Two-Factor Authentication for Banking

Building the Business Case

www.cryptomathic.com

1 Executive Summary

As a leading security vendor to the financial sector, Cryptomathic have extensive experience in developing and delivering two-factor authentication solutions.

This White Paper aims to share that experience, providing an up-to-date overview of Internet banking threats and the range of authentication technologies available to counter them, explaining the key advantages and disadvantages of each.

We go on to explain how the business case for deploying two-factor authentication extends beyond a simple 'fraud minus costs' calculation to include a wide range of other factors. Our aim is to ensure strategic decision makers fully understand the range of opportunities for business development and cost reduction offered by two-factor authentication, and thereby enable a more positive, realistic business case.

Finally, we present our vision of a secure, scalable, flexible and token-vendor independent authentication infrastructure, supporting a comprehensive range of authentication methods. This approach enables banks to offer the optimal user experience across a range of applications and channels, whilst reducing development and deployment costs and avoiding token-vendor lock-in.
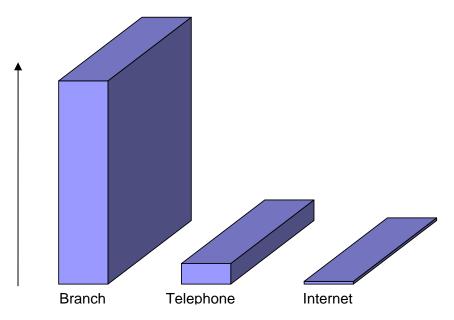
Cryptomathic's existing product portfolio delivers this vision, and has been proven in large-scale deployments with major international financial institutions. Working with Cryptomathic offers financial institutions access to the expertise, practical experience and technology necessary to successfully deploy two-factor authentication to their customer base.
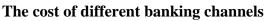
Introduction

The Internet is the fastest growing banking channel today, both in the fields of corporate and retail banking. The development is no longer just driven by the banks' desire to reduce costs: first and foremost it is a manifestation of customers' demand to access bank services on-line—at any time and from any location.

The importance of Internet banking is obvious for several reasons. Firstly, it offers a cost-efficient alternative to telephone and branch banking due to the relatively low capital and maintenance costs, and its fully-automated processing of most transactions. Secondly, it offers unparalleled customer convenience by enabling 24-hour access to a wide range of services.

The cost of different banking channels

Despite this win-win proposition, Internet banking is not without its drawbacks. Foremost among these in recent years has been the widespread targeting of on-line banking systems by international criminal gangs, by means of a variety of attacks.

2 Threats and Countermeasures

2.1 Attacks on Internet Banking

The first 'phishing' emails targeting on-line financial systems were seen in 2001, as a 'Post 911 ID check' following the September 11 attacks on the World Trade Centre[1]. From 2004 onwards, the industry has seen a dramatic rise in attacks against both large and small financial institutions worldwide.

In parallel with this growth in attack volume, there has been a parallel rise in the variety and complexity of attacks. Banking security experts must now be familiar with a bewildering array of techniques and terminology: phishing, pharming, spear phishing, session hijack, man-in-the-middle, man-in-the-browser, Trojans, Rock Phish…the list goes on.

Despite the diversity in attack methods, most aim to achieve the same objective: to obtain confidential user information, such as usernames, passwords, credit card numbers and social security numbers. These are all *static* credentials—they don't change—and therein lies the problem. Once obtained, they can be used by the attacker to impersonate the customer to perpetrate fraud.

---

[1] Source: http://en.wikipedia.org/wiki/Phishing

2.2 Two-Factor Authentication

Whilst it is useful to try to counter specific attacks (and as part of a layered security strategy, we would always recommend this), the only long-term, strategic solution is to move away from the current dependence on static credentials.

Traditionally, all authentication mechanisms can be placed into one of the following three categories:

- Something you **know**—a secret, such as a password.

- Something you **are**—a biometric, such as a fingerprint.

- Something you **have**—a device or object or some kind, such as a credit card.

