UNIVERSITY OF SOUTH FLORIDA
COLLEGE OF BUSINESS

[DRAFT:] 01/24/12

MANISH AGRAWAL

Nation Technologies[1]

So much opportunity. I had no idea that would be a problem.

Stephen Nation, founder of the eponymous firm, had been wrestling with this thought for the last few weeks. Over the last 6 years, he had spent nearly all his spare time refining his idea, developing the technology to implement the idea and finally productizing the technology to the point where he now believed he was ready to hit the market. His early trials showed that users liked his product and most customers who saw his product were interested in further discussions with him and his firm. Most customers agreed that his product filled major need and was clearly differentiated from the offerings of his major competitors, including the largest players in the industry. This gave him reason to feel positive about his company's prospects.

Nation, a former NYPD intelligence officer in the post 9/11 scenario, was wrestling with how to best manage the opportunities available to his firm. His efforts had led to the creation of an easy-to-use encryption key distribution service that would allow people and firms to exchange documents securely, even if the method of delivery was itself insecure. His firm's tagline was "getting back to the basics of information security." Until now, he had been focused on getting the firm's name out and had not been particularly selective about the industries and firms he dealt with. But as he explored his leads, he found that while information security was on everybody's minds, and his technology could be productively used by almost every one of his potential customers, information security meant different things to different people. Almost every vertical market he would end up serving would require significant investments on his part to understand the business needs of the market and to develop marketing and distribution channels focused on the market. He was not sure how his start-up firm would find the necessary resources to do that. He was therefore wondering if he should focus on a few of these markets initially.

Coupled with this decision were several other associated decisions. If he decided to focus on a small set of markets, which should they be? Once he had identified these markets, how should he market his services to firms in these selected markets? What partnerships and revenue sharing arrangements should he explore?

Based on his assessment of the market, he could see at least seven major markets relevant to his firm:

- healthcare
- banking
- insurance
- consumer
- government
- enterprise

He had narrowed his choices down to the following:

1. Identify the best vertical among those above and bet the firm on success in the vertical
2. Identify a few select vertical markets
3. Let the market decide, and go after all available opportunities

He knew he had to move quickly. The time for this technology was now. Unlike the major software vendors, his firm had very little brand recognition and almost no established relationship with IT managers. The market was too big for the major firms to ignore once they got wind of the opportunity. If he did not establish himself as a major player in the market in the next few months, the market could be stolen from right under his nose.

Information Security

Information security is the act of protecting information. Industry-wide, it has traditionally been agreed that information security refers to maintaining the confidentiality, integrity and availability (called the CIA triad) of information. Confidentiality refers to preventing disclosure of information to unauthorized users. For example, we expect retailers to keep our credit card numbers confidential. Integrity refers to the accurate preservation of information and authenticity of the source. For example, we expect our medical records to correctly record our medication history and allergy information. Availability refers to the information being available when needed. Information that is not available when needed is not particularly useful.

The software, hardware and business practices used in organizations to manage information are called its information system. The appropriate use of technology and business practices helps organizations maintain information security. A well understood example is the use of passwords. Most information systems today require the use of passwords for access to sensitive information.

Organizations are increasingly experiencing the need for other information security requirements that do not easily fit into the classical CIA triad. One example is usability issues such as transparency and flexibility. Security frequently adds multiple steps to information processing, imposing training costs and preventing the smooth exchange of information across applications. Another set of issues is driven by regulatory and legal requirements. For example, regulations in many industries require that organizations know who had access to a specific piece of information. This is called chain of custody. When the veracity of information on a form or application is disputed in a court of law, an authoritative chain of custody is necessary for defense.

State of the market

At the time of the case, the standard method to maintain information security was to encrypt information. Encryption is the act of making information unreadable to anyone who does not possess some special information. This special information is called a key.

Encryption works much like locks and keys work to secure homes. Doors have locks. Each lock accepts a specific key. Anyone possessing the key can open or close the house. In information systems, the analogue for the lock is an algorithm. The analogue for the key is a secret number, which is called a key, to maintain the analogy with physical keys. Since the key is kept secret, this form of encryption is also called secret key encryption.

To encrypt information, when the user provides the information system some secret information, usually a password or PKI certificate or biometrics such as a fingerprint, the system uses the key to activate the algorithm and transform the information into an unreadable form. Later, when the information is to be read, the user provides the password again, and the system uses the key to decrypt the information and make it readable again. Exhibit 1 provides an overview of the difference between passwords and keys and why information systems ask users to remember passwords instead of keys.

When information is to be sent to a user in another organization, the standard technology in use today is to ask the receiver for a key to encrypt the data. The technology used to do this safely is called public key encryption. Exhibit 2 provides an overview of public key encryption and the difference between public key (asymmetric) encryption and secret key (symmetric) encryption.

The one remaining issue is key trust. How do you know that the public key you received is trustworthy, that it was sent by the receiver? What prevents an adversary from sending a key and claiming that it comes from Amazon? Most firms in the industry have focused on facilitating this trust. These firms are called certificate authorities. Examples of these firms include Equifax, Global Sign and VeriSign. Companies such as Amazon get their keys certified by these certificate authorities. E-mail systems and web browsers can verify the legitimacy of the keys from these certificate authorities. Exhibit 3 shows an example of a list of these certificate authorities under the hood of the popular web browser, Google Chrome.

