CRYPTOMATHIC
www.cryptomathic.com

Authenticator Case Study – permanent tsb

STRONG USER AUTHENTICATION FOR MULTI CHANNEL BANKING

permanent tsb has implemented the Cryptomathic Authenticator to secure transactions for its internet and telephone banking services. The aim of the implementation was to provide a high level of security eliminating fraud while ensuring an easy and improved customer experience. permanent tsb chose the Cryptomathic solution as the market leader in authentication due to its flexibility in supporting multiple authentication mechanisms and its ease of integration.

PERMANENT TSB'S REQUIREMENT FOR STRONG USER AUTHENTICATION

The permanent tsb Group Holdings plc is one of the top three providers of personal financial services in the Irish market. The group has over one million customers in Ireland, and offers a full range of personal banking services through a multi-channel distribution network of branches and remote customer interfaces including direct access via telephone and internet.

Although telephone and internet banking provides a convenient way for customers to manage their accounts they are like all retail banking customers a target for fraud, in particular Phishing. As these channels are independent of location, as opposed to person to person branch banking, the attacks can come from anywhere in the world. Prior to this project the bank used security call backs as a successful additional control method but these do not deliver a great customer experience and are cumbersome to maintain.

This has led permanent tsb to recognise the need for securing their remote banking channels before being hit by major fraud, thereby securing the banks reputation, increasing customer confidence and ensuring new customers are comfortable using the remote banking channels.

