Formulating a Complete Payment and Data Security Approach in Higher Education

The rules, regulations and considerations around protecting PHI, PII and payment data in the higher education environment and how encryption and tokenization work to provide an omnichannel security strategy.

Overview

With the continued rise of data compromises across higher education, understanding how to protect against cyberthreats in a simplified and comprehensive manner is crucial. When the changes to user behaviors from the global pandemic are included, the need for omnichannel data protection escalated very quickly.

Cyberattacks on colleges and universities significantly increased in 2020, with almost half of all data breaches now blamed on ransomware attacks. While it is vital that organizations protect their system perimeter from hackers, securing Personally Identifiable Information (PII), Protected Health Information (PHI), and cardholder data (CHD) is of equal importance. If hackers manage to breach the campus system or network and find clear-text data of value, this data can be used to leverage a ransom payout or worse – be sold on the Dark Web, causing irreparable brand and monetary damages.

Whether your organization needs to protect CHD, PHI, PII, or combinations of these, this paper will provide guidance on how to achieve a complete data security approach.

In the payments space, protecting CHD with PCI-validated Point-to-Point Encryption (P2PE) is an available best practice. However, this technology only protects card-present (CP) data – it does not protect Ecommerce or card-not-present (CNP) transactions, with the notable exception of encrypted keypads used in contact centers or the back office. In the data privacy space, more sensitive data is being entered online than ever before, requiring that this data be protected both upon intake and in storage. This paper will review how tokenization can be combined with encryption in a way that offers a single approach to securing higher education CHD, PHI and PII, regardless of how you capture or use this data.

With many options for encryption and tokenization available, this paper will also provide critical information to make informed business decisions related to data security programs. The paper also reviews how Bluefin's encryption and tokenization solutions, including PCI-validated P2PE and the ShieldConex® data security platform, can protect against increased cyberthreats, meet payment and data security regulations, and simplify your omnichannel data security challenges.

Background

Payment data history

As payments have moved online, the threats to Ecommerce and web intake forms have risen dramatically. Two of the most significant regulatory bodies governing payments across industries are the Payment Card Industry Security Standards Council (PCI SSC) and the National Automated Clearing House Association (NACHA). The PCI SSC was created to protect card payments and NACHA was created to protect banking transactions commonly known as Automated Clearing House (ACH) transactions.

Both organizations provide standards to protect sensitive payment data, specifically CHD and banking account information. The PCI SSC created the PCI Data Security Standard (DSS) in 2004 to protect CHD and today is a well-established standard. In the last few years, NACHA has started to refer to the PCI DSS when it comes to methods for protecting ACH Account Data.[1]

As these standards matured and expanded, so did cyberthreats and data breaches. After the mass U.S. retail breaches in 2013 and 2014, the Europay MasterCard and Visa (EMV) authentication method, managed by EMVco, was seen by many as the answer to card-present payment data protection in the U.S. While important, the EMV standards limit card-present fraud by authenticating the physical card with a chip, but the technology does not specifically protect CHD.

When PCI released their P2PE standard in 2011, it was the first standard focused on providing a PCI-validated security solution to protect card-present CHD in transit, from the point of encryption in the payment terminal, to decryption in hardware by the validated P2PE solution provider. While card-present encryption solutions existed before the introduction of P2PE, the complexity of how to efficiently and effectively protect CHD had become confusing and difficult.

The P2PE standard provided organizations with a solution that had met the rigorous requirements put forth by PCI for the highest level of encryption available for card-present transactions.[2]

[1] For additional information on Nacha rules and how they map to PCI DSS requirements, see our white paper, "Nacha and PCI Payment Security," https://www.bluefin.com/resources/media/white-papers-briefs/nacha-data-regulations-white-paper/.

In October 2019, PCI published their standard for 3D Secure (3DS), which is a secure consumer authentication (SCA) solution for Ecommerce transactions. Similar to EMV at the point-of-sale (POS), the goal of 3DS is to authenticate the consumer making the online purchase. However, like EMV, 3DS does not secure Ecommerce transactions and data. This is where encryption and tokenization solutions come into play, which secure data upon intake in web-based forms and protect that data at rest or in storage in a system or network.