TLS and VPN

In practice, the implementation of public key encryption takes 2 forms - TLS and VPN. In simple terms, these would be called “secure the target” and “secure the perimeter.” In TLS, the “secure the target” technology, the data to be transferred is encrypted before transmission and decrypted upon reception. In VPN, the “secure the perimeter” technology, the transmission channel is encrypted, and all data passing through the channel is hidden from the outside world. Exhibit 4 shows a comparison of TLS and VPN technologies.

Most users are familiar with TLS by the more familiar name of SSL. Most secure web sites such as banks and retailers use TLS for secure transactions. Corporate travelers are familiar with VPN, which allows them to communicate securely with their home offices.

The major limitations of both technologies are apparent from exhibit 4. These include:

1. The technologies are limited to information exchange between two parties. There is no simple mechanism to securely exchange information among three or more parties.
2. Once information is delivered, encryption is no longer in operation.
3. The sender has no control over the information after it is delivered to the receiver.
4. Limited tracking and auditing controls
5. The process puts the receiver in charge of the exchange. The receiver passes the key and decides the level of security.

Nation believed that his solution addressed all these limitations. His technology allowed information to be exchanged securely among any number of users. BIOWRAP gets back to the basics of information security by focusing on who created the unalterable information and who has gained access. It also provided the receiver with a level of confidence as to the source of the information. By creating a platform for sharing information securely, BIOWRAP even removes the traditional concepts of ‘Sender’ and ‘Receiver’, which are based on an e-mail-centric view of the world. This allowed professionals in

many industries to better comply with regulations that governed their work. He believed there was no comparable offering in the market.

Firm background

Nation Technologies was a small high-tech start-up firm located in Lake Mary, near Orlando, Fl. It was founded by Stephen Nation, a former NYPD Intelligence officer, who sensed an opportunity in helping organizations exchange documents easily and securely without having to invest heavily in technology infrastructure, expertise and end-user training.

Stephen Nation

Stephen Nation attended the US Merchant Marine Academy at Kings Point, NY. He helped build the NYPD Intelligence Division in the aftermath of 9/11. His time at NYPD included stints at US embassies abroad as a liaison with domestic and international intelligence agencies. While at NYPD, he recognized the great need for an easy-to-use solution that improved the security, management and tracking of digital information. He realized that the solution would need to be easy-to-use, even easier to set up, readily available, provide strong but flexible security options and allow users to track and control their information at all times. From these requirements, BIOWRAP was born…patented…and became available internationally.

Nation Technologies

Nation Technologies was founded in December of 2008, located in Lake Mary, Florida. After focusing on technology development and intellectual property protection in the early years, the firm had recently focused on strengthening its financial position. Towards this end, after considering options including organic growth, strategic partnerships, venture capital and angel investments, the firm decided to focus on strategic partnerships. In addition, Nation Technologies was also going through a private placement offering to generate funds for the near term.

At the time of the case, the firm had four employees including the founder. One of these employees, Marc Matoza, who was recently brought in to the firm is responsible for business development. Matoza had significant prior experience in technology business development from working at HP and being associated with Netscape from its early days.

All of the BIOWRAP technology, with the exception of web development, was performed in house and led by Rod Meli. Meli was an extremely talented project manager with extensive experience in leading international cross functional development teams. Considerations were made to outsource non-vital projects but the firm had yet to utilize outsourced development.

BIOWRAP

BIOWRAP was the flagship technology of the firm. In its basic form, BIOWRAP allowed a user to encrypt any digital information, assign flexible permissions for access, specify an expiration for access, track all activity (real-time and auditing reports) and certify that information with a username/password, PKI certificate or even biometric. A BIOWRAP encrypted file could be shared by any electronic means, but only those that meet the security requirements will be able to decrypt and read the file. All file activity (including unauthorized attempts) was tracked in real-time and recorded in a detailed auditing report known as the Accountability Report.

Technically, BIOWRAP was an identity-based cloud encryption key management service that was currently available as an application, secure website (https://mybiowrap.com), with integration with a mobile app planned for the near future. Exhibit 5 provides an overview of the technology and its operation.

By utilizing a high availability cloud service such as BIOWRAP–which had a rich feature set including application integration and online security--a company had significantly reduced the requirement for technical customizations. BIOWRAP could meet most technical requirements of the large majority of customers. Nation Technologies was also willing to develop any specific enhancements requested by customers following standard cost-sharing industry practices.

Market entry

Nation was convinced that the technology, while simple to use, would revolutionize information security. Current best practices for information security did not secure the information. Rather, they secured the channels through which the information passed or was stored (TLS, VPN or hard disk encryption). This required securing every single node through which sensitive information might pass, a very expensive affair. BIOWRAP on the other hand, secured the information itself. Once encrypted, the data was secure even if the container in which the data was stored was itself insecure. Without authorization from the creator of the data, the file was unreadable.