With this approach, it can readily be seen that the problems with phishing arise from an over-reliance on the first category. Strong authentication can be achieved by employing two different authentication credentials in parallel, from *different* categories. This is known as *Two-Factor Authentication (2FA).*

For reasons of cost, complexity, reliability and privacy, biometrics are not widely used in banking. There are however a wide variety of low-cost, dependable security devices available.

Typically, such devices generate and display a *One-Time Password (or OTP).* As the name suggests, an OTP is valid for a single use only, and many are also time-limited. Rather than being static, OTPs are *dynamic*—new OTPs can be generated on demand, from an inexhaustible sequence that is unique to each device.

The OTP is copied from the device to the web terminal by the customer. To the bank, knowledge of a valid OTP demonstrates proof of possession of the device, which when coupled with a traditional static password can offer an extremely effective defence against on-line attacks.

2.3 Attacks Against 2FA

A small number of successful attacks against 2FA-enabled Internet banking systems have led to press reports that 2FA as a general approach has been 'broken'. The reality is rather more complex, as we shall discuss below.

An attacker may obtain a valid OTP from a customer using the same methods as those used to obtain a static password. If the bank has deployed a simple system with 2FA used for log-in only, this attack may succeed.

To understand how to mitigate or eliminate this risk, it is first necessary to understand how attackers operate. Rather than one individual or organisation being responsible, attacks are carried out by loose associations of individuals or groups, each with their own specialist role. Different parties cooperate, each providing a service: creating a fake web site, sending spam email, collecting passwords, and finally using those passwords to obtain cash.

Passwords and other credentials are bought and sold between groups. This takes time. Since most OTPs include an expiry mechanism, the attacker's standard operating model is no longer effective, and a considerably more complicated model of real-time attacks is being

adopted. This explains the continuing technological advances in on-line attacks which we discussed earlier.

Is this a never-ending arms race, or will there eventually be an outright winner? Happily, the strongest forms of 2FA available today offer a long-term, provably secure solution. The key is to move from authenticating the customer, to authenticating the transaction which the customer wishes to perform.

The user experience remains simple: the user simply enters the beneficiary account number and transaction amount into their authentication device, by means of an integral keyboard. The OTP thus created acts as a digital signature on those transaction details—even if obtained by an attacker, the OTP cannot be used for *any* other purpose.

Whilst this step may not be necessary today, many banks are deploying 2FA solutions with the option to upgrade to transaction authentication in the future. By this route, their customers first gain familiarity with the simplest form of the technology, and the bank is strategically placed to respond to future threats.

3 Deployment Options

3.1 Authentication Methods

Any bank considering deploying 2FA must choose between a wide range of possible authentication devices. The following list, whilst not exhaustive, gives a representative sample.

EMV Card and Reader

MasterCard has devised a scheme based on existing retail banking smart cards and PINs. Dubbed the Chip Authentication Program (CAP), it has also been adopted by Visa, under the Dynamic Passcode Authentication (DPA) banner.

The customer is supplied with a small, hand-held card reader, into which their existing EMV 'Chip and PIN' card is inserted. On entering the card PIN, the chip on the card is used to generate an OTP, which is displayed on the reader's screen. Additional functions on the reader also support transaction authentication.

The advantages include a high security, whilst by leveraging existing cards and issuance processes deployment and management costs are reduced. However, the user experience, whilst familiar, is more complicated than with other tokens.

Hardware & Software OTP Tokens

Many vendors offer OTP-generating tokens. They are available in a wide range of shapes and sizes, and many offer custom branding options.

The simplest tokens are suitable for user authentication only. More advanced tokens incorporate a keyboard, making them suitable for transaction authentication.
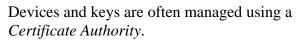
Most vendors employ proprietary algorithms to generate the OTPs. However, the Initiative for Open Authentication (OATH, see www.openauthentication.org) is an industry consortium promoting standardisation and interoperability.

Hardware-based PKI Tokens

A PKI system employs a *private key*, used to make *digital signatures* that are validated using a *public key*. The public key is held by the bank, and the private key by the customer.

