Bio ID – Secure Communication Product Review

Author: Prof Bill Buchanan 25th March 2015

1 Executive Summary

The **Bio ID Enterprise Suite** shows great potential in the market place, and addresses many of the problems within electronic mail, and within any other form of passing highly sensitive messages from one person to another. It has been designed with scale and trust in mind, and will easily scale into a corporate infrastructure, especially where there is trust between organisations. Many existing products do not scale well, and are often customized plug-ins for email clients. The architecture for **Bio ID Secure Communication** has been designed in a way that defines a core trust infrastructure, where two organisations can trust the **Bio ID J2EE Server** infrastructure to secure the fingerprint signatures and in the distribution of encryption keys. Every aspect of the communications and in the encryption elements has been reviewed, and it has been designed using the best available technologies. The main focus of the product is on the Microsoft Windows integration, especially into Active Directory infrastructure, which is a good approach, especially in a roll-out across an organisation. Further development of a mobile app plug-in will see great benefits, especially in providing fingerprint signatures which are integrated into devices.

The key market is in DLP (Data Loss Prevention), especially in high-risk areas such as in the finance industry, the energy sector, corporate acquisitions and mergers, homeland defence, the public sector and law enforcement. With the increasing requirements around data protection, organisations will have to show that they protect data in every state that it can exist on the network. Along with this the increasing usage of Cloud-based systems exposes companies to large-scale data loss, especially from insiders and/or privileged access. The **Bio ID Enterprise Suite** completely covers this aspect, as it encrypts the data at source, and with the chosen biometric technology of the sender and recipient. Any accesses to the data, no matter where it is stored, will be protected. With the application of access policies, the product has the potential to scale to multiple methods of authentication, including face recognition and IRIS scans, along with creating an extensible access policy, where things like location and other attributes can be integrated.

BIO ID Enterprise Suite

The BIO ID Secure Communication product forms part of the **BIO ID Enterprise Suite** and is structured as:

- **J2EE Enterprise Server** (acts as root server for bio certificates as well as administrator for all certified BIO ID Enterprise Servers)

- **BIO ID Enterprise Server** (extension of the MS Active Directory schemata in a MS 2008R2 or 2012R2 server domain)
- **BIO ID Logon** (extension of the credential provider to replace passwords with chosen biometrics to log onto clients in a domain network – can also be used for stand-alone-clients)
- **BIO ID Secure Application** (API for any application – server or client side – to replace passwords with chosen biometrics)

2 Context

The protocols which have been developed on the Internet are inherently insecure, and three of the worst offenders are related to the sending and receiving of email: SMTP (Secure Mail Transmission Protocol); POP-3 (Post Office Protocol-3); and IMAP (Internet Message Access Protocol). Currently email suffers from many inherent problems, including:

- **Lack of authentication of the sender and recipient.** Overall SMTP is used to send email and POP-3 and IMAP for reading email, but they often lack any security, and they often cannot be trusted to verify the sender of the email, or that the email has not been changed in some way. Newer protocols, such as SMTPs, aim to improve the security of email, but often only protect the sending and receipt of an email. The authentication of the email is thus a machine-to-machine one, and not a person-to-person one, where there is a complete end-to-end tunnelling of an email from one person to another (Figure 1).
- **Exposure to large-scale data loss**. The recent Sony hack highlights how easy it is for an insider, or an outsider with pre-installed malware, to create a large-scale export of the contents of a Microsoft Exchange email server to a PST file, and then tunnel it out of the network. Along with this there are greater risks around the usage of mobile devices which have single sign-ons, and where the authentication is focused on a single authentication to the whole of the user's Inbox.
- **Lack of access control on emails.** Few too organisations have proper classifications for their email classifications, where low risk ones are treated with the same access requirements as high risk ones. The systems they use can often be used internally, but many struggle to cope with sending and receiving encrypted emails from trusted third parties.
- **The crisis in passwords and PKI.** The security of the Internet has been on passwords and the PKI (Public Key Infrastructure). Passwords can now only be seen as one method of identifying a person, and many passwords systems can be easily breached. Along with this, the loss of a private key for an organisation can cause large scale data loss. Few people, even experienced security professionals, actually fully understand how PKI works, and it can thus never be completely trusted by users.

2.1 Some basics

There are three main methods of encryption: symmetric key; asymmetric key; and one-way hashing. Normally all three methods work together to create the secure infrastructure (Figure 2):

- **Symmetric key encryption**. With this we have a single key which is used to encrypt, and then the same key is used to decrypt. Typical methods for this are AES and 3DES. These methods are highly optimized, and allow for fast processing, with typical key sizes of 128 bits and 256 bits. We normally define this method as **private key**.
- **Asymmetric key encryption**. With this we have a key pair, where one key is used to encrypt, and the other is used to decrypt. Typical methods for this are RSA and ElGamal, with typical key sizes of 1,024 bits, and 112 bits, respectively. The public key of a recipient can be used to encrypt data sent to them, but more commonly it is the private key of the sender that is used to prove the sender's identity. We normally define this method as **public key**.
- **One-way hashing**. With this we have a one-way mathematical function that is difficult to reverse. Often we use hashing methods to provide the integrity of an entity, where we produce a fixed length code for the entity we wish to prove. Typical methods include MD5 (which is a 128-bit hash code) or SHA-1 (which has 160 bits).

