



Protecting PII:

Plain Talk About Protecting Personally Identifiable Information (PII) in Your SAP Environment

July 2011

Questions this paper will answer:

What is Personally Identifiable Information?

What obligations do I have to protect PII?

How do I structure an assessment of my PII security risks?

What challenges do I face in protecting PII in SAP?

What is Tokenization and how does it work in SAP?

What elements of PII protection are not addressed by Tokenization?

Is the data safer on-site or off-site?

How long does it take to set up my SAP shop for PII Tokenization?

In April 2011 hackers gained access to Sony's PS3 network and stole the personal information of 75 million people world wide - including people who stream Netflix or Hulu. The hackers potentially have information that includes credit card and other PII information.

I. Introduction to PII

Security breaches involving Personally Identifiable Information (PII) have been escalating over the past few years, resulting in millions of records and dollars lost. As an employer, you need to safely store the PII of your staff and contractors. This paper will help you learn how to secure this data, and will give you a foundation of language and concepts on which to establish in-house leadership on this topic.

Plainly, the breaches that involve PII can be costly to companies and individuals, for example the recent Playstation breach included credit cards and other PII information. Every company has PII data that can be breached. This Plain Talk white paper on Personally Identifiable Information (PII) will help you identify and protect the data in your SAP environment.

The Whys and Hows of PII

As an executive, an assessment of your potential weaknesses with respect to PII confidentiality is your responsibility. Reducing your organizational risk related to PII is not simple, but can be done with a common-sense, multi-step process. A recommended approach:

- a. Identify and minimize the PII you hold.
- b. Vet operating procedures and policies, and assure the effectiveness of employee security-awareness training.
- c. Assess IT system and database strengths and weaknesses (including test systems). *The latter includes, most importantly, adequately securing the data while in use, in storage and in transmission.*

While Princeton Payment Solutions provides solutions for securing PII, this document briefly sets that solution in its broader PII context. Here, we will lay out a framework: the whys and hows of minimizing the likelihood of a PII breach; nascent statutory obligations; and your intermediate goals in identifying and reducing risk. Then we'll move on to special SAP challenges in securing confidentiality, PII tokenization/ encryption as part of a comprehensive approach, and myths and facts in protecting PII.

Examples of Fields Being Protected

Data protected by Massachusetts and Texas Mandates

1. Social Security Number
2. Bank Account Number
3. Credit Account Number
4. Driver's License Number
5. Date of Birth

Other fields that have been requested

1. Resident or Tax ID Numbers
2. Salaries
3. Telephone Numbers
4. Addresses
5. Medical History Tags to Patient Name
6. Email Addresses
7. Passwords

Government PII Documents

NIST - Guide to Protecting the Confidentiality of Personally Identifiable Information

<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

Massachusetts (201 CMR 17)

<http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

also see

<http://www.networkworld.com/news/2009/111809-the-mass-201-cmr-17.html>

Nevada (NRS 603A)

<http://www.leg.state.nv.us/nrs/nrs-603a.html>

Texas - Identity Theft Enforcement and Protection Act of 2009

<http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm>

II. Understanding Personally Identifiable Information

PII is typically segregated into two categories:

1. Any information about an individual maintained by an organization, including any information that can be used to trace an individual's identity, such as name, social security number, address (street, e-mail, or even IP or MAC address), date and place of birth, or mother's maiden name.
2. Any other information that is linked or linkable to an individual, such as educational, employment, financial or medical data.

Disclosure of such information can be categorized as low, moderate or high risk, based on the potential harm that might result if the PII were inappropriately accessed, used or disclosed. Such harm ranges from a limited adverse effect ("minor" damage to corporate assets, or to individuals), to severe, or even a catastrophic adverse effect. For an individual this would mean loss of livelihood, blackmail, or even personal injury. For a corporation the inability to carry out one or more primary functions, or a crippling financial loss, or both, are possible consequences. The loss of PII on one of your own essential IT employees may be an overture, en route to hacking your most secure functions and databases.