However, Nation was aware that he was facing a paradigm conflict. Best practices such as those advocated by the premier certifying organizations such as ICS2 (which administered the well-recognized CISSP certification) promoted the classical paradigm of securing the medium and channel using technologies such as TLS and VPN. Most industry professionals felt comfortable adopting the practices advocated by the industry standard best practices. However, he also knew that these professionals were aware of the high costs of maintaining end-to-end security and the regulatory fines that could be levied in the case of a breach. With the right approach, these professionals could be won over, he thought.

Regulatory environment

The primary driver for BIOWRAP's market was the regulatory environment around 2010.There was great concern among legislators and the public about careful handling of personal data by trusted agents. It was recognized that sensitive personal data about customers was scattered in many places at companies and mishandling of such data could cause serious inconvenience to individuals. These concerns were amplified by well-publicized incidents of document theft such as Wiki leaks, where intercepted cables from embassies caused embarrassment to the US government, or intellectual property theft such as the case involving the F-35 Stealth Bomber[2]. Accordingly many industry-specific laws had been created to establish responsibilities of organizations regarding data handling. Healthcare and finance were the two leading industries affected by these regulations.

Data concerns in healthcare - HIPAA[3]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed by President Bill Clinton on Aug 21, 1996. It had two main parts. The first part (Title I) aimed to protect health insurance coverage when workers changed or lost their jobs. Title II (with the heading "Preventing health care fraud and abuse; administrative simplification; medical liability reform") commonly known as the Administrative Simplification (AS) provisions of the act. These provisions contained clauses that addressed the security and privacy of health data. The principal provision in this part of the act was

[2] Siobhan Gorman, August Cols and Yochi Dreazen, "Computer spies breach fighter-jet project," Wall Street Journal, 4/21/2009

[3] For a good overview of HIPAA, please see the Wikipedia article on HIPAA. The health information privacy page of the Department of Health and Human Services (http://www.hhs.gov/ocr/privacy/) also has a very good overview of the privacy provisions of HIPAA.

section 264. The text of the section is shown in Exhibit 6. It can be seen that Congress left it upon the Secretary of Health and Human Services (HHS) to issue rules to implement the provisions of the act.

Accordingly, HHS issued the privacy rules in their current form on Aug 14, 2002. The Privacy Rules identify information called protected health information (PHI). This specified the individual health information that needs to be protected. The rules also identify organizations subject to the Privacy Rule. These were called covered entities. Within HHS, the Office for Civil Rights ("OCR") was assigned responsibility for implementing and enforcing the Privacy Rules.

To meet HIPAA requirements for protecting the integrity, confidentiality, and availability of PHI stored in electronic form (e-PHI), HHS developed rules that were published on February 20, 2003. The Rules specified administrative, technical, and physical security procedures for covered entities to assure the confidentiality, integrity, and availability of e-PHI.

Doctors, pharmacies and health insurance companies were mostly comfortable with the HIPAA privacy rule requirements in their current operations. However, a new wrinkle had emerged in the industry. This was the push by the government for all covered entities to move to electronic health records (EHR) by 2014. This meant that doctors' offices would have to store patient records in electronic form and send prescriptions to pharmacies electronically. There was therefore a need for solutions that would help the industry to comply with the HIPAA privacy rules without complicating doctors' practice of medicine.

Data concerns in the financial industry – Gramm-Leach-Bliley act of 1999[4] and the Red flag rules of the FACT Act 2003

Similar to the concerns in the healthcare industry, privacy concerns have been important in the financial sector as well. The Gramm-Leach-Bliley act passed on Nov 12, 1999, included provisions requiring financial companies to safeguard client information. Section 501 of this act required that banks and other financial institutions maintain the confidentiality of customer records and protect against the unauthorized use of such records. Section 502 of this act defined how banks and other financial institutions could share customer information with other institutions. These two sections of the law are shown in Exhibit 7.

The Fair and Accurate Credit Transactions Act of 2003, also known as the FACT act, was best known for allowing consumers to get a free credit report once every 12 months from each of the three large credit reporting companies (Equifax, Experian and Trans Union). The act also had provisions dealing with preventing identity theft such as fraud alerts and printing of credit card numbers on merchant receipts.

Less well known among the public, but of major concern to professionals in the industry were the Red Flag rules created as a result of the act. These rules, created by banking regulators, require financial institutions to make reasonable efforts to prevent and mitigate identity theft, assess the validity of change of address requests they receive for debit cards and credit cards etc.

Industry comparisons

Driven by these provisions and based on his assessment of the opportunities in various industries, also referred to as *vertical markets*, Nation had shortlisted the following industries to focus on in the initial years:

1. Healthcare
2. Finance – specifically mortgage brokers and insurance agents
3. Corporate data

[4] Again, Wikipedia has a very good overview of the Gramm-Leach-Bliley act of 1999 and the FACT act of 2003.