Any higher education organization with complex financial data challenges needs the ability to leverage all security technologies with a single and simplified approach to data protection.

Privacy data history

Privacy data efforts have significantly increased over the past few years, with the addition of several new laws and regulations.

One of the earliest privacy regulations, the U.S. Privacy Act, was enacted in 1974 to govern the collection, maintenance, use, and dissemination of information about individuals. The Health Insurance Portability and Accountability Act (HIPAA) was put in place in 1996 to protect health information. In 1999 came the Gramm-Leach-Biley Act (GLBA) to protect financial and non-public personal information (NPI). 2002 brought two new Acts: the Sarbanes-Oxley Act (SOX) to protect the public from fraudulent practices by corporations, and the Federal Information Security Management Acts (FISMA) which ordered U.S. agencies to protect data. The International Organization for Standardization (ISO) generated ISO 27001 in 2013 to act as a framework for organizations' information security management systems.

More recent regulations include the General Data Protection Regulation (GDPR), which was enacted by the European Union (EU) in 2018 and focuses on protecting EU citizens' personal data globally. Other countries have been following the EU's lead with GDPR, including the U.S. with state-based laws including the California Consumer Privacy Act (CCPA), which restricts the collection and use of personal data, effective in January 2020. Other states with privacy laws and protections include New York, Hawaii, Maryland, Massachusetts and New Mexico.

While each law, act or regulation varies on what data is considered "private," the core concept is to protect data that could potentially harm an individual or data which consumers may not want disclosed. Like the need in payment security to have a single approach to protect CHD and Account Data across acceptance channels, it is also increasingly critical that colleges and universities have the ability to address the different privacy requirements with a single security approach.

[2] A list of current validated P2PE solution providers can be viewed at https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions?agree=true.

Complete Data Protection

There are key considerations when selecting a single payment and data security solution. What are the factors that have the most impact on protecting different types of data within your campus acceptance points? What should you look for in order to simplify your approach, while making your entire system more secure? And finally, understanding your core business objectives is also important, including when and how you need access to data.

Higher education has a more complex environment than the average enterprise organization. Privacy and financial data security and compliance concerns are both present across a diverse environment typically with multiple third-party vendors. Education environments are a significant target for hackers looking for credit card data specifically.

Payment data can be found in many different locations that require protection including:

- Bursar's office
- Food and beverage
- Sports and fitness
- Health
- Bookstores
- Parking

Encryption of payment data leveraging P2PE is one of the best ways to minimize the scope of payment data impacts across the many devices in each of these locations to secure the payment transaction.

As discussed in the financial data section, P2PE only protects card-present transactions. When implemented correctly, P2PE can also protect another payment method which is common to higher education – call center, telephone and mail order transactions. P2PE does not cover web-based Ecommerce transactions, which are common in higher education, and with the pandemic, the pressure on these systems has increased dramatically.

Once again, the need for tokenization becomes clear. POS credit card payments can be protected with P2PE but other payments, such as ACH, Ecommerce and recurring payments all need to additionally leverage tokenization.

PHI and PII entered online often also need to be protected and still retrievable in a secure manner. This is where a complete solution that can provide encryption and tokenization to address multiple standards and thus allow secure handling of all types of sensitive data in a complex networking environment becomes critical.

Financial Data

The primary objective for financial standards is to protect sensitive payment information by implementing both environmental and data protection methods.