Protecting the confidentiality of PII has been a concern since at least the 1980's. As modern life has become more computer-dependent, PII concerns continue to escalate. Identity theft has become a highly feared personal life event, the more so because the information is often stolen from a third party. A most serious threat to both corporate and government secure systems is ill-intentioned access by way of hijacked PII.

To motivate action, the U.S. federal government has passed legislation focused on specific high-risk industries (finance, healthcare). *Although those laws might not apply directly to your business, they have heightened public awareness and raised expectations.* (For instance, no federal law applied to Sony's failure to protect PII, but the public is still outraged.) In a similar vein, the U.S. National Institute of Standards and Technology (NIST) has published recommendations for protecting confidentiality of PII for government agencies, which raise the curtain on issues but don't spell out options. More specific direction comes from mandates published by individual states such as Massachusetts (201 CMR 17), Nevada (NRS 603A), and Texas (Identity Theft Enforcement and Protection Act of 2009, BCC Chapter 521). Those vary in their approach: either mandating the confidentiality of the PII of residents of those states (Mass.), or conferring specific obligations to protect PII on organizations doing business in those states (Nevada, Texas). In addition, four out of five states have enacted laws regarding the timely disclosure of data breaches to affected individuals.

Even if your company isn't affected by these laws, there are simple goals that make sense for every organization holding PII. Reducing risk needs a multi-pronged effort, but protecting data is elemental.

A May 2011 report by McAfee estimated that only 1 in 3 employees are “very aware” of their company’s mobile security policies, even though 95% of the 1500 organizations surveyed have policies in place. Further, four in ten organizations stated that they have had mobile devices lost or stolen, and half of those contained business-critical data.

See news item at

<http://www.securityweek.com/employees-dark-corporate-mobile-security-policies>

See full report

<http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf>

III. Goals of Securing PII – Minimizing the Risks

If you run on SAP, protecting personally identifiable information can present a distinct challenge. Protecting PII is not an auditable function, there are no standard questionnaires, and the data characteristics vary widely. Yet, it is not difficult to envision the elements of a “reasonable effort” to protect confidentiality, which would encompass all staff (education/training), operating procedures, and processes and technology (both software and hardware). *Your goal is simple: effectively and efficiently minimize the risks to all stakeholders* (your organization, your employees/vendors, and customers or others, if applicable).

At the same time, you don’t want this effort to be more complicated, time-consuming or expensive than necessary. To strike a balance, consider a common-sense approach, with three areas of focus to minimize various types of risk:

- Operational Safeguards
 - Policy and procedures
 - Education, training and awareness
- Privacy-specific Safeguards
 - Minimizing the use, collection and retention of PII
- Security Controls
 - Access enforcement (personnel access)
 - Separation of duties
 - Access control (remote or mobile device)
 - Auditable events, monitoring
 - Protection of data at rest, in use, and in transmission
 - Media sanitization prior to disposal in any form

A fourth area to consider is pre-planning the incident response to any breach involving PII, to be prepared to meet applicable state laws and mitigate consumer outrage. Preparation in this area does nothing to reduce risk, but is still important to your overall effort by properly addressing legal obligations and honoring consumer sensibilities following an incident.

These focus areas are straightforward but thorough. You need your IT, HR, and possibly finance/accounting and customer service/sales business teams to consider many technical angles of how PII data is handled, stored and transmitted, plus consider the human element (procedures, policies). You may eventually also pull in other corporate functions (building security, custodial services, communications, etc.). Data breaches are actually more likely to arise from internal human error (such as an unlocked office or unattended computer screen), or accident (personal computer stored in a car that is stolen, lost mobile device) than they are from a malicious attack. Protecting the data via encryption or tokenization won’t eliminate human error and accidents, but it will reduce the risk of unintended disclosure. You, and senior management, can rest easier.

A **token** is a surrogate, or voucher value that stands in for actual data in processing systems, while the original data is encrypted and resides in secure storage segregated from the ERP environment. A token strategy requires SAP to fetch the token when a record is called up, via a routine known as a "conversion exit." The original data remains encrypted and out of sight.