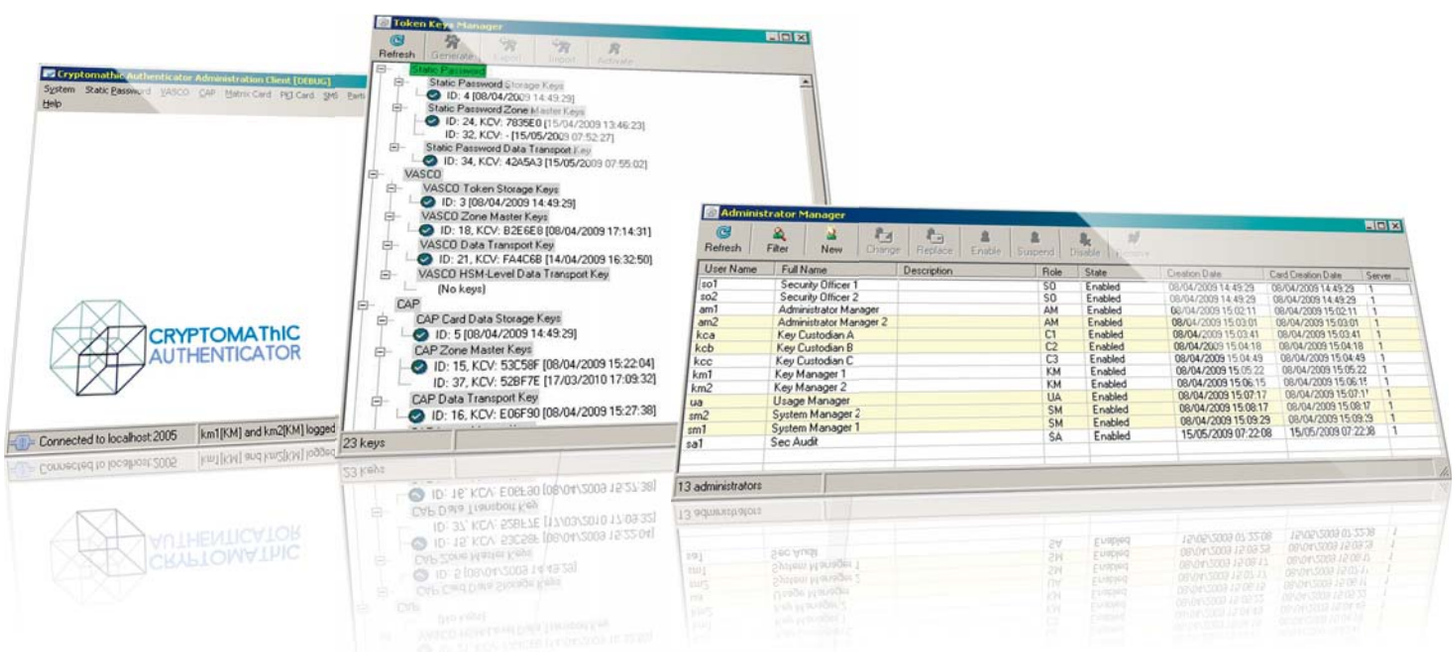
Authentication

The solution to this problem is strong authentication, which is a powerful security method that can be implemented across multiple channels. Strong authentication is based on the use of more than one authentication method within a single transaction. The three main authentication methods are *something you know*, *something you have* and *something you are*. Traditional authentication is based solely on something you know, such as static passwords and cherished questions. Two-factor authentication couples something you know with something you have.

Karina O'Donnell,
Head of Customer Operations,
permanent tsb

We are delighted with the service provided by Cryptomathic in delivering a robust, flexible and future proof authentication solution for the Open24 channels. We got exactly what was promised on day 1 and customer feedback has been excellent."

permanent tsb researched the market for the most appropriate two-factor authentication solution and chose Cryptomathic Authenticator. The Authenticator was chosen over other solutions for its functionality and flexibility in that it supports multiple different authentication mechanisms and token form factors and because Cryptomathic had a clear understanding of the issues facing the bank and the preferred method of authentication. The Authenticator was also easily integrated into the existing back-end infrastructure through its ability to run as a stand alone service.



Solution Overview

permanent tsb customers already enjoy the flexibility to manage their accounts through multiple channels, including internet banking and telephone banking via a customer contact centre.

The initial drive by the bank to move to strong authentication was targeted at securing the initialisation of payments (Standing Orders, Bill payments, etc.) through the Open24 internet banking platform and the telephone banking system. This meant that Cryptomathic Authenticator would not be integrated with the bank's core platform, for token provisioning and customer information, but it would instead have to interface with two distinct internal banking systems – the internally developed Open24 system and the GTX customer contact centre workflow system provided by Kainos.

One of the key requirements from permanent tsb when selecting an authentication server was that it needed to be flexible, not only in its integration but also in the range and type of authentication methods that were supported. This was key to the bank implementing a cost effective solution but also to ease the migration between different authentication methods if or when the security landscape changes over time.

The initial authentication method chosen by permanent tsb was the SMS token generated by Cryptomathic Authenticator. Using SMS messages for an authentication method tied into the bank's mobile banking strategy and negated the requirement for a large scale delivery of a token, while providing a very robust level of security because the token is delivered "out-of-band" (i.e. not through the existing customer interface networks). While no method of authentication could be considered foolproof the ease of delivery of an SMS solution in conjunction with the flexibility of the Authenticator platform made this the preferred choice. In order to support this, the bank and Cryptomathic had to work with a third service provider in Zamano – an SMS gateway provider in Ireland.

Solution Implementation

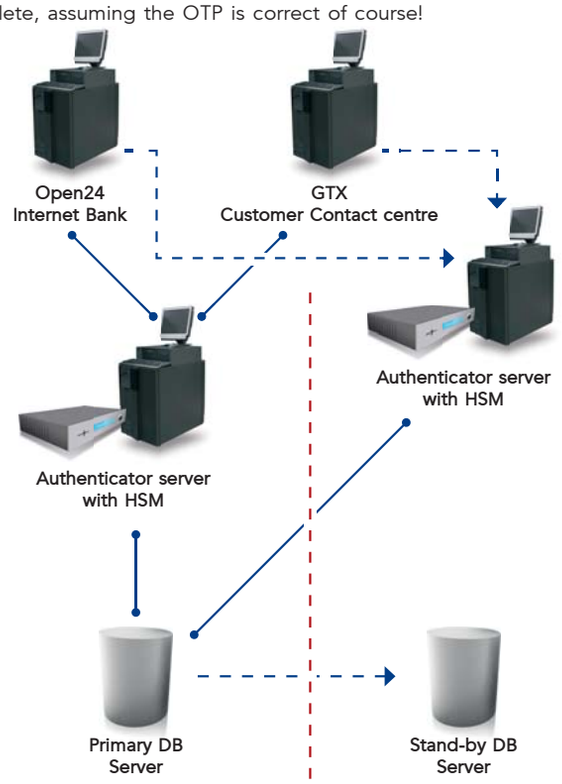
permanent tsb also needed to implement a solution which was robust and could provide high availability and ultimately scalability to support its 24 by 7 internet banking operation. To ensure this, Cryptomathic Authenticator was deployed in each of the permanent tsb data centres.