PCI DSS

In addition to the PCI DSS, the PCI SSC also created several other standards. Here is a partial and simplified list: [3]

- PCI DSS – Focused on securing the networking environment
- PA-DSS – Payment Application – Focused on securing applications
- SSF – Software Security Framework – Replacing the PA-DSS this year
- PTS – PIN Transaction Security – Focused on securing hardware
- P2PE – Point-to-Point Encryption – Focused on securing data
- PCI 3DS – 3D Secure – Focused on securing Ecommerce transactions

The last few years have seen many colleges and universities adhering to the above standards using three technologies that have been called a “silver bullet” for securing payment data:

01 Encryption

02 Tokenization

03 EMV

P2PE with approved Point-of-Interaction (POI) devices is used to encrypt POS data in transit, while tokenization is typically used to protect data at rest and EMV authenticates the physical card being used. This approach seemed to provide a complete solution to protect payment transactions across all industries.

[3] Note that there are additional PCI DSS guidance documents to cover many other topics, including tokenization and Ecommerce. These guidelines are supplements to the standards, although some of these eventually can become new standards or become incorporated into existing standards.

However, it can be difficult to implement each of these independently, and this approach still has a significant gap for most organizations: Ecommerce transactions. Based on the rise of online fraud observed in Europe and other locations that first implemented EMV, it was not surprising to see the same shift from card-present fraud into Ecommerce or CNP fraud as the U.S. began to enforce EMV.

Pandemic Impact

In the beginning of 2020, the primary security focus for the majority of organizations in higher education was on protecting card present payment transactions since it represented the bulk of payment activity.

With the global pandemic, colleges and universiteis were forced to switch to Ecommerce and mobile in-app payment channels in order to continue serving students. Organizations that had both physical locations and an online presence were also impacted because the number of Ecommerce transactions rose dramatically, along with associated security vulnerabilities and threats. While we will see a balancing of payment channels with the pandemic behind us, student and alumni payments are no longer likely to be dominated by the brick-and-mortar model.

ACH

Where PCI is focused on protecting CHD, ACH is focused on protecting Bank Account Numbers, also called Account Data. As previously mentioned, NACHA refers to the PCI standards as a baseline for how organizations accepting ACH payments can approach the protection of Account Numbers. This is helpful since any college or university that processes credit cards, regardless of industry, is required to comply with the PCI DSS for card payments.

However, starting this year, new Nacha regulations require the protection of Account Numbers and Account Data at rest – organizations with over 6 million ACH payments annually will need to demonstrate best effort to comply by June 30th, 2021 and those with over 2 million ACH payments annually by June 30th, 2022. This is a crucial consideration for any college or university that utilizes ACH data in their payment process, whether for card on file, new payments or recurring payments.

While the overarching regulations around ACH Data are different from PCI, the security approaches are very similar. Higher education organizations with the need to protect both CHD and Account Data then need to find an approach to data security that can handle both types of data. While this need is a relatively new challenge, the good news is that encryption and tokenization can be leveraged to meet these needs – provided the solution your organization chooses is able to adapt to meet both.

ENCRYPTION, TOKENIZATION AND FORMAT PRESERVING ABC'S

A quick explanation of the differences between encryption and tokenization will help simplify the understanding of how to protect data.

Encryption

simplistically put, is taking a known piece of data and locking it up so that the data can only be retrieved with a key. In more technical terms, encryption uses an algorithm and a key to take the data and make it unreadable. Of course, this key must be controlled, typically called key management, to keep the data safe. If your data is "123", and you encrypt the data with key "ABC", resulting in "98zy65x", and protect the key properly, all an attacker will be able to see is 98zy65x, which is useless to them.

Tokenization

is taking a known piece of data and replacing it with a new random value. For example, the value "123" could be replaced with an unrelated value, such as "978".

There are 2 common ways to tokenize data. The older of the two methods maps a token in a database so that it can be retrieved, which is typically referred to as vaulted tokenization. This approach requires the database be properly secured and has limitations on scalability. The newer approach is known as vaultless tokenization and allows for greater speed and scalability.

Vaultless tokenization

is similar to encryption in that it also requires an algorithm to retrieve the original data. Both types of tokenization have value to organizations depending on different use cases and data security requirements.[4]

Another aspect to consider is the ability to leverage secure hosted fields and iFrame technologies to support in-page tokenization for Ecommerce transactions. Much the way P2PE leverages a very strict separation between the hardware and the applications that run on that hardware, iFrame technology separates the tokenization of sensitive data from the rest of the webpage.