4. Consumers

As he compared these industries for the opportunities they presented, Nation believed that the following criteria would be relevant to his analysis:

1. *Regulatory environment*: rules and regulations that a big driver of demand for security solutions. Clearly, industries with clearly defined regulatory requirements for data security would present him with the best opportunities. In the shortlisted industries above, healthcare and finance had the most rigorous regulatory requirements.
2. *Existing procedures*: Industries with primitive processes such as those that still relied on paper-based records were most likely to be receptive to new security solutions either to lower costs or for legal compliance. Nation thought that the extensive use of paper-based forms for mortgage applications presented a particularly lucrative opportunity for him to get an entrée into industry. Similarly, most doctors' offices still used paper records. This should be an important business for him, he thought. Another example in the consumer sector that drew Nation's attention was the use of fax for wire transfer requests. He couldn't help but think of the number of people who had access to the confidential information on these requests and the safeguards on this access. How many of these employees were trained to handle information responsibly? How did these offices deal with employee turnover? Could there be something he could do to help these firms send certified wire transfer requests?
3. *Intrinsic value of data*: In general, valuable data has more rigorous security requirements. For example, a credit card number has street value, but the students score on an assignment does not have the market price. Therefore credit card information is more vulnerable because more people are trying to steal credit card information than are trying to steal assignments scores. Accordingly, the requirements for handling credit cards are more rigorous than the requirements for handling student assignment grades and the fines for compromising credit card information are greater than the penalties for revealing student grades. BIOWRAP should have greater opportunity in industries such as finance where the data is intrinsically of higher value.
4. *Cost of breach*: Fines, penalties, adverse publicity, reports of job loss etc. have a way of drawing executive attention. Industries with well-publicized breach incidents were likely to be looking for security solutions and look favorably upon solutions such as BIOWRAP. According to a well-recognized study, 22% of all breaches reported in 2010 occurred in financial services firms and about 35% of all compromised records stolen were from the financial services sector[5]. By comparison, only about 1% of all breaches in 2010 affected the healthcare industry. While the financial sector took great effort to secure customer data, it appeared that even as late as 2010 it was relatively easy for thieves to steal data from some of the large financial institutions and information on over 200,000 credit cards was stolen from Citigroup by bypassing the firm's information security controls[6]. This breach has attracted a lot of attention in the information security industry.
5. *Transaction volume*: Nation was quite proud of the usability features of his technology and the limited to nonexistent learning curve to use BIOWRAP. He was confident that industries with high transaction volumes but still using old paper-based processes would see a significant productivity increase the switchover the best technology.
6. *Industry awareness*: This was a sore point for Nation. At customer after customer, he ran into the problem of security professionals not realizing the limitations of current information security practices, which rested on storage, whereas regulatory requirements were technology agnostic and focus only on the data. To his surprise therefore, at most clients he received no interest from

[5] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
[6] http://www.nytimes.com/2011/06/14/technology/14security.html?_r=1&ref=technology

the IT group, but he was very well received by management. He could not discern any differences across industries in their awareness of the need for his technology.

7. *Information chain*: Nation's solution was particularly useful to record chain of custody for information. This feature would be most useful to industries where information passed many hands before a decision can be made. For example, patient records usually stay confined within a doctor's office and only a limited number of users access the record. By contrast, a mortgage application might originate at a bank branch, get processed by the bank's lending unit, be sent over to a title company for third-party services, get handed over to a mortgage aggregator, and from there to a pension fund that buys the mortgage and many other players in the industry. Courts are increasingly taking a hard look at how the industry was handling customer information and chain of custody could be useful in establishing mortgage ownership, particularly if the market turns sour and the loan went into foreclosure. Having an easy-to-use, secure, electronic chain of custody solution such as that provided by BIOWRAP could be immensely useful in the industry.
8. *Information integrity and trust:* Consider the case of a high-value banking customer. BIOWRAP would be a very useful mechanism for delivering bank statements and related communiqués because the banks could use the service to restrict access to a specific customer, track document views, and alert the customer in case of suspected privacy violations. The customer could trust that the information was from the bank and was un-altered even if it was removed from the protection of BIOWRAP. An added benefit would be the ability of banks to distinguish legitimate electronic communication from spam. This service could also be useful for lawyers and their clients.
9. *Availability*: Traditional data privacy solutions are hardware based and require expensive and time consuming IT support and implementation. The BIOWRAP service is currently available as an application as well as at a secure website (https://mybiowrap.com). Integration with a mobile app is also planned for the near future.
10. *User network complexity*: Related to the information chain, and as highlighted in the example above, a chain of custody solution is particularly useful when a large complex network of users from multiple organizations is dependent on the same bit of information. Nation expected to see significant adoption in industries with large and complex networks of users of information, as for example in the housing industry where mortgage forms are shared between home buyers, sellers, banks, realtors, pension funds etc.
11. *Sales cycle*: finally the sales cycle was likely to impact adoption. The buying process was often centralized and many organizations preferred to deal with large established vendors, particularly those vendors with which the organization had existing relationships. This practice could adversely affect Nation Technologies because it was after all a startup with limited industry history. Nation however was determined to overcome this obstacle and has set out on the path of partnering with the top Certificate Authorities (CAs). Accordingly, he recently established the company's first CA partnership with GlobalSign. As seen in exhibit 3, the top CA's were already embedded within the top enterprises and applications in all vertical markets. This would allow these organizations to seamlessly provision their existing certificates to use BIOWRAP.

