment trends. This new generation of payment switching solution will have a foundation built on the latest flexible technologies such that whenever information is transferred among two or more entities, the connection links must be secured since it offers an attractive opportunity for attackers to catch sensitive contents.

Benefits

1. Less than 300 Bytes to establish a link
2. Zero overhead on encrypted packet
3. Automatic Key evolution
4. Permanent Session
5. Crypto Agility
6. Network Optimisation

Minimum Bandwidth | 0 Encryption Overhead | Key Evolution | Permanent Session | Crypto Agility

Introducing the SE*link*™ is a very light technology, derived from over 10 years of military based techniques, easy to be implemented in any environment (over any protocol), portable, multi-device and multi-paradigm. Every establishment of connection over SE*link*™ requires *20 times less than TLS*. What is more appealing is that upon secure channel negotiation, *0 data overhead* is required to encrypt the transmission channel. Another cutting-edge security mechanism is that SE*link*™ cryptographic keys evolve at every packet transmission without the need to establish new session. Unlike TLS and other standard encryption protocols, SE*link*™ generates new session keys either every 'N' seconds or every 'M' bytes. *Automatic key evolution* mechanism allows SE*link*™ to keep alive a *Permanent Security Session* without compromising the quality of key material. On the contrary, TLS requires the creation a new security session at every new connection which are time and bandwidth consuming and greatly deteriorates the final performances of the entire infrastructure. Perhaps the most unique benefit offered by SE*link*™ is the capacity to adopt alternatives to the original encryption method or cryptographic primitive without significant change to system infrastructure. This capability is called *Crypto Agility* and is the most effective way to face Quantum Computing attacks. As detailed in the NIST report on Post-Quantum Cryptography, NISTIR8105, all the algorithms used in PKI and certificate-based security systems are no longer secure. SE*link*™ is capable to manage both symmetrical and asymmetrical (PKI) schemes with default configuration based on symmetrical algorithms which are still considered robust against Quantum Computing attacks. Crypto agility allows financial institutions to migrate with ease to any new symmetrical algorithms in a centralised way since SE*link*™ readily supports Post-Quantum algorithms as shortlisted by NIST. SE*link*™ can be easily installed on any ATM machines as a TCP proxy, and at the financial institution data centres as a SE*link*™ TCP gateway. Beyond the encryption capabilities, the SE*link*™ TCP Gateway is able to virtualise the source IP of any ATM machines and binding respective ATM machine MAC addresses. This architecture allows financial institutions to optimise the network infrastructure as ATM machines no longer require fixed IP reachable as mandated by the legacy BASE24 protocol. This puts SE*link*™ a notch higher against all other data-in-motion security technologies in the market.


Offsite ATM Management
INTERNET
LTE/3G
ATM
SElink Agent
SElink Agent
SElink Agent
Intranet
SElink Virtual or PhysicalGateway
SElink Agent
Admin Station
Monitoring Center
SElink Agent
ATM Host Processing Center
BANK
Bank Headquarters
Intranet
SElink Virtual or PhysicalGateway
SElink Agent
Admin Station
Monitoring Center
SElink Agent
ATM Host Processing Center
BANK
Bank Branch