[4] For a comprehensive overview of tokenization, see Bluefin's white paper, "Using Bluefin's ShieldConex® for Data Protection," https://www.bluefin.com/resources/media/white-papers-briefs/shieldconex-data-protection/.

A final consideration when encrypting or tokenizing data is the ability to use the new value in an existing campus system without needing to re-write applications to accommodate different value lengths or data values. For example, if a 9-digit Social Security number or a 16-digit credit card value doesn't stay 9 or 16 digits, and/or if alpha characters are added to the numerical characters, most processes to handle that data need to be modified.

To avoid these potentially expensive and time-consuming problems, Format Preserving Encryption (FPE) and Format Preserving Tokenization (FPT) offer a way to gain the benefits of encryption or tokenization and maintain existing data processing needs. Both FPE and FPT have the ability to create a new value of the same length and same character boundaries for the different data types that payment data and privacy data encompass.

Financial Data Conclusion

The convergence of existing complex payment security challenges, combined with global circumstances, has dramatically escalated the need to implement a complete payment data security solution. If this was not enough of a challenge, colleges and universities must also consider the impact of increasing privacy data requirements.

Privacy Data

There are dozens of different data regulations, laws and standards that colleges and universities may need to consider. Rather than focus on one specific regulation, we consider the most common data types that may need protection, including:

- Bank account and credit card information
- Social Security, driver's license and passport numbers
- Medical or health information
- Names and signatures
- Address and telephone numbers
- Unique account names or personal identifiers, including email addresses
- Education or employment information

The above can be expanded into many different data components that need to be protected. Unlike payment data, privacy data cannot be as easily narrowed down to CHD or Account Data as payment security has done. However, as long as your organization can define what type of data needs protection, the same methods used to protect payment data can typically also be leveraged to protect privacy data. Because each of these data types need to not only be protected, but also used by your organization, tokenization and approaches like FPE and FPT rise to the top as some of the best options, especially if the same tokenization solutions can be leveraged across both privacy and payment data.

Storage and Transmission of Data

A critical component of any solution is how it will secure data in different states. Storing data (at rest) and moving data (transmission) each require entirely different approaches, yet both need to leverage the same security technologies such as encryption and tokenization.

Storage of Sensitive Data

There are different reasons to store sensitive data, and while standards may suggest various ways to do this, the core technology to secure data when stored is tokenization. If you have a defined business need to store sensitive data, then you need to encrypt and tokenize that data and limit who has access to the data. Looking at CHD as an example, PCI has specific and strict requirements for how to store sensitive data as part of requirement 3 of PCI DSS.[5] One of the best ways to reduce the scope of your compliance reviews is to minimize or reduce what data you store, and where you store that data. Tokenization can be leveraged in many cases to maintain access to data as needed, and still remove the data from your environment.

Transmission of Sensitive Data

Movement of sensitive data includes the initial input of data and then the transmission of that data between any two systems, regardless of what the need for movement is. This data can be transmitted as clear-text data, or as encrypted data. When sending un-encrypted or clear-text data that is sensitive, it is possible to encrypt the channel or tunnel over which the data is transmitted. Additionally, the point where the data originates and the point where the data is sent then have to handle this clear-text data appropriately. There are multiple challenges in doing this, so when possible, sending either fully encrypted or tokenized data makes this process much simpler and more secure. In this scenario, from a security perspective, what remains is to secure the keys and the authentication processes.

[5] See https://www.pcisecuritystandards.org/document_library for the most current version of the PCI DSS

Authentication for Protecting Data

One final factor should be considered when protecting sensitive data in the higher education environment. It is valuable to first separate and consider environmental security protections independently from data security needs, and then combine solutions that can benefit both. However, when doing this, it is also important to understand that however data or the environment is secured, someone must also be in charge of maintaining a secure state for both. The credentials to administer the environment or to encrypt/decrypt the secured data are critical, dare we say key, to full protection of any data or environment. The more solutions employed to secure the environment and data, the more opportunities exist to have all that investment compromised.