Chip-card or USB devices are commonly used to secure the customer's private key. Since PKI tokens cannot generate OTPs, they must instead be connected to the customer's PC.

Devices and keys are often managed using a *Certificate Authority*.

They offer a high security level, although PC-based attacks may use the token illicitly. By including the ability to sign transactions and other instructions, they offer great flexibility to banking applications. As a result, they are more common in business banking than consumer banking.

Software-Based PKI Tokens

Rather than storing PKI private keys in a physical device, they can also be stored on the customer's PC, protected by software. By eliminating the device, such systems offer significant cost savings in distribution and maintenance.

However, the software-based signing key may be vulnerable to PC-based attacks, and since the key is installed on a particular PC, customer mobility is reduced.

SMS-based OTPs

An appealing alternative to deploying tokens is to use something the customer already has—their mobile phone. In this case, the bank generates the OTP and sends it to the customer as an SMS message. The customer returns the OTP to the bank through their web browser.

Naturally, this approach relies on the bank maintaining current details of the customer's telephone number and the customer being able to receive messages at the particular moment of logon.

Additionally, a transaction summary may be included in the SMS. This enables the user to detect fraudulently modified transactions.

AnyBank Online

To confirm payment of €500 to account xxxx4204, please enter the following security code: 394GYB

01	492380	11	803432
02	952334	12	342039
03	102875	13	689452
04	028942	14	439773
05	680328	15	569034
06	240935	16	184943
07	023941	17	439023
08	678304	18	649357
09	802439	19	093494
10	225894	20	748399

TAN Lists

TAN (Transaction Authentication Number) lists are paper-based lists of one-time passwords. They are securely generated by the bank and issued to each customer.

The customer provides an OTP every time she logs on or submits a transaction. The OTPs are either used in sequence, or the bank requests a specific OTP using an index.

Whilst offering a lower security level, this low-technology approach offers a combination of simplicity, reliability and low cost.

Matrix Cards

Also called grid card, this is a random grid of numbers or letters typically printed on a credit-card sized piece of plastic issued by the bank.

The customer is prompted to supply the contents of 2 or 3 cells during logon or when submitting a transaction. For example, the prompt "A4, C7" would give the log-on response "5, 8" using the card shown.

With similar advantages to TAN lists, the card format is convenient and durable. Whilst re-use of cells make the security analysis less clear, it also allows for a more flexible expiry policy.

3.2 Pros and Cons

To compare authentication methods, they must each be assessed against a range of criteria:

- **Customer acceptability**—ease of deployment and use, portability and reliability

- **Cost**—initial purchase, deployment, support, lifetime and replacement

- **Effectiveness**—how effective is it against a wide range of simple and advanced attack scenarios?

Table 1 below gives a simple comparison of the main features of the authentication methods discussed previously.

Advantages	Method	Disadvantages
Simple to use Timely authentication	Hardware OTP tokens	User authentication only on simple models Cost of tokens
Simple to use Many users already carry capable smart phones Timely authentication Low cost	Software OTP tokens	User authentication only on simple applications Applications can be compromised
Transaction & user authentication Card PIN provides 2nd factor—no need for separate password Simple deployment	CAP/DPA	Cost of card readers Possible card reissuing costs Usability for some customers
Small form-factor Low cost Easy to use	Matrix card / TAN list	User authentication only Lower security level Easy to copy Relatively short lifetime
Transaction & user authentication Timely authentication Low initial cost Most users already carry mobile phones	SMS	Customer management expensive Availability to all customers Availability of coverage Ongoing cost of SMS messages
Transaction & user authentication Highly secure digital signature	PKI token (hardware / software)	Low user mobility Vulnerable to PC Trojans Hardware costs (high) High integration and support costs Internet channel only
Useful as second factor Familiar to all customers	Static & partial password / PIN	Very low security if sole method Password reset/PIN mailer costs

Table 1: Comparison of authentication methods

4 The Business Case

As we have seen, there are a wide range of two-factor authentication devices available, each with their own advantages and disadvantages. Combined with vendor spin and confusing media reporting, this often leads to confusion and internal conflict within the bank as to the best approach to take. Given the large investment required, and the visibility of the decision to customers, the end result can be procrastination and delay.