IV. The SAP Encryption Challenge

Introducing Tokenization

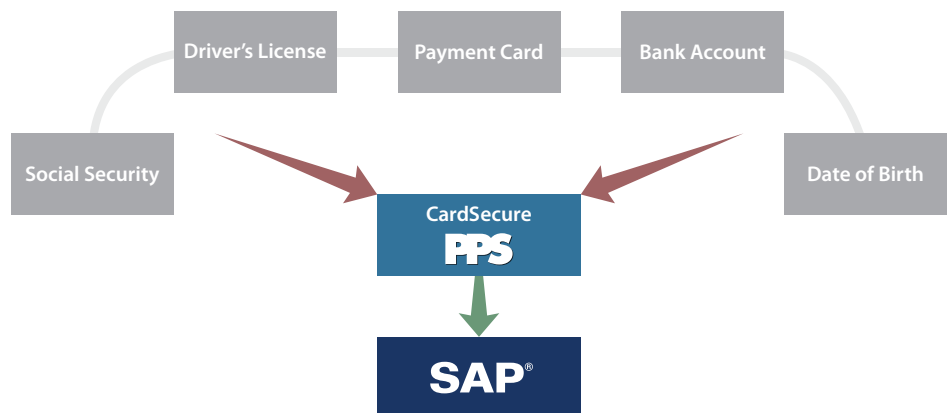
Encryption at the database level is a common activity, and is a primary defense for PII confidentiality. Many good solutions are available on the market to protect data such as payment card numbers. The same are often applicable to PII-type data. But not every solution is suitable for SAP. *Unfortunately, SAP does not normally work with encryption libraries other than its own, and SAP's encryption is not designed to work with PII data.* This situation creates a challenge for companies that use SAP to take reasonable steps to shield themselves from a high-risk incident, much less meet obligations under the state laws that mandate the protection of PII data. One route around these encryption issues is the newer technique of *tokenization*.

What are the criteria of a successful PII *tokenization* solution in SAP? The successful solution must address:

- SAP data field storage constraints on encrypted material
- Accommodation and adaptation of SAP logic checks
- Conversion exits
- Expedited implementation issues such as database conversion
- Ongoing PII database updates, for sales or customer service
- Transmission of PII to outside agencies (banks, tax authorities, etc)
- Exception reporting
- Sanitizing production data copied to other environments for testing

SAP's Hard-Coded Storage Constraints

SAP normally allots a fixed length for any one data field. However, encrypting a data element with a commercial grade algorithm creates a string longer than the standard field sizes allotted by SAP, which are highly structured based on common usage or industry standards. For example, a date-of-birth might be MM/DD/YY (or post-Y2K, MM/DD/YYYY). Thus a standard encryption algorithm fails to return a result that honors the field limit. One way to adapt the result is to utilize *tokenization* to tailor the result to SAP limits. This approach leads into a different but solvable issue with SAP functionality, the logic check.



Logic Checks

An attractive feature of a typical SAP database is the logic-check functionality built into the ERP to assure accurate data values, reducing the incidence of storing invalid data. Tokenization, which returns a scrambled alpha-numeric value, will trip these checks and stop the application from doing its job. Again, to use the date-of-birth example, SAP is checking for digits. A token application might return a combination of digits and alpha characters, which will fail the logic check. In order to utilize a token approach, the security solution must be designed to coordinate with the range of SAP's logic check capabilities, including:

- Support of special characters
- Support of country specific data types and double byte
- Masking techniques with a choice of identifiers before and after token values (including instance of no masking)
- Token formatting options to allow users to easily distinguish token values from authentic data, and provide enough information to allow confirmation

Database Conversion

In-house PII data is not as fluid as payment card information, so the successful security provider must be ready to provide knowledgeable implementation support for the database conversion of employee and vendor records. The solution must offer a "quick load" capability which circumvents the ERP system and works directly with the database, especially important for large installations. Conversion reports must be able to document the location of PII data, convert it, test its processing and restore it to production. Other conversion reports must confirm that each token is unique, and detect exception conditions needing attention.