When reviewing the solutions available, those that can offer security protection to cover encryption, tokenization, EMV and Ecommerce can reduce the footprint of vulnerable credentials. With this, the ability to secure the authentication of those credentials becomes paramount.

Complex Data Environments

For some organizations, size alone can create complex data security challenges, while for others, the industries that are involved introduce unique challenges – which is true in the case of higher education. The pandemic drove all organizations toward an increased need for Ecommerce. Most colleges and universities that once had one data security standard or framework may now have multiple standards and frameworks to contend with.

Before looking at a given solution, we summarize key components to look for in a complete solution for data protection:

- The ability to secure multiple data types, including:
  - *Financial data such as CHD and ACH Account Data*
  - *Privacy data such as PHI and PII*
- The ability to secure data with multiple security technologies, including:
  - *Encryption*
  - *Tokenization*
- The ability to secure multiple types of data input, including:
  - *Physical access (CP) such as card-present via devices, attended and unattended*
  - *Virtual access (CNP) such as web/Ecommerce, call centers, and mobile*
- The ability to leverage iFrame technologies and secure hosted fields to support in-page tokenization

- The ability to implement into IT environments that have multiple segments and different infrastructures
- The ability to simplify the scope of data secured within an environment
- The ability to support multiple third-party vendors
- The ability to apply each of the above in a single solution, including centralized management and awareness of all data secured

If you are using a variety of different solutions to cover each of these areas, it's time to consolidate and simplify your approach to payment and data security.

Bluefin´s payment and data security suite

PCI-validated P2PE

In 2014, Bluefin became the first PCI-validated P2PE solution provider in North America. Most encryption solutions at that time were not validated to the level of rigor that the PCI P2PE program requires. Bluefin's P2PE solution is one of very few that has been validated to all 3 versions of this technically difficult standard. Being built from the ground up, with P2PE inherent in the design, enabled Bluefin to meet and exceed the strict P2PE requirements.

PCI-validated P2PE provides numerous benefits over non-validated, or end-to-end encryption (E2EE), solutions, including reduced PCI scope, immediate encryption of card data, decryption only done in hardware outside the merchant environment, tamper-proof devices, and documented chain of custody processes to ensure security.

With Bluefin's P2PE solution, colleges and universities can choose several implementation options, select from over 100 validated payment devices, and utilize the company's P2PE Manager® - a 100% online portal for chain of custody activities and PCI attestation.[6] Additionally, Bluefin is partnered with multiple higher education software systems that provide our P2PE solution through their current integrations, including TouchNet, AudienceView, University Tickets, Blackbaud, Paciolan and more.[7]

[6] For a deeper dive into P2PE, download Bluefin's white paper, authored by Verizon, "The Value of Point-to-Point Encryption in POI Environments," https://www.bluefin.com/p/p2pe-white-paper/.
[7] A representative list of Bluefin partners can be seen at https://www.bluefin.com/partners/

P2PE Implementation Options

PayConex™ Gateway

PayConex provides merchants and integrated partners a payment processing platform with both P2PE and ShieldConex, protecting face-to-face, call center, mobile, and unattended payments, and online PHI, PII and financial data.

Decryptx®

Decryptx, Bluefin's Decryption as a Service (Daas) P2PE solution, enables payment gateways, processors and software vendors to directly connect to Bluefin and provide P2PE through their own platform. This option requires no change to existing processing relationships for partner merchants.

P2PE Direct

Larger retailers, universities and enterprises can directly connect to Bluefin's P2PE solution to support P2PE in their own environment.

ShieldConex®

Bluefin's ShieldConex data security platform has the ability to secure any data types entered online, including CHD, ACH data, PHI and PII.