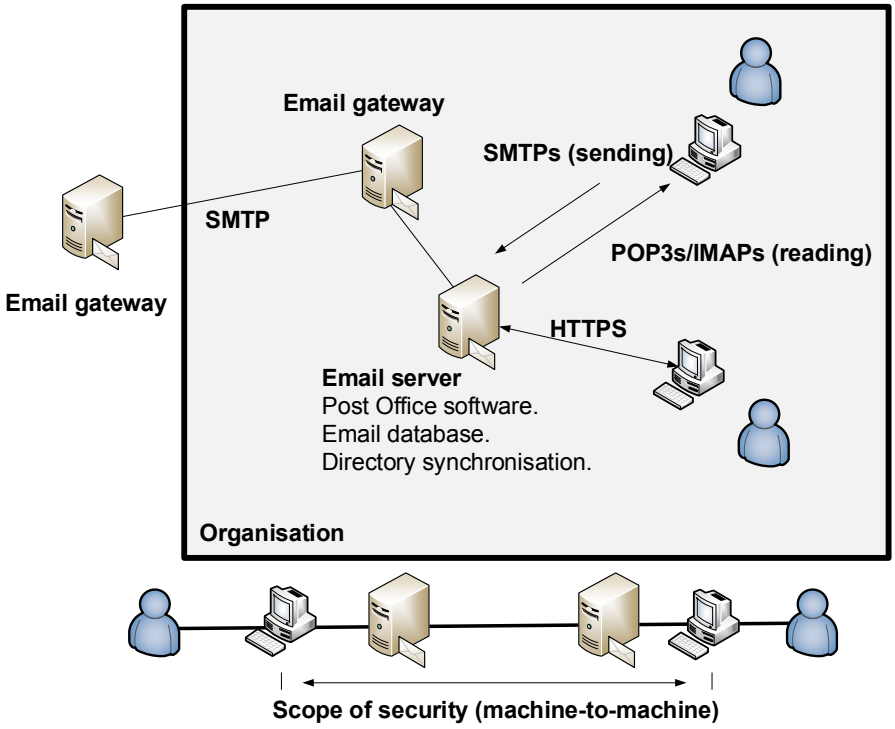

Figure 1: Overview of email

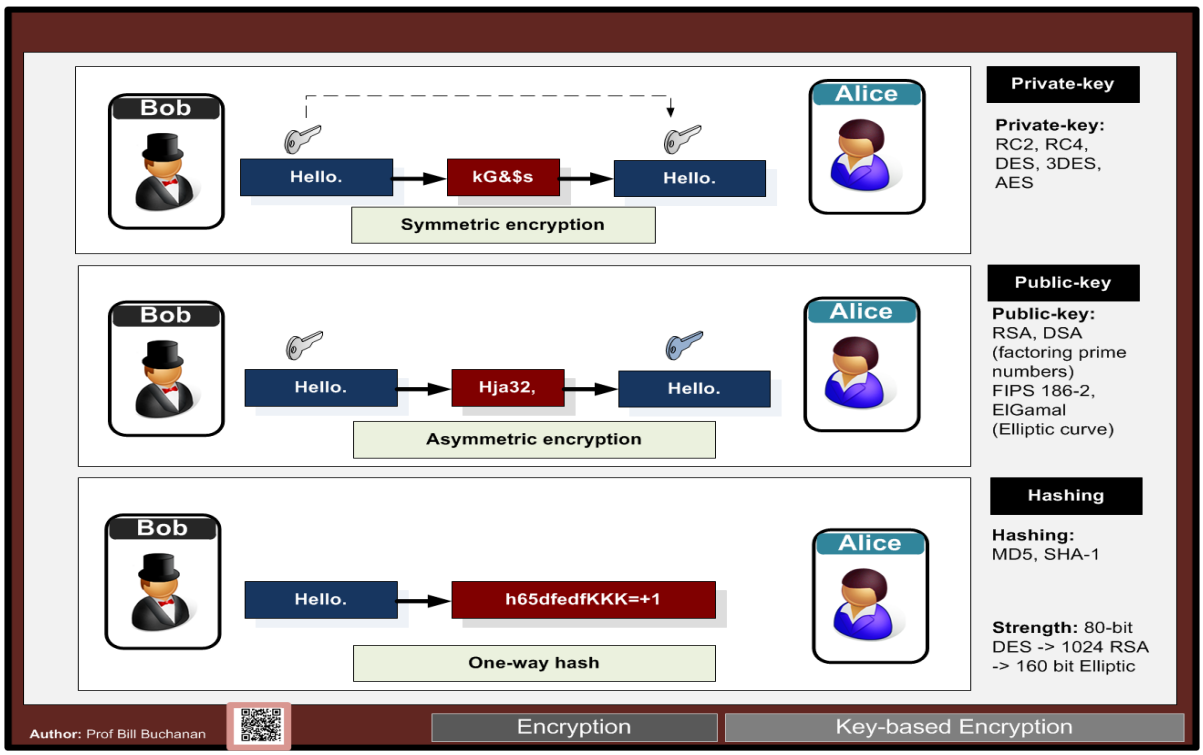

Figure 2: Encryption methods

Normally all three of these methods work seamlessly together. Figure 3 outlines how Bob can send secure messages to Alice. Bob uses Alice's public key to encrypt the data to her. To prove his identity he takes a hash signature of the data and encrypts it with his private key. He adds this to the data, and then encrypts the whole lot with Alice's public key. Alice then decrypts this with her private key, and can view the data. She then decrypts the hashed value with Bob's public key, and then compares the hash value that he has generated with the hash value that she calculates from the data. If they are the same, then she has proven the identity of Bob (as only he has the private key which matches the public key that she used to decrypt the hashed value), and also have proven the integrity of the data. The method typically used for Bob to get Alice's public key is to access a digital certificate which contains her public key, and which has been verified by a trusted identity provider (such as from Verisign or GoDaddy). In the same way, Alice gets Bob's digital certificate to gain access to his public key (Figure 4).

The two problems with the method defined above are that we need to pass digital certificates for both Bob and Alice, and public key encryption is often processor intensive when we have large amounts of data. With RSA, key sizes up to 1,024 bits have been cracked, and many think that larger key sizes can also be broken by the NSA. Thus 4,096 bit public keys are now recommended, in order to keep the messages secure for a few years, as many believe that the RSA method of public key encryption will come under increasing pressure due to improved factorization of the prime numbers involved in the RSA process. Thus, it would be difficult to implement public key

encryption for large email messages, especially with attachments (note that an email message and all its associated attachments are sent as a single entity).

PGP (Pretty Good Privacy) was developed by Phil Zimmerman, and overcomes the problems around public key encryption, as it uses the concept of a key ring for the public keys of trusted entities, and it uses private key methods to encrypt all of the email contents.

The PGP method of email encryption thus generates a one-time private key to encrypt the message, and then takes a hash of the message and encrypts this hash with the sender's private key (and which will be used to prove the identity of the sender). Both the email contents and the encrypted hashed value are then encrypted with the one-time private key. Next the private key is encrypted with the public key of the recipient, and added to the encrypted message. At the end other the recipient takes the encrypted key, and decrypts with their private key (from their key pair), and can reveal the one time key used to encrypt the message. They can then read the email, and now need to prove the sender. For this, they take the encrypted hashed value, and decrypt it with the sender's public key. If the hash matches the contents of the message, they have proven both the sender of the email, and also that the contents have not changed. In this way, we have CIA – confidentiality, integrity and assurance.