The Decision

By late 2011, Nation had made a number of customer visits and received varying levels of interest across industries. As he plotted the future direction of his company, he could see that he would need to make some choices regarding the industries he wanted to focus on. As he saw it, he had the following decision options:

1. *Identify* the best vertical among those above and bet the firm on success in the vertical
2. Identify a few select vertical markets
3. Let the market decide, and go after all available opportunities

4. Sell the company

Making the wrong choice could have a severe impact on the company's prospects. As a start up with limited resources Nation was aware that there were limitations to what he could accomplish at once. He was also aware that delaying entry into an industry could give opportunity to anyone of the large systems software vendors such as Microsoft and Symantec to dominate the sector. Could he find someone to help them navigate his options, and immediately?

Exhibit 1: Passwords and keys

In the physical world, we carry our keys with us in a keychain. In the digital world, we carry passwords. Passwords are not keys, what is the difference?

A key is information that cannot be guessed even by a motivated attacker. Since modern computers are extremely fast, each computer can try millions of keys every hour to read encrypted information. Since modern computers are also extremely cheap, motivated attackers can easily acquire hundreds or thousands of computers dedicated to the task of decrypting protected information. The keys used in modern encryption must be capable of withstanding such attacks.

Keys are made secure by making the pool of available keys extremely large. For example, if a system has a thousand possible keys and an intruder can try out 1 key a minute, it would take the intruder 1,000 minutes (about 17 hours) to try out all keys. This is the basic math behind modern key selection.

A simple calculation can show the formidable power of modern computers. At the time of writing this case, processors ran with clock cycles of about 3 Ghz, and many modern desktop processors had up to 8 cores, giving an effective clock rate of 24 Ghz. Assuming 10 clock cycles to try one key, and ignoring network delays, a modern desktop computer can try 2.4 billion keys per second (24 billion clock cycles/ 10 cycles for each key). For convenience, let us round this number to 2 billion ($2 * 10^9$) keys per second. This translates to 172.8 trillion keys per day and $63 * 10^{15}$ keys per year. This is from just one computer! An adversary with a 1,000 computers dedicated to the job can try $63 * 10^{18}$ keys per year.

To keep information secure, we need a key pool that is so large that even when keys are tried at such a fast pace, the likelihood of an intruder finding the right key is very low. Since computers store all information as numbers, encryption keys are simply numbers. These numbers are chosen from a sufficiently large pool of numbers to maintain security. How large should these numbers be?

Say we used 1 digit numbers as keys. These numbers range from 0 – 9, giving us 10 possible keys. If we used 2 digits, we would have numbers in the range 0 – 99, or 10^2 possible keys. As can be seen, as we increase the number of digits, we get an exponentially increasing number of keys.

Computers store numbers as binary digits, where each digit can take the value 0 or 1. Binary digits are called bits. Using 1 bit binary numbers, we would have 2 possible keys (0 and 1), using 2-bit binary numbers, we would have 4 possible keys (00, 01, 10 and 11). With n-bit binary numbers, we would have 2^n possible keys.

So, how large should our key size be to be secure? Let us start by calculating the number of bits required to obtain $63*10^{18}$ keys, so that a group of 1,000 modern computers would take one year to go through all the possible keys. This gives us a key length of 66 bits[7].

Each additional bit doubles the pool of keys, making the encryption scheme twice as secure. For example, if we used 67-bit keys, we would get $2 * 2^{66}$ keys. Most experts agree that 128 bits offer sufficient protection for the near future. 256 bit keys are also used.

[7] $2^{10} = 1{,}024$. Therefore, a rule of thumb is to approximate $10^3 = 2^{10}$. $10^{18} = 10^{3*6}$ is then $2^{10*6} = 2^{60}$. $64 = 2^6$. Therefore, $63 * 10^{18}$ is approximately equal to 2^{66}.

Passwords

An example 128-bit key is the following:

01010110101111011101111111111100100010110101010010111111011010011000111011101110101001100100000010110111001100110000000101101001001111101011110111011111111111001111000001100100101111111011010011000111011101110101000101100000010110111001100110000000101101001

Try remembering it. After all, if you want to encrypt information using this key, you need to provide this key to the information system to perform the encryption.

It is not easy to commit such large number to memory. Information systems therefore use passwords as the user interface to access the keys. The system saves the key internally and makes it available only to users who can provide the correct password.

Passwords are typically much shorter than the secret keys. To defend against the possibility that intruders may try to guess passwords instead of the keys, systems typically lock themselves out after some number of failed login attempts. Through this procedure, users can get the security of a large key while only being required to remember a much shorter password.

Exhibit 2: Public key and secret key encryption

Secret key encryption works well to save our own data. To send encrypted data to a receiver, we would need the receiver to send us the key. This is the Achilles Heel of secret key encryption. How do you secretly send the key to someone? If you use email or other insecure channels, the key is liable to be stolen during transmission.

Fortunately, we have another method of encryption. It uses two keys – one for encryption and another for decryption. The key used for encryption cannot be used for decryption. To use the 2-key method of encryption, we ask the receiver of the data for his encryption key. This key can safely be sent over the Internet. The sender uses this key to encrypt data and the receiver uses his decryption key to read the data.