A business case for 2FA should not be based solely on 'fraud minus cost', as this is overly simplistic. Additional factors including potential loss of business, reputational damage, cost savings and opportunities for growth need to be considered to ensure a broader and more accurate business case is created.

4.1 Customer Acceptance

The most important factor to consider is *always* customer ease-of-use. People will simply not use systems they find difficult, and so a positive customer response is essential to the success of any deployment. Also, with large banking customer bases, if even 1% of customers require telephone support, the total deployment cost increases dramatically. The authentication method or mix of methods selected must be simple, intuitive and reliable.

Customer attitudes towards a particular 2FA technology are best established through market research. Whilst internal opinion-gathering can act as a rough guide, it is important to remember that bank staff are not a good representation of customers in general. Surveys of customer opinion often produce surprising results, which only serves to underscore their value. By obtaining meaningful data, sufficient assurance of customer acceptance be demonstrated, thereby resolving internal debate and enabling additional resources to be committed with confidence.

4.2 Customer Confidence

Several customer surveys have highlighted security concerns as obstacles to the uptake of Internet banking. They are also frequently cited as a major factor in people moving away from on-line services to more expensive channels.

2FA is unique amongst anti-fraud technologies in its visibility to the customer, and is therefore uniquely placed to placate such fears. Conversely, the impact to consumer confidence and reputation of doing nothing, whilst the attack emails and media reports continue, must not be underestimated.

Being seen to be secure can help to achieve business targets by driving the uptake of Internet banking. Even for existing web users, increased confidence leads to increased usage for a wider range of transactions.

Visibly better security can also act as a competitive differentiator to boost migration from other banks, either for security reasons or because a more appealing technology is offered. Placing a device in every customers' wallet or pocket is also a powerful marketing opportunity, an ideal vehicle for driving brand awareness.

4.3 Fraud and Risk Reduction

Any assessment of potential savings arising from fraud reduction must start with current fraud levels. Extrapolating from past data to project future losses typically shows a growing exposure.

Any such estimates must also take into account the intrinsic insecurity of non-2FA systems, and the rapid ability of attackers to package and commoditise today's advanced attacks to deliver them *en masse* tomorrow. Failing to invest in 2FA can be seen as a 'ticking bomb', waiting for a fraud explosion.

In addition, it's important to recognise the fraud where it is occurring. Most banks currently refund defrauded customers in full, leaving the bank open to first-party fraud. Whilst this can be addressed through careful processes, these are costly and time-consuming. By forcing active customer participation in each transaction, 2FA reduces the opportunity for first-party fraud and increases the scope for the bank to disclaim liability in suspicious cases.

Lastly, card-not-present (CNP) fraud must be considered alongside Internet banking fraud. E-commerce transactions can be secured by integrating 2FA into 3-D Secure systems (MasterCard SecureCode / Verified by Visa). In some countries, this approach is being extended to incorporate mail order and telephone order (MOTO) transactions.

4.4 Additional Cost Savings

Having considered a range of direct benefits, indirect benefits must also be considered.

By using 2FA to present a more difficult target, the overall volume of attacks is likely to be reduced. Operational costs in researching and shutting down such attacks are thus reduced, freeing resources for more productive work. A similar workload reduction for front-line staff currently handling fraud claims can also be expected.

In addition, once deployed and proven effective, 2FA may allow current expenditure on complementary anti-phishing technologies and services to be reduced or even eliminated.

Finally, deployment of 2FA technology may enable existing processes elsewhere to be re-engineered, with considerable cost savings. One UK bank realised that 2FA enabled them to automate their call centre customer authentication process—the resulting savings were sufficient to cover the *entire* deployment costs. Strong, automatic customer authentication also increases the range of services that can be offered without the involvement of an operator.