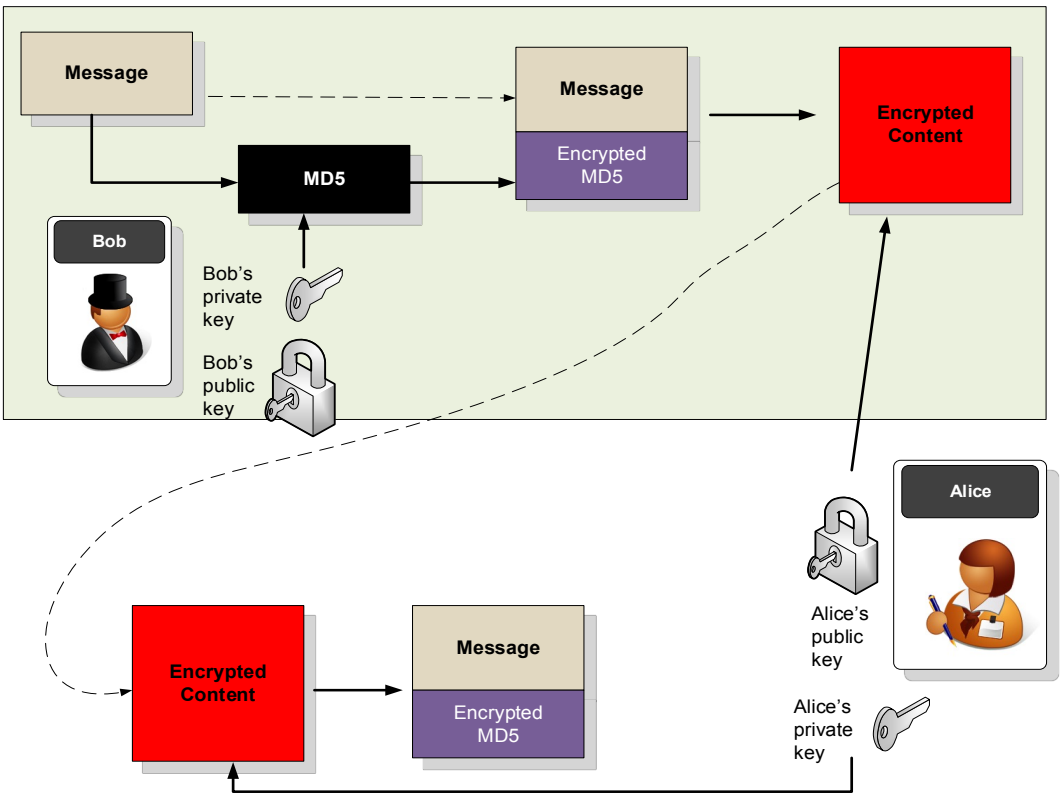

Figure 3: Encrypting data for Alice.

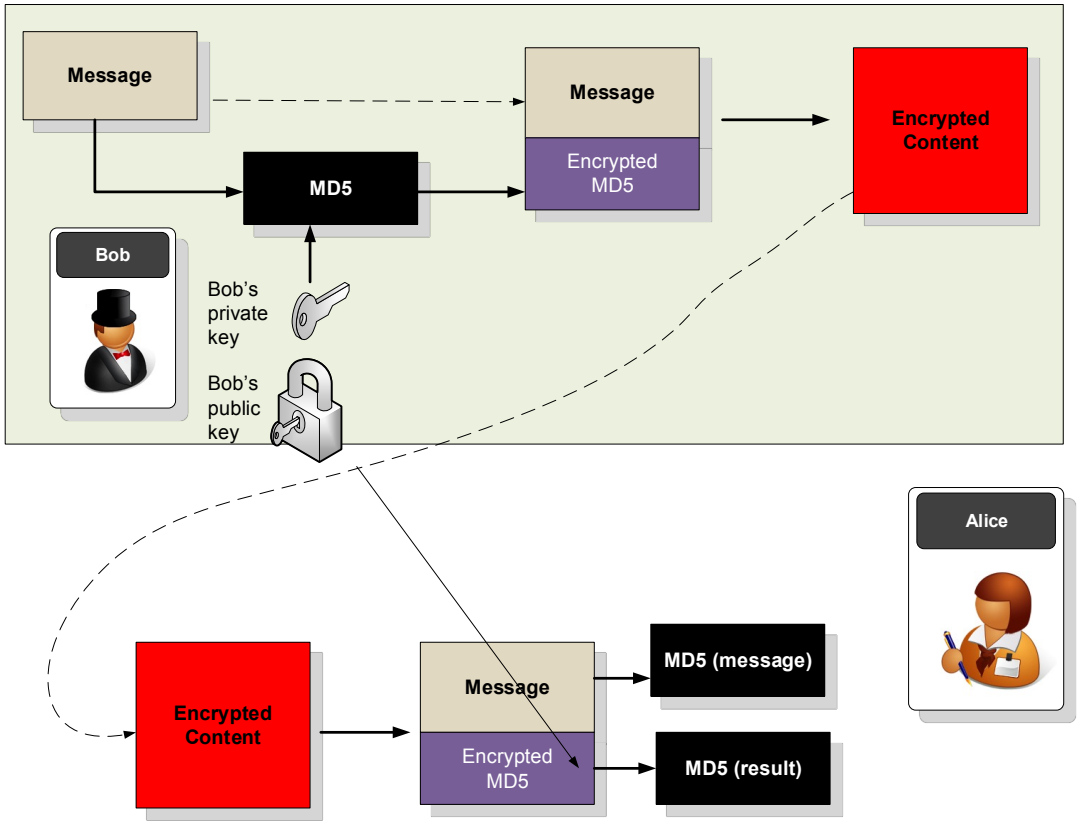

Figure 4: Generalised proof-of-identity

2.2 Data Loss Prevention

Bio ID Secure Communication aims itself in the Data Loss Prevention (DLP) market, and aims to create a complete person-to-person tunnel of email, where biometrics are used to authenticate both entities, along with securing the transmission, processing and storage of the message. Overall DLP is a growing market, especially after Edward Joseph "Ed" Snowden who, in June 2013, leaked classified information from the National Security Agency (NSA) to the mainstream media. As with many large-scale data leaks, he worked from the inside of the company and was a system administrator at Central Intelligence Agency (CIA). Chelsea (Bradley) Manning also highlighted the problems around the insider threat, when in August 2013 he leaked hundreds of thousands of classified documents to WikiLeaks, which was setup by Julian Paul Assange. The recent Sony hack actually shows a timeline of many years of problems around APT (Advanced Persistent Threat).

DLP continues to grow as a market, and the sell typically focuses on:

- **Audit/Compliance**. With Audit/Compliance, companies will often have to comply with an audit/compliance, such as PCI-DSS (for Finance) and HIPPA (for Health Care).

- **Direct Losses**. The Direct Losses can often be clearly defined, such as with investigation costs, customer compensation, litigation, and so on. In the finance industry, the fines can be heavy, such as where the FSA hit Zurich UK with a fine of £2.75 million for the loss of 46,000 customer details.
- **Indirect Losses**. Indirect Losses is often the major sell in DLP, such as a falling in share price, company reputation, and loss of customer faith (Figure 5). The effects on brands can have a long-term effect on a company, especially within areas such as the finance sector, the public sector, and other areas that have sensitive information. Electronic mail is often one of the most sensitive areas within data loss, where personal information can often be included, and a large-scale loss of emails can lead to a great deal of embarrassment.