Public Keys (and private keys) are typically stored in a special container called a certificate. The certificate and by extension, the keys can be authenticated by the Certificate Authority that generated the keys.

Since the encryption key can now be sent publicly, the 2-key method of encryption is popularly called public key encryption. Figure 1 shows an overview of public key encryption.

Figure 1: Public key encryption

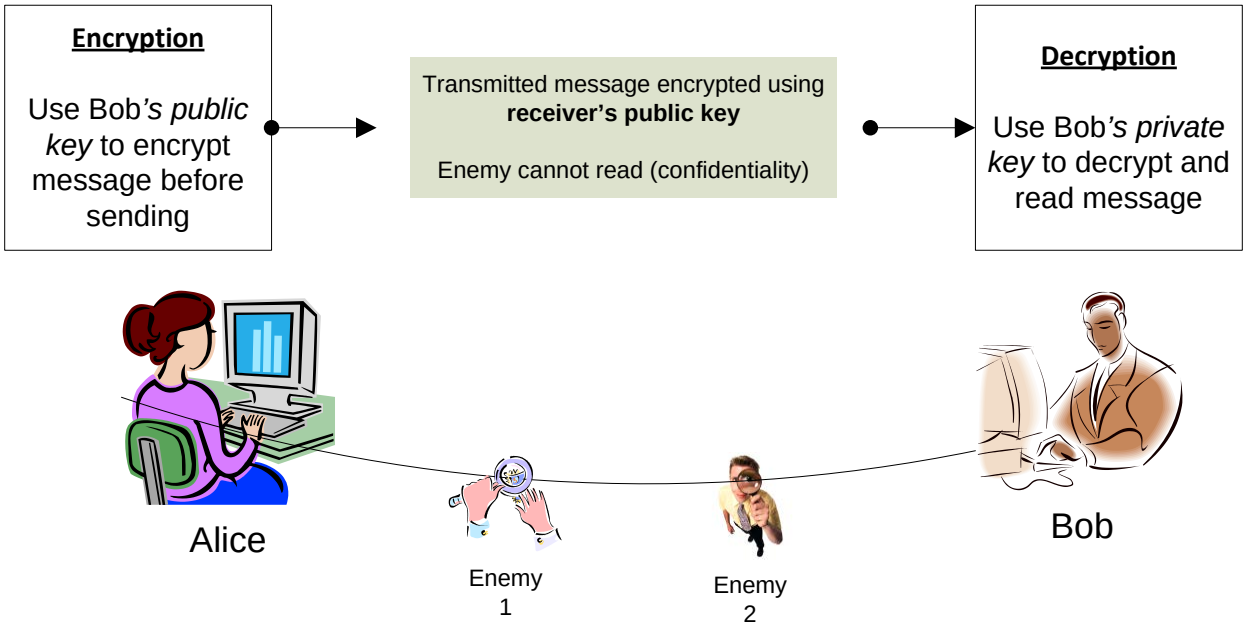