4.5 Deployment and Maintenance Costs

Having considered the full range of potential benefits, it is of course essential to consider the full costs, and to devise a strategy to extract the greatest return on the necessary investment.

Device costs comprise the initial purchase price, together with the costs associated with packaging and delivery. Reliability and robustness must be taken into account when calculating re-issuance costs due to device failures, and the lifetime of the device also considered. Market acceptance of charging either for the initial device or for replacements varies between countries.

The second component to consider is the cost of the necessary supporting infrastructure. Rather than tightly coupling the 2FA system to the Internet banking application, a dedicated

authentication system offers numerous advantages: it allows multiple applications and channels to leverage the investment; it provides a consistent user experience across applications and channels; and it reduces the Internet banking development resources required.

Large banks typically offer a range of products to a variety of market segments. Each product has its own security requirements, and its own budget, and there can be a huge variation in acceptance of authentication technology across different customer groups. A central authentication server must therefore be sufficiently flexible to offer a hybrid approach, in which certain products or customers use one kind of authentication, whilst a different approach is used in parallel elsewhere.

As well as being better able to support today's requirements, a flexible authentication server can enable longer-term cost savings. By not tying the bank to a particular vendor, on-going device costs are more easily controlled. And the ability to switch devices or device modes enables the bank to react rapidly to new attacks.

The final component in the cost calculation is resource costs: project management, development, operations and customer support. An efficient and effective infrastructure strategy minimises the first three of these; the last must be addressed through careful choice of a simple authentication method coupled with clear customer communication, refined through experience obtained by an initial pilot deployment.

5 Cryptomathic Offerings

As a leading security vendor specialising in the financial sector, Cryptomathic has helped to secure Internet banking solutions for more than a decade. Having obtained a unique insight into banking requirements for authentication systems, Cryptomathic is able to offer a complete range of 2FA solutions.

Central to these are the Cryptomathic Authenticator and our complete range of PKI products. These proven products are available today.

5.1 The Cryptomathic Authenticator

The Cryptomathic Authenticator forms the cornerstone of our authentication offerings, as an authentication server designed specifically for banking applications. In contrast with other authentication systems, the Authenticator offers a unique combination of advantages:

- A **token-vendor independent**, modular architecture

- **Best-in-class security**, through use of **Hardware Security Modules** with custom firmware

- **Strong administrative controls**, especially for critical key management tasks

- **Simple integration** into existing systems

- A flexible, scalable **token management** system designed for consumer deployments

- **High performance and availability**, through redundancy and clustering

- **Tamper-evident** audit logging

By being token-vendor independent, Cryptomathic is able to offer the broadest range of options to our banking customers and enable them to negotiate the best possible prices on authentication devices. The flexibility to change authentication methods also ensures long-term value from the investment in our infrastructure, regardless of future attack and authentication trends.

Smart Phone App & SMS · Display · CAP · OATH Token · USB · Authenticator · Fax · Gridcard · Proprietary Token · Static & Partial Password · Digital Signatures · CodeSure

For a banking authentication server, it is crucial that the management of secret information is secure, be it a token key, static password, or similar, that is shared with the customer but which must not be shared with any other individual. Clearly, a compromise of these authentication secrets would be disastrous for the bank. In addition, to ensure that customer actions cannot be repudiated, the bank requires the ability to demonstrate, to a high level of certainty, that such a compromise could not have occurred.

Such assurance can be achieved only with strong technical and procedural controls, both of which are fully supported. Central to this is our use of Hardware Security Modules (HSMs)—secure, tamper-proof hardware devices which have exclusive control of the server-side authentication secrets.

Managing the secure delivery and registration of authentication devices is a critical step in any 2FA deployment. The Cryptomathic Authenticator supports this process either through our own Token Manager server, or via third-party or in-house systems.

The product offers straightforward integration with most banking infrastructures. A remote administration client offers easy management of the system, which is usually clustered to ensure continuous availability.