The market for DLP splits into four main areas (Figure 6): standard security methods; encryption and access control; DLP Solutions; and Advanced Security systems. At the core of any secure system must be the encryption policy, especially on sensitive documents. Most DLP solutions focus on detecting signatures of activity related to *in-motion*, *at-rest* and *in-process* (Figure 7). Unfortunately these systems do not provide a complete end-to-end solution, and intruders and insiders can often hide data taken from an organisation within encryption tunnels, compressed files or can take the data off-site through an SD card. **Bio ID Secure Communication** protects against all the states the email can be in: stored on system (data at-rest), being transmitted or read (data in-motion) and loaded into memory (data in-process). Figure 8 outlines the possible methods that occurred of data loss in the Sony hack, and where all of the methods that could have been used, and many companies can be exposed to each of these, especially for privileged access to data.

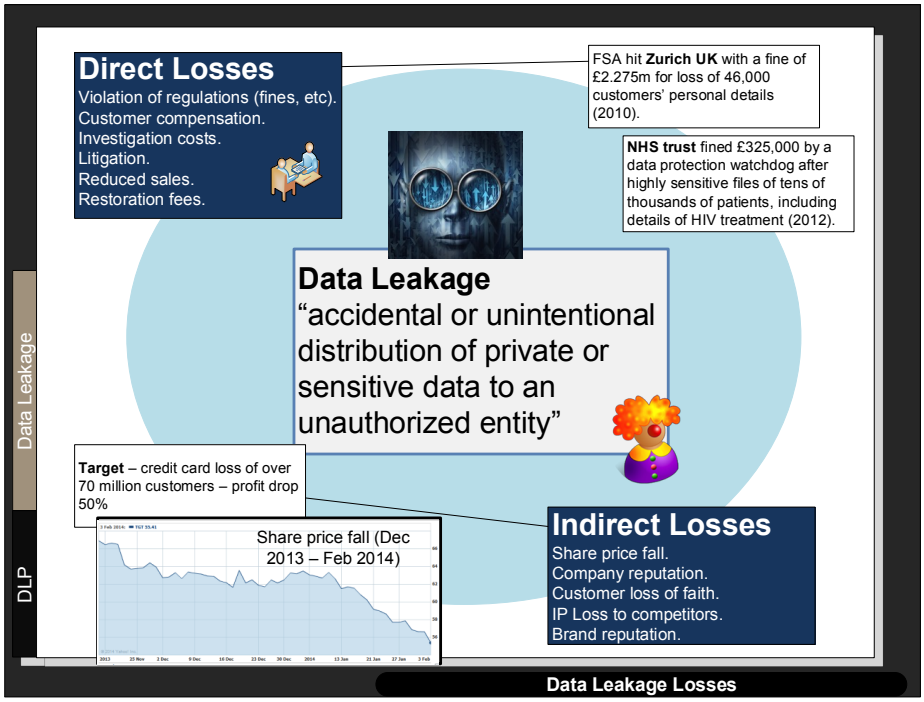

Figure 5: Data Losses

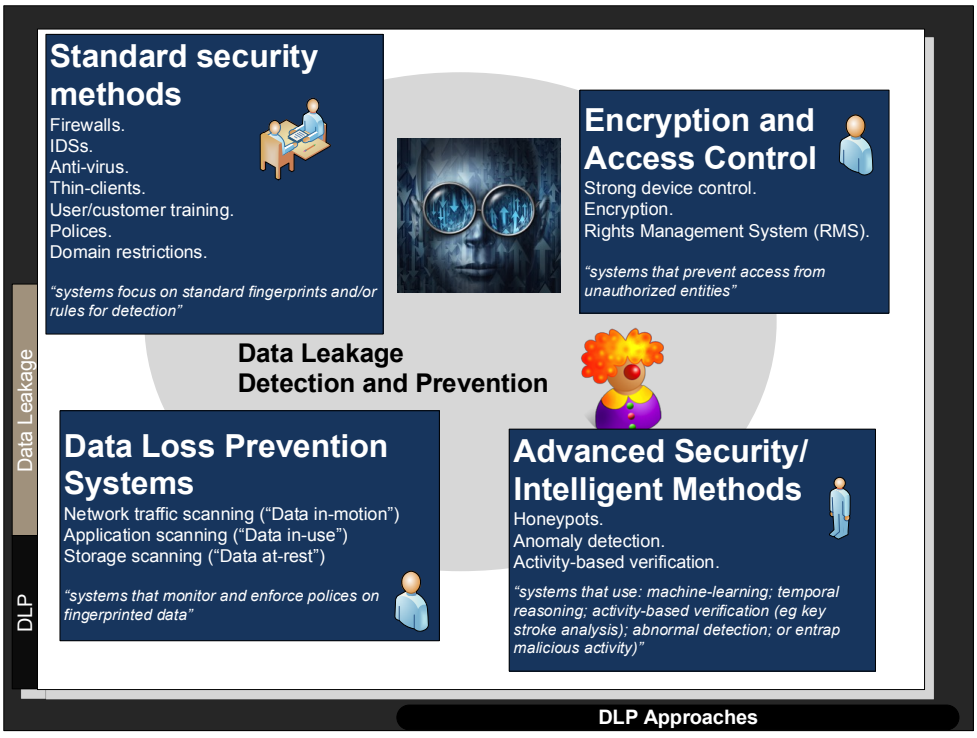

Figure 6: Data Losses

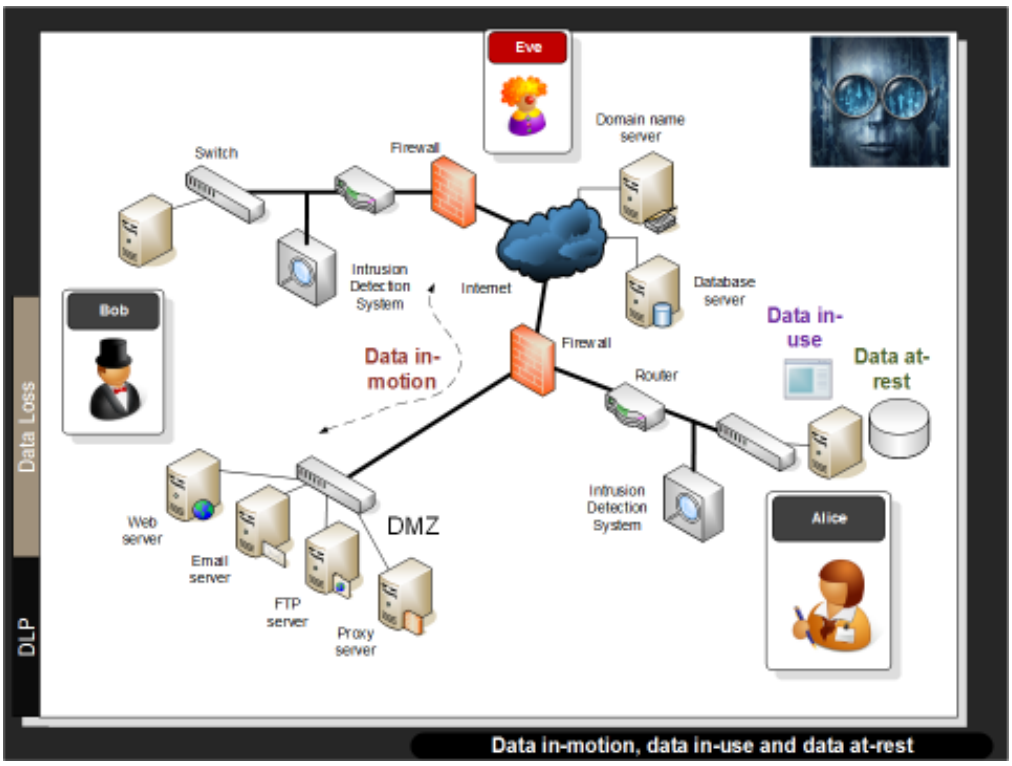

Figure 7: Data at-rest, data in-motion and data in-process

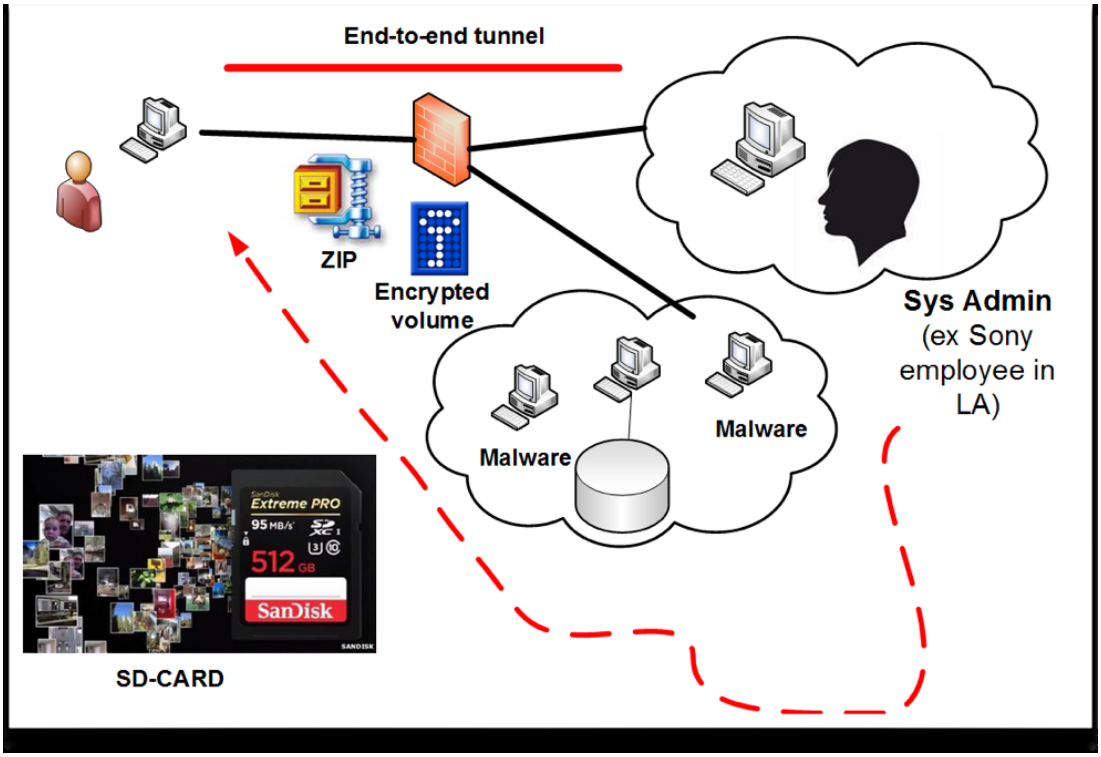

Figure 8: Possible methods used for data loss

Increasingly companies will have to prove that they provide security in every aspect of states that data can be in. While network communication can be seen to be relevantly secure in terms of the transmission of the data, such as using secure sockets (SSL and TLS), it has been seen recently with FREAK and Heartbleed that these secure connections can often be breached using weak keys, or with the usage of a proxy agent to act as a man-in-the-middle. The Superfish example even compromised the browser activity with a **man-in-the-browser** type compromise.

Most secure systems suffer from only protecting the layers of the networking stack, and the only true way of protecting data is to encrypt the data itself, and send over the network. In this way, even if the communications, processing and/or storage of data was compromised, the data would still be protected. This applies to electronic mail as it exists in each of the three states, and it is the *at-rest* state which can be the most sensitive for data leakage. Along with this, many organisations use proxy systems to allow scanners to inspect the contents of network accesses. Thus the data is often insecure from the user to the proxy (Figure 10), which can leave many risks for highly sensitive information, especially from an **insider threat.**