Exhibit 3: Public key and secret key encryption

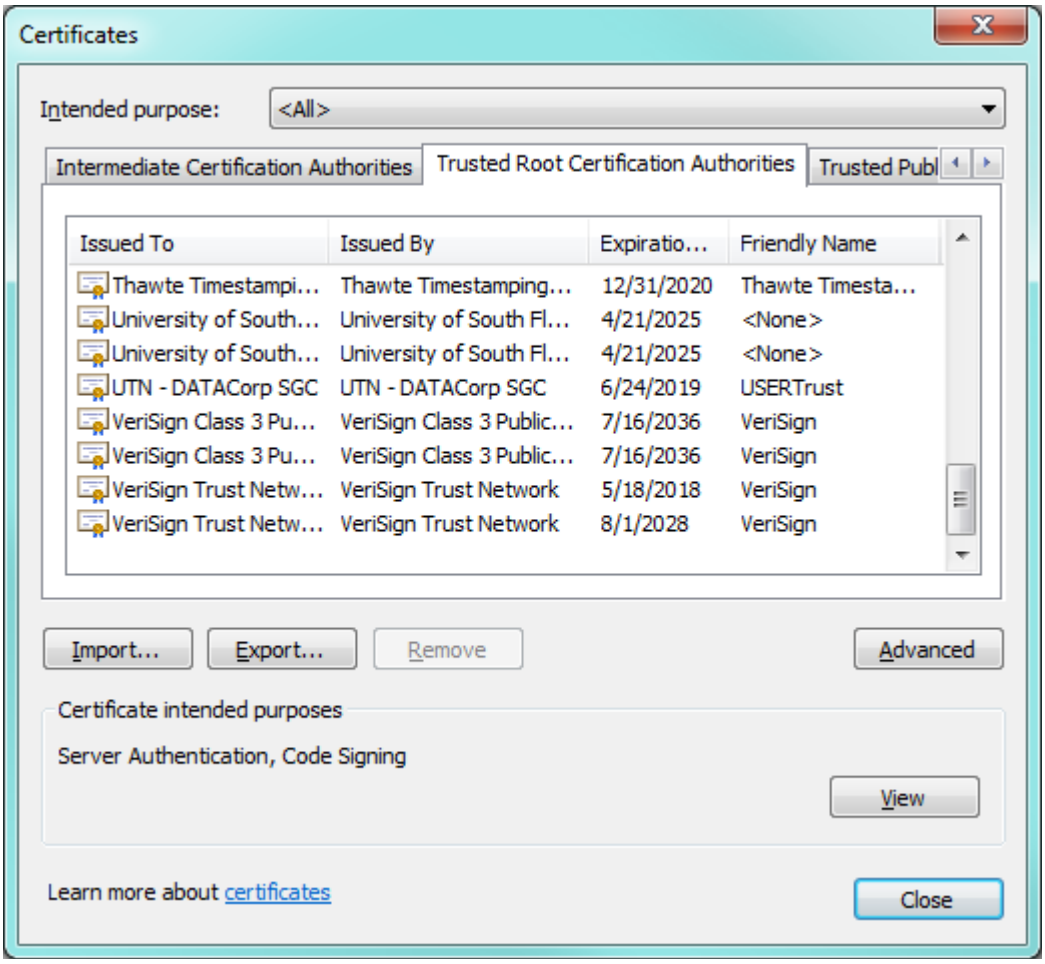


Exhibit 4: TLS and VPN

In TLS, only specific data items are encrypted before transmission. In VPN, all traffic is encrypted. This is shown in Figure 2 and Figure 3 below.

Figure 2: TLS used to "secure the target" by encrypting specific data items

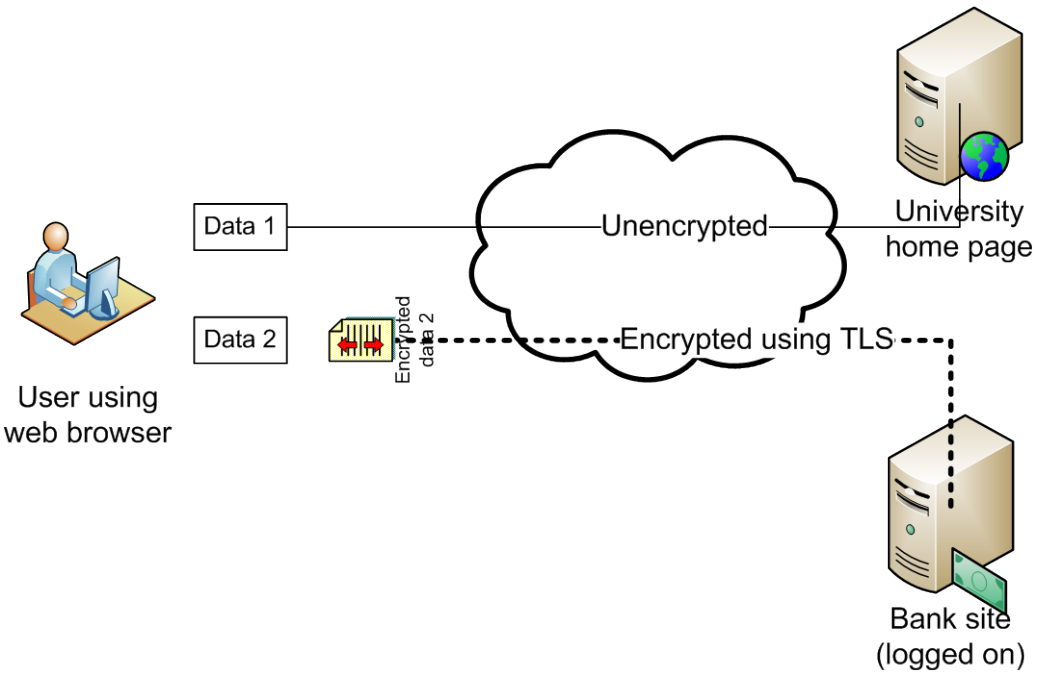


Figure 3: VPN used to "secure the perimeter" and hide all information in the channel