Cryptomathic has unrivalled experience in developing HSM-based systems, and our R&D facility includes a world-class HSM programming team with unrivalled experience. Cryptomathic works with a wide range of HSM vendors, again offering our customers vendor independence.

5.2 PKI Solutions

As we have seen, PKI-based authentication solutions differ from OTP-based schemes in that a PC-connected (or software) device is used to manage the user's private key. Each approach has its own advantages and disadvantages, and either may be appropriate depending on the requirements of the business application. A PKI offering is therefore an essential part of any complete authentication package.

Cryptomathic has been delivering PKI solutions over 10 years. Our offering includes a full suite of PKI products:

- **Certificate Authority**, for issuing and managing certificates and revocation lists

- **OCSP Responder**, for real-time, on-line certificate status checks

- **Time-Stamping Authority**, for independent audit-keeping and non-repudiation

- **The Signer**, a central, server-based alternative to device-based user private keys

- **Cryptographic toolkits**, for certificate handling and application integration

Each of our PKI servers shares the operational and security advantages of the Authenticator: high security (including HSM support), tight procedural controls, scalability and redundancy through clustering, and tamper-evident audit logging. And since all our PKI products are standards-based, they can integrate out-of-the box with other PKI systems from other vendors.

5.3 EMV Solutions

The MasterCard CAP / Visa DPA authentication system described earlier leverages EMV ('Chip and PIN') payment cards to provide a strong 2FA solution.

Cryptomathic has worked with EMV since its inception, our CardInk data preparation product being widely used by banks and bureaux worldwide to issue millions of cards every year. Our systems have been issuing CAP-compliant cards since 2004.

By translating this in-depth EMV experience to the Authenticator, we were able to take a pro-active role in implementing CAP validation support. The Authenticator has been certified by MasterCard as a CAP Token Validation Service (CTVS) since March 2006.

CRYPTOMAThIC

5.4 Benefits of Working with Cryptomathic

Working with Cryptomathic on securing Web banking you will experience a number of technical and business benefits:

- **Comprehensive offerings in 2FA**—from tokens to PKI to consultancy services.

- **The most innovative, skilled and experienced company in banking 2FA**—with over 10 years experience of large-scale banking authentication projects.

- **The highest degree of flexibility on the market**—a complete range of authentication methods, not tied up with any token or HSM provider, and able to match any requirement for peak performance and availability.

- **The most secure solution**—designed for banks and other financial-sector institutions, using specialised Hardware Security Module code and the highest security standards including tamper-evident auditing and tight access control.

- **Prime contractor capability**—taking full responsibility for the coordination and integration of other suppliers, including device vendors and distribution bureaux.

- **A trusted technology provider**—we have successfully lead comprehensive 2FA projects with high-street banks including Lloyds TSB (UK) and LuxTrust (Luxembourg).

6 About Cryptomathic

6.1 Company Background

With 25 years of experience, Cryptomathic is one of the world's leading providers of electronic security solutions. We specialise in commercial cryptography, and assist our customers in securing their businesses by providing best-of-breed security software products and technologies together with consultancy and education.

Our extensive expertise in the financial services industry has been achieved through investment in research and development and by providing customers worldwide with both product-based and tailor-made solutions. Our product portfolio ranges from cryptographic tools to large-scale server applications, such as the Authenticator for banking authentication, and CardInk, a data preparation product for card issuing.

Our customers include banking organisations, central banks, commercial banks, card bureaux and transaction processors, as well as other large corporations outside the financial sector. They are served through our offices in Denmark, the UK and Germany.

6.2 Further Reading

For further reading on the topic please consult the following resources:

- The Cryptomathic Web site: http://www.cryptomathic.com

- The Cryptomathic Authenticator Technical White Paper

- The EMV Go CAP—the end to end payment card solution (www.emvcap.com)

- The Future of Phishing, Cryptomathic Newsletter 'NewsOnInk' #2, 2004

Please contact us for more information—you will find our contact details on page 2.