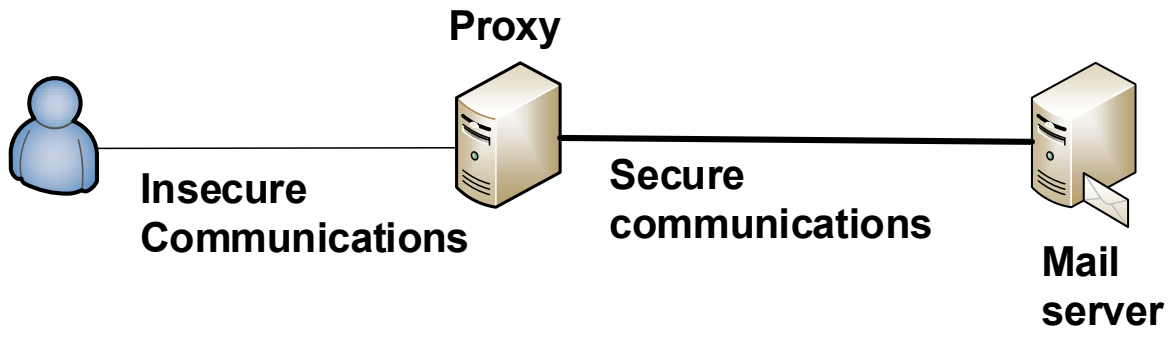

Figure 9: Proxy systems

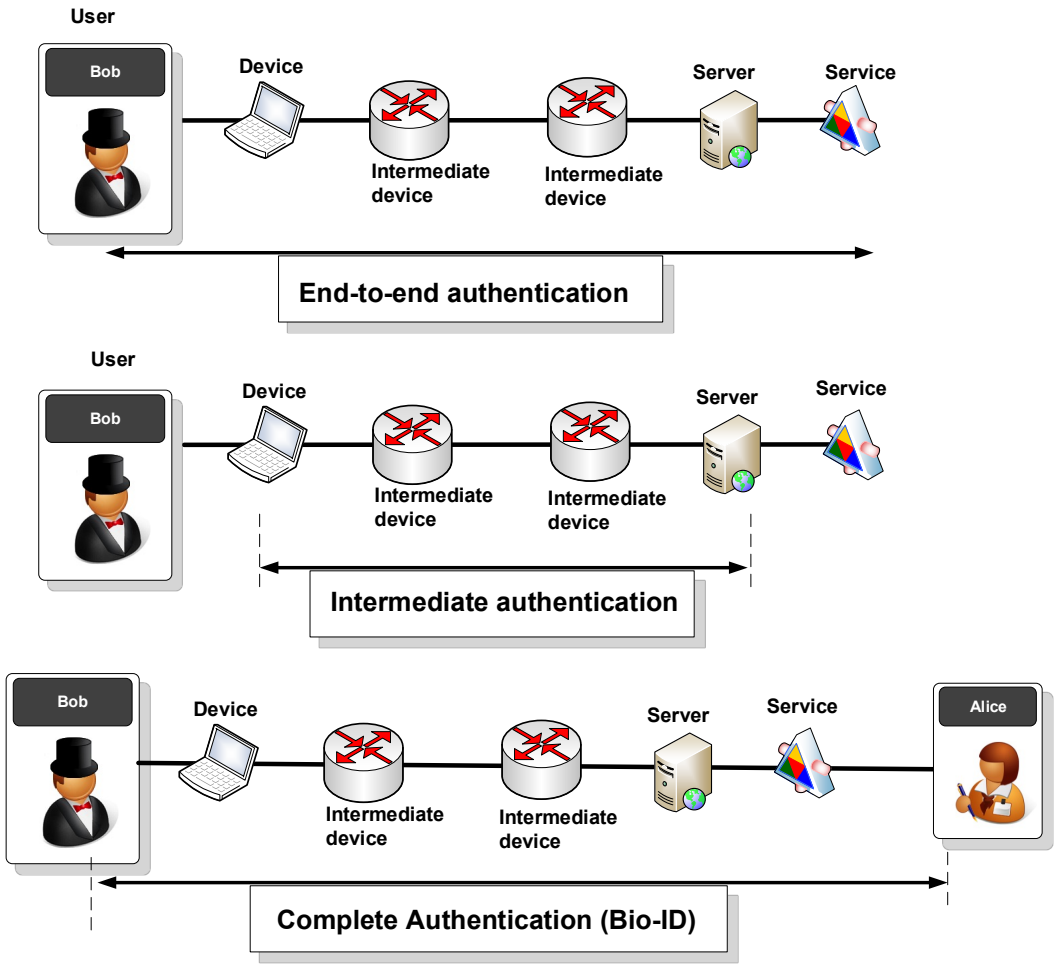

Figure 10: Different type of authentication

3 Review of existing methods

3.1 Outline

Currently most systems are based on PKI (Public Key Infrastructure) where a public key is used to secure the encryption key used in protecting the contents of the email, and a private key is used to sign the email. This includes:

- **Secure email**. The email contents are secured with a session key, and then this key is secured using the public key of the recipients (Figure 3). Only the recipients can decrypt the key, and unencrypt the contents. The sender must thus send the recipients their public key for this process to take place (normally done through sending the recipients' digital certificate).
- **Signing of the email.** The sender normally takes a hash signature of the email contents, and then encrypts this with their private key. When receiving the secure email, the recipient must use the public key of the sender to authenticate them, and

decrypt the encrypted hash signature. If the recipient gets the same hash signature for the contents, both the contents of the email and the sender have been verified.

These types of approach are flawed in sending email, including for example:

- Digital certificates with private keys are used for the signing and the securing of the email, and these could be easily stolen, or even replicated.
- Whoever can gain access to the recipients' digital certificates can read their emails.
- The digital certificates require complex installs on hosts, and often require complex trust policies.
- The digital certificates which are transferred with signed emails are often blocked as a security risk on many email systems.
- Key rings for storing encryption keys are often complex to manage and difficult to secure.

The usage of end-to-end email thus requires an improved method to not only secure the email but also to verify both the sender and the recipient.

3.2 Level of identity checking

Many systems suffer from not properly proving identity properly. Figure 10 outlines three different methods. With intermediate authentication, we typically authenticate a device to another device, such as an email server sender to the email server which is receiving the data. Unfortunately there is no way to verify that each of the users are actually connected to the associated devices. With end-to-end authentication, we can verify the user to the end service, which improves the security of the secure communications channel. Again it suffers from not knowing if the recipient is the one who actually connects to the email server. Bio-ID overcomes all of these problems, as it authenticates the recipient directly with the sender, and the data tunnels securely through the whole of the network infrastructure. Even those administering the email infrastructure cannot get access to the email data, as the message uses biometrics to generate the key to encrypt the email.

Increasingly passwords are becoming a problem area for security, where anything up to eight characters can be easily cracked in the Cloud. Passwords which are greater than this are often easily crackable, especially where weak passwords are used, and where social engineering can be used to gain access to a password. The industry is thus moving towards multi-factor authentication for high risk access, focusing on (Figure 11):

- **What you know** (your password)?
- **What you have** (such as an RSA token key)?
- **Something you are** (such as your fingerprint)?

Also increasingly we have an extra attribute of: **somewhere you are** (such as the GPS location generated from your IP address).

With high-risk emails the usage of passwords is extremely difficult, as both sides would have to agree to the password, and pass it through a secure channel (typically known as an *out-of-band* message). Bob could send Alice an email and then send an SMS message with the password of “5inkTh35hip”. It is unlikely that Eve will get access to both Bob’s emails and his mobile phone, so it will be relatively secure. Unfortunately it is not really scalable, and is still open to snooping.

Many users now encrypt their disk, and then use a token key to generate the password code so that they can access their system. This would not work with email, as every email message would require a unique key to access them.

The most natural way to protect every message and also to prove the users on either end is to use biometrics. Many biometric methods suffer from issues related to repeatability (can the attribute be repeated each time?), distinctiveness (does the attribute change effectively between differed users?), universality (is the human attribute universal for all?), acceptability (do users want to use it?). While iris scans are fairly good for repeatability, users do not like staring into a scanner. Palm prints are also fairly good for acceptability, but they are not distinctive enough. Fingerprints, of all the methods, probably cover the identity of the sender and the receiver best when secure emails are used.