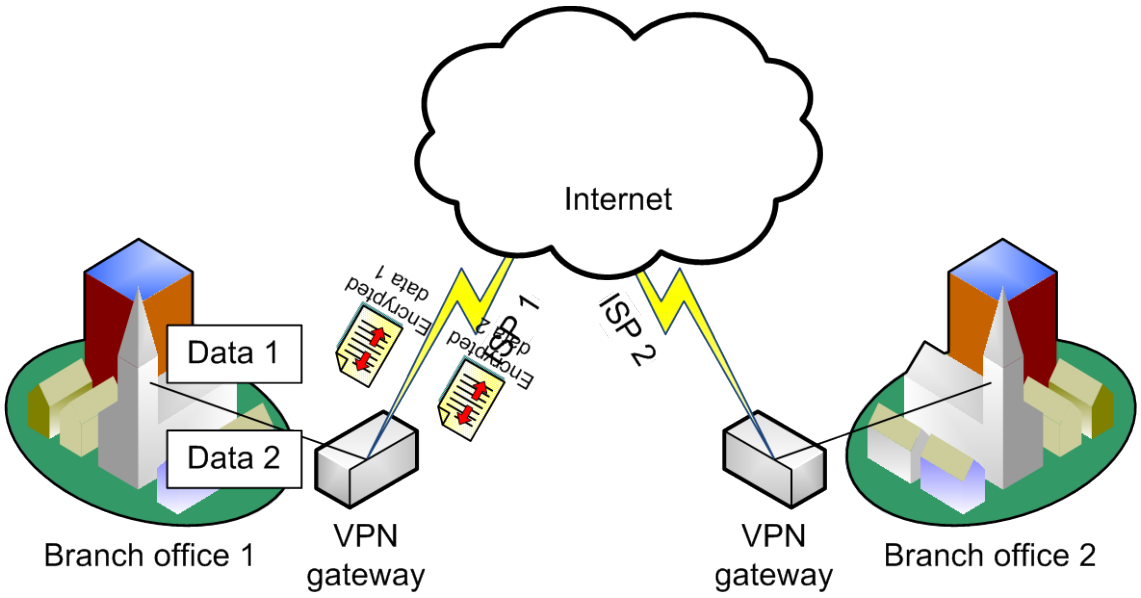
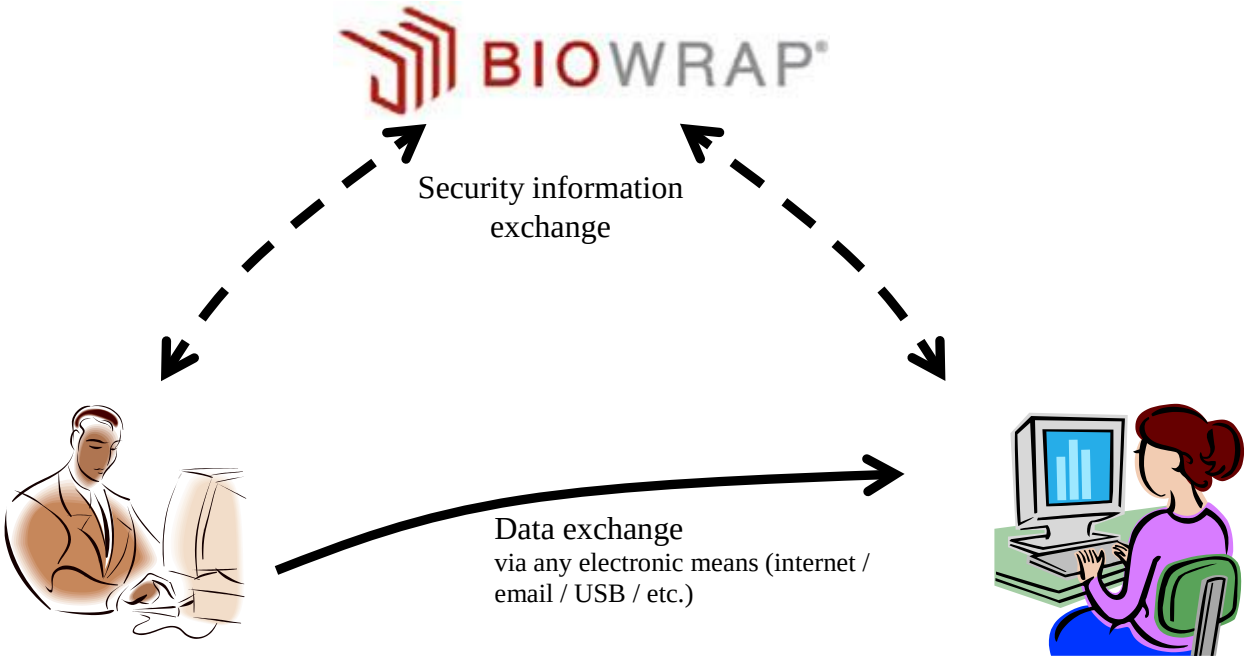


Exhibit 5: BIOWRAP operation



The BIOWRAP operation is shown in the figure above. The BIOWRAP central service authenticates the sender's credentials and provides the encryption key to the BIOWRAP client. The BIOWRAP client encrypts the files. The encrypted files are delivered to the receiver. When the receiver provides the correct credentials and satisfies any confidentiality rules the BIOWRAP central service provides the encryption key to the BIOWRAP client. Encryption and decryption may be done using the BIOWRAP web site, or using the BIOWRAP desktop application.

Exhibit 6: HIPAA privacy provisions

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) In General.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) Subjects for Recommendations.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) Regulations.--

(1) In general.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(2) Preemption.--A regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) Consultation.--In carrying out this section, the Secretary of Health and Human Services shall consult with--

(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and

(2) the Attorney General.

Exhibit 7: Gramm-Beach-Bliley act non-disclosure provisions

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) Privacy Obligation Policy.--It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial Institutions Safeguards.--In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

SEC. 502. OBLIGATIONS WITH RESPECT TO DISCLOSURES OF PERSONAL INFORMATION.

(a) Notice Requirements.--Except as otherwise provided in this subtitle, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 503.

(b) Opt Out.--

(1) In general.--A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless--

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2) Exception.--This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

(c) Limits on Reuse of Information.--Except as otherwise provided in this subtitle, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(d) Limitations on the Sharing of Account Number Information for Marketing Purposes.--A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(e) General Exceptions.--Subsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information--

(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with--

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, United States Code, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act, or (B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.