The first site became the primary data centre for all SMS and authentication requests from both the GTX (contact centre application) and Open24 systems. A second authentication server in the secondary data centre acts as a hot standby system. Through database replication across the two sites it becomes possible for SMS authentication requests to be serviced from either data centre at the "flip of a switch" while maintaining transparency to the banking customer and never losing in-stream transaction data.

Process Flow

permanent tsb customers can now access their accounts through Open24 (or the customer contact centre) in the usual way with their customer number and existing log-in credentials. Once on the site they can request to set up a third party transfer or standing order at which point the Open24 system will automatically request an SMS One Time Password (OTP) to be sent to the customer's pre-registered mobile phone number. In the background, Cryptomathic Authenticator is securely generating a unique OTP within the HSM and packaging this, along with any message to the customer, in an SMS text message, which is delivered from Authenticator directly to Zamano – the SMS gateway provider.

From the customer's perspective, they simply click a button to request a payment process in the usual way and are then requested to enter the OTP, which is sent to their mobile phone. Once received (just a few seconds depending on the mobile network) the OTP is typed into the web browser or read out to the contact centre operator and the transaction is complete, assuming the OTP is correct of course!



CRYPTOMATHIC PRODUCTS IN THE AUTHENTICATION SUITE

CRYPTOMATHIC AUTHENTICATOR – AN INDEPENDENT FUTURE PROOF SOLUTION

The Authenticator is an independent solution for a number of reasons. Firstly, it is independent of token suppliers so customers are not tied to any particular authentication vendors or technologies when choosing the Authenticator. Secondly, the same level of independence applies to HSMs, allowing the Authenticator to support the customer's preferred HSM brands and models.

Through a wide and growing range of user and transaction authentication methods, the Authenticator is able to adapt to future requirements and safeguard the value of the initial investment. It is also possible to provide your customer base with tokens that meet their individual needs without the need for additional infrastructure costs. For example: high risk customers could be provided with tokens based on more complex authentication techniques or even multiple authentication techniques, while low risk customers could be issued with tokens using less complex authentication therefore maximising protection while also minimising costs. Cryptomathic Authenticator allows the business to tailor the authentication needs across the business and to migrate between authentication mechanisms as the prevalent fraud migrates.

CRYPTOMATHIC TOKEN MANAGER

Cryptomathic Token Manger is designed to provide full lifecycle management of physical tokens to those organizations who require a strong authentication solution but have no existing management infrastructure. The product is designed to manage the end-2-end lifecycle of the token from the point at which it is initially requested, through its manufacture and distribution and on to its expiry and replacement. As part of this overall management process the issuer can also manage stock in several locations, handle multiple manufacturers and distributors and track various token types within a single implementation.

Tokens can be managed through a simple GUI interface on a customer services workstation or via direct web service integration into existing customer services workflow tools. The flexibility of this interface allows the token status to be managed at the single token level, the distributed packet level, the batch level or the stock location level which simplifies the management process.

CRYPTOMATHIC SIGNER

Cryptomathic Signer is an innovation in digitally signing and certifying electronic documents, from emails through to pdf and any other document type. The basis of the solution differs from other PKI implementations in that the user does not have to carry their private key around with them or store it on their computer. Instead, they simply have to authenticate themselves to the service and sign the relevant electronic document within the server itself. This means that they are not only signing exactly what they see but they also maintain the security of the private signing key.

ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With more than 25 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com