Bio ID Secure Communication has thus focused on the right biometric method for the product, but could easily integrate other methods, including face recognition and iris scanning.

Figure 11: Multi-factor authentication

4 Competing product review

The main focus of existing products are Microsoft Exchange plug-ins and Data Loss Prevention tools. Overall the plug-in tools are compromised by storing encryption keys on the server, and few use biometrics for the confirmation of identity.

4.1 PGP (Pretty Good Privacy)

The solution to secure email within many companies is to use PGP either to directly send and receive emails, or to automatically intercept emails that look as if they contain sensitive information. With PGP, users generate their public and private key pairs, and then forward their public key to the sender for them to add the recipient's key to their key ring.

This method suffers from many problems, including:

- **Non-technical users.** The method works well with highly technical staff who understand cryptography. It will not work with most users, and often an automated method is put in place by the system administrators that will store the keys.
- **The storage of the keys.** The keys have got to be stored somewhere on the network and these can often be accessed by those with privileged access (or, of course, by hackers). Anyone who has access to these keys will be able to read (and generate) email messages from users.

- **Keys can be deleted.** If the keys are deleted, it is almost impossible to re-generate them. The deletion of keys can be unintentional (such as where a user's computer has corrupted its disk where the keys are stored) or intentional (such as for an insider within a company who has a grudge against the individual or company).
- **Access from trusted partners.** Many systems are compromised as they allow trusted partners access to their site, and even share their keys with them. Along with this, to guard against keys being lost, the keys are often kept in *escrow*, where malicious agents can gain access to them. There are many cases where electronic keys kept in *escrow* have been stolen by malicious agents, as the *escrow* agents have limited understanding of how the keys should be properly stored.

4.2 DLP Solutions

In terms of DLP, Gartner defines three leaders in the market: Symantec, Websense, RSA and McAfee (Figure 12). Within email protection, the systems tend to focus on mining email for its content, thus the emails often have to be sent or received in a non-encrypted way, so that the scanners can mine their content. Some systems, such as Symantec, do offer automated encryption of emails, but this is triggered by some content or tag within documents or in the body of the email. Again, this is rather hit or miss, and the encryption is basically just to tunnel through untrusted networks. Once the email is stored, the scope of the encryption then ends, and the authentication method used within the corporate environment is then used to validate the user to read the message.

An example of the integration of PGP and automated email encryption is Desktop Email from Symantec, and which manages the complex process of managing encryption keys within the corporate infrastructure. The focus, though, is to sense certain keys words in the email, and automate the protection of the email from one email gateway to another. A complex series of encryption keys are used by the system, which are extremely difficult to manage. These keys, though, have to be stored somewhere, and can be often copied or deleted by malicious parties. The controversy around Superfish shows that users can be tricked into thinking there is a secure tunnel being created, while the private key has been breached through bad practice. In the Superfish case, Lenovo allowed a proxy to be installed on the laptop which created an alternative tunnel which modified Google results. This created a secure tunnel, but unfortunately the Superfish app installed a digital certificate on the host, which had both the public and private key on it. This was then cracked within 10 seconds, using the name of the company who created the proxy for Superfish.

The insider threat is probably the greatest weakness in many systems when it comes to access to email, and the system administrator can often gain access to private keys used to create tunnels and also to access secure email. Most of the tools available are easily compromised where the administrator has privileged access, as they can often

gain access to the private keys used to read the email. If they have privileged access, they can thus also sign emails on behalf of an individual, without their consent.

Figure 12: DLP Garner (Gartner, 2013)

4.3 Biometric email

Ceelox SecureMail is one of the few biometric email packages, and uses a simple Outlook plug-in to secure the transmission and storage of the email. This product improves on the DLP solutions, but it is still complex when sending between organisations, and does not scale well where there are many trust relationships between organisations. **Bio ID Secure Communication** offers much greater scalability of secure email, as it supports trust relationships between companies, whereas the complexity of most biometric email systems makes it difficult to truly trust the transfer of emails across different email systems.

5 Bio ID Secure Communication

5.1 Introduction

The product is fairly unique in that it uses the Bio ID server infrastructure as a trusted broker for the transmission of the email. In order to verify the sender, they must present their fingerprint, after which a secure one-time encryption key is sent to the sender, who will then secure the message with it, and then sign it with the one-time key. On the receipt at the other end, the recipient logs into Bio ID and presents the required bio

identity to the server, and securely receives the key, which can then determine both the contents of the email and the sender. In this way the authentication of the user's ID has been achieved through their biometrics, and not by digital certificates.

One of the strong features in **Bio ID Secure Communication** is that it integrates between trusted Windows Domain servers, and uses a trusted broker to mediate between the two. This supports the possible transfer of secure email between different organisations.

5.2 Market Potential

The key focus of the product includes:

- **High-risk information sharing**. There are many areas of business that have high risks of data loss, including within health and social care, homeland security and in criminal investigations. The recent loss of two CDs by HMRC shows how weak some of the procedures are with Government departments.
- **Data Loss Prevention**. With the Sony hack in the headlines, the issues around Data Loss Prevention (DLP) have come to the fore.
- **Mobile and remote working**. Increasingly companies support mobile and remote working, and the common practice is to create an encrypted tunnel to the corporate site. Unfortunately, users often use mobile devices that are not often connected to the encryption tunnel, and they are at risk of others gaining access their emails (especially where there is a one-time login).

5.3 Patent protection

There are interesting areas which can be investigated in terms of gaining a patent, including:

- **Trust architecture**. There is good scope for defining the process flow within the creation of the trust relationship between organisations, and how differing levels of trust can be applied.
- **Integration of sticky policies**, where the access to the data is protected by a trust policy, and the original email could only be revealed depending on a strong trust and governance policy.
- **Break-glass and self-destruct emails**. The encryption on the email could integrate a break-glass method of revealing the email, along with a self-destruct mode, where the policy of these could be embedded into the transmission and reception of the email. For example the email could have a read once attribute, and then bar any reading of the message after that.
- **The usage of a keyless mode of operation**, where email fragments can be broken up into a number of *shares*, and only when the shares are brought together will the message be revealed. This would support trusted relationships being formed where two or more organisations can be brought together to reveal the original message.

6 Case Studies

The following outline some recent case studies which highlight the problems around data leakage and high-risk information sharing, and how **Bio ID Secure Communication** could be used to overcome the problems.

6.1 Case Study 1: Sony Hack

Within the Sony hack, over 26 million files have been taken from the site, along with movies, private keys, and sensitive client data. The files leaked have no signs of access control, and contained documents that were saved from email messages, such as:

- BBC_KoreaTV_Che_approval_email_032709.doc
- BeforetheDevil_approval_email_June2008.doc

While North Korea has been pin-pointed as the source of the leak, it is more likely that the data leakage was related to System Administrator access, as the System Administrator can have highly privileged access to internal systems. An export of an Exchange email record will thus contain sensitive information that can be used to embarrass a company, and can lead to litigation and data loss fines.