ShieldConex leverages industry standard tokenization and hardware-based encryption methodologies in a proprietary way that can take input from any online format and allow the flexibility to use and access the data without exposing the data insecurely. ShieldConex is vaultless, meaning that Bluefin never stores any of the sensitive data, and only the organization using ShieldConex can access the original data in a way that is secure, scalable and fast.[8]

[8] For additional technical understanding, Bluefin's white paper highlights the values of vaultless tokenization and how FPT and FPE can be leveraged with multiple data types, https://www.bluefin.com/resources/media/white-papers-briefs/shieldconex-data-protection/.

With a cloud-based approach, ShieldConex can easily be integrated into multiple IT environments and through different third-parties connected to an organization's infrastructure. Key benefits include:

- Omni-channel tokenization (same CHD token across channels)
- iFrame technology for in-page tokenization
- Cloud-based implementation
- A global approach that supports direct and partner integrations
- Flexible access to all data types while maintaining data security
- Reduction of scope for security & compliance regulations & frameworks
- Scalability for changing data security needs
- High speed, secure access to sensitive data

Using ShieldConex in conjunction with P2PE adds the protection of physical data entry needs and offers industry standard encryption for additional data types, particularly payment data. Doing this all under one integrated solution offering can dramatically reduce scope and simplify the management of multiple security and compliance frameworks.

ShieldConex Implementation options

Integrated

The integrated approach leverages the entire Bluefin set of services, ShieldConex, PayConex and Decryptx, to cover all data input options, physical and online. This has the greatest reduction for the scope of the various standards and frameworks, especially PCI, ACH, HIPAA and GDPR.

Standalone

This method focuses on leveraging Bluefin's iFrame as a service. The data can be processed through any processor, and all data is fully tokenized and available for later use. This can descope various types of online data input via websites.

Partnership

This is a decoupled method that allows an organization to leverage the ability to tokenize large volumes of data, specifically privacy data types such as PHI and PII. This method helps with scope by removing the need to store sensitive data.

As your organization matures in the handling of data security, these various methods can be utilized to increase your data security posture.

Conclusion

If the two things certain in life are death and taxes, then the two things certain in payment and data security are change and requirements. Cyberthreats are constantly evolving, and the regulations and compliance frameworks to secure data must also change to keep up with these threats. As this complexity increases, the need to protect different types of data in different types of environments from different threats based on different requirements becomes increasingly challenging.

This paper explained each of the aspects surrounding data security with the goal of identifying key considerations when conquering your unique data security challenges. Regardless of the size of your organization, the technologies in use, the data handling requirements you face, or the maturity of your security approach, one thing stands out: the challenges you face can be simplified by a complete and comprehensive approach to protecting and managing data.

Cyberattacks in higher education show no signs of slowing – but you can quickly and effectively "devalue" CHD, PHI, PII and ACH Account Data with Bluefin's payment and data security products. Together, P2PE and ShieldConex offer the most complete and holistic solution for protecting payment and sensitive data across every campus channel.

About Bluefin

Bluefin is the recognized leader in encryption and tokenization technologies for payment and data security. The company's security suite includes PCI-validated point-to-point encryption (P2PE) for contactless face-to-face, call center, mobile and unattended payments, and our ShieldConex® data security platform for the protection of personally Identifiable Information (PII), Protected Health Information (PHI), and payment data entered online. The company's partner network currently includes over 200 processors, payment gateways and ISV's operating in 41 countries, which provide Bluefin's P2PE solutions direct to merchants, enterprises, healthcare and higher education organizations and more. Bluefin is a Participating Organization (PO) of the PCI Security Standards Council (SSC) and is headquartered in Atlanta, with offices in Waterford, Ireland. For more information, please visit https://www.bluefin.com.

About Alpine

Alpine was founded to fulfill a passion to help businesses and the people that work in them overcome today's cybersecurity challenges and succeed in new ways by leveraging the untapped value that an innovate approach to security can provide. With a background of over 20 years in technology, security and compliance, Alpine's skill set can help virtually any business learn how to leverage innovative security technologies with the result of translating security investments into tangible business value.