With **Bio ID Secure Communication**, the emails and documents could have exported to an external site, but the contents of the documents or emails would have still been protected. Without doubt, the embarrassing leakage of the Sony information would not have happened if **Bio ID Secure Communication** had been used for emails. Overall, the **Insider Threat** is a massive problem at the current time, especially where individuals have privileged access to view emails within the organisation, and possibly export them.

There are many ways that data can leave organisations these days, typically either through high-capacity memory cards (now up to 2TB can be stored), or though encryption tunnels or with ZIP files.

6.2 Case Study 2: Public Sector Data Breach

In Jan 2015, a couple of CDs related to investigations related to Mark Duggan, Azelle Rodney and Robert Hamill went missing. It brings back chilling memories of the HMRC breach, where sensitive details of child benefit records were lost in the post in the North of England.

The data for at least one of the investigations (the police shooting of Mark Duggan - which ended up with the August 2011 riots) should have been marked with ‘highly

sensitive', and the dropping of files onto a CD for postal delivery sounds more like something from the 20th Century than our Cyber Age. The information itself contained evidence gained, anonymously, from firearms officers. The worry is that the names of these officers could have been included on the CDs. The statement defines that:

> "The Government takes information security extremely seriously, and this incident is a breach of the arrangements that should be in place."

which is worrying, as there seems to be a complete failing in any form of proper data handling on this. Ask any data loss professional, and they will put dumping highly sensitive documents on a disk and posting them, as probably a method that is as secure as actually leaving printed versions in the back seat of a taxi.

The data loss echoed back to November 2007 where CDs sent from the HM Revenue and Customs (HMRC) in Tyne and Wear to the National Audit Office (NAO) were sent though unrecorded internal mail, and went missing. The data on the disk related to child benefit information including 7.25 million claimants and 15.5 million children. These documents on the CDs were password protected, using Winzip 8 password protection. Unfortunately WinZip 8 is fairly easy to crack using well-known tools, or with brute force methods. WinZip Version 9 now uses AES encryption, and would only be breakable by brute force.

While many systems are being hacked, especially from insider threats, the complete lack of process in this case is mind-blowing. The department tries to side-step the issue with:

> "At this stage there is no evidence to indicate that the information loss arose from malicious intent"

but which completely misses the point, as there was:

- No encryption on documents.
- No encryption on the transport.
- No form of control of the access to the document.

The other cases are also extremely sensitive, such as the case of Mr. Rodney who was shot dead by police, in 2005, and which resulted in a police marksman facing trial for murder. The third case related to Mr. Hamill, a Roman Catholic, who was beaten to death by a Protestant crowd in Northern Ireland.

Many people see things going missing in the post on a daily basis, and even a courier system cannot be fully trusted. Overall encryption, whether protecting the document, protecting access, and protecting the channel, is almost infinitely more secure than any physical distribution of documents. The problem is education, especially the lack of it in understanding how documents are properly marked, and protected.

Government departments need to understand the new technologies, especially defining the risk level and in securing all forms of the transmission and storage of these documents. Many companies now have defined processes in place with can protect documents, and these typically involve electronic methods for the distribution of documents. Government departments have a lot to learn from industry in this area, especially from the finance sector, and who will often detect sensitive information and automatically protect.

Bio ID Secure Communication would have overcome the breach, in that it would have protected the documents contained, and would have controlled the access to them.

6.3 Mobile working

There is an increasing trend in mobile working, especially through the use of tablets, which often have single sign-ons. This means that a device which is switched on will often allow a user access to the email running on the system. With the integration of biometrics, the **Bio ID Secure Communication** system should be able to lock-down the creation, sending and reading of the email message. With the addition of a policy, there is scope to build-in an extensible policy, such as locking down the attributes of the access. This will typically relate to the location of the access or the time window of the access.

7 Possible Areas for Technical Innovation

The important step in the innovation of the process is the workflow around the storage of the keys and fingerprint IDs that are stored on a trusted infrastructure. There is good scope for technical innovation especially in looking at keyless encryption methods as a further step in innovating around the product, and in creating a scalable authentication infrastructure. Areas where a patent could be applied include:

- **Mobile integration.** This includes the methods used to store the signatures of the user on the mobile device, and the integration.
- **Enhanced access control.** This includes a complete framework for defining identification properties for an extensible policy.
- **Extensible Policy Control.** This extends the policy beyond fingerprinting, where an access policy can be unique for every email sent. This might include time restrictions for the email and the methods that are required to access the email.
- **Federated Trust Models.** A key factor for the scalability of the product is with federated ID provision to be added as a feature of the secure infrastructure, such as using Google or Facebook as trusted identity providers.

The fingerprint recognition approach is the best use case for the email, but future developments will allow a range of biometric and multi-factor authentication methods to be integrated.

8 Funding Opportunities

There are many opportunities for further funding, including SMART R&D and SMART R&D+. A key factor in gaining funding will be the application of high risk technology, such as using extensive policy restrictions on email.

A focus will be to provide end-to-end email security with advanced cryptography to lock down data to strict policies, based on Location (L), Role (R), Trust Levels (T), Identity (I) and Access definition (A). Data can thus be stored in any location, and be completely protected, and where only when TRAIL policy is verified, will any user be able to view data.

The innovation could look at restricting access to well-known formats within email messages, such as Microsoft Word and Excel, so that they can only be accessed using an access policy integrated into the encrypted document. This policy defines TRAIL: Location (L), Role (R), Trust Levels (T), Identity (I) and Access definition (A), where no access can be given without the required parameters around T, R, A, I and L. The system will thus exist as a layer between the encrypted content, and sticky policy agent, and the associated application software. This method embeds the TRAIL access policy, with a scalable method of providing the access, using federated identity provider. In this way an organisation can lock down email documents based on TRAIL.

The research project will be scalable, and use standard cryptography methods, and where the market sector is agnostic to the platform. For example, it can be used within every public sector application, along with any market that requires the secure storage, transmission and access to data. Standard infrastructures, such as Federated ID are used in the project, and open data standards, are used.

For the technical approach:

- The data is encrypted with a hard shell using best practice encryption, with a match to the TRAIL policy;
- Access policy which uses location as a key aspect of the rights to access, where a movement from one wireless domain into another will cause a change of rights in the access to the data;
- Access to the documents can either be from the cloud or it can be stored locally on the computer;
- Integration with Microsoft Office (or compatible format) to access the data, and thus the user will be able to access the data in an easy to access way.
- All the data sent will be protected with the TRAIL policy, with the most robust encryption and hashing possible; lock-down access to the document using a sticky policy.