Database Updates

In contrast to your internal PII needs, many businesses provide services as a third party, utilizing PII data supplied to them by a customer. Similarly, some businesses purchase PII databases (such as driver's license information) to use in verification of new customers. These databases need to be refreshed on a regular basis. The successful security solution will offer a quick-load capability which can easily be used to tokenize and encrypt for storage on a regular schedule, not just for a one-time conversion effort.

Data Warehousing Support

If your business engages in data mining of PII databases, you need a solution that can support a tokenized/encrypted database without interfering with your analytics.

Management Reporting

A successful PII tokenization solution will only maintain that status as long as assurance can be obtained that all data is properly shielded, and that no PII can be located in unexpected places beyond the scope of the tokenization effort. The solution provider should be prepared to deliver such reporting capabilities. Tokenized data also flows to available BI systems for reporting.

Sanitizing Production Data

Most ERP's routinely refresh test, or QA, systems with production data and sometimes development systems with some level of production data, a major security risk unless sensitive data is scrubbed immediately. An essential tool, a data scrubber eliminates that threat by replacing the production data, now stored in a non-production environment, with dummy PII values, sanitizing the QA systems without causing problems with SAP's database.

V. PII Tokenization as Part of a Comprehensive Approach

Earlier, on page 3, three possible areas of focus for your PII risk assessment were laid out:

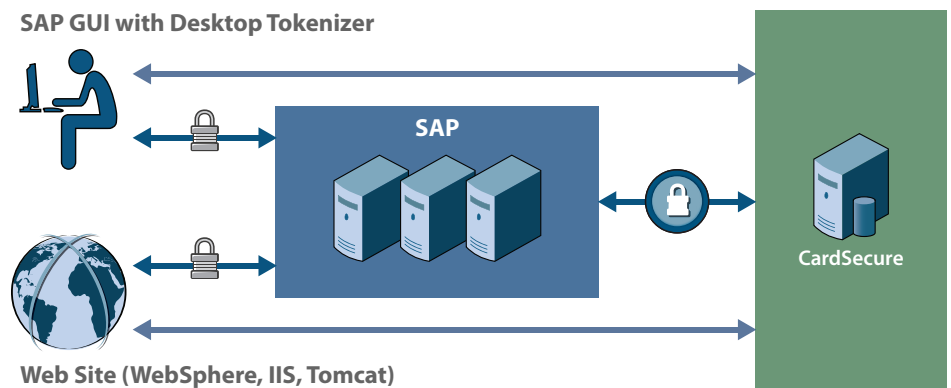
- Operational safeguards
- Privacy-specific safeguards
- Security controls

While it is beyond the scope of this offering to go into details on the first and second focus area, the issue of security controls/physical location of data storage is closely linked to minimizing risk via tokenization.

Assurance of the lock down of both internet and physical access to your PII data is a critical element of security control. Your system administration procedures for your production and test environments must comply with industry best practices. Plans for business continuity should be ready for you to execute at a moment's notice.

Tokenization with On-Site Storage

One option for PII data protection is an on-site tokenization engine with key management and key rollover. The engine will protect the data and store it (encrypted) in a hardened, secure onsite server, separate from the SAP application servers. The PII is secure both in storage and in handling.



Tokenization with Off-Site storage

A second option is to create the security capability described above but host it at an off-site facility. Having the data off-site is not an advantage as far as the PII laws to date, but the benefits are comparable to those received when you host card processing and data offsite for PCI purposes. Hosting offers you an offsite, turnkey, fully managed implementation of security applications dedicated to your business, including monthly patch management and daily log reviews. This service allows you to achieve a very high degree of confidence in:

- Protection of personally identifiable information (PII)
- Isolation of the servers and the databases from the public internet
- Stabilization of monthly expenses for security management

Off site assures the resiliency of your security package, and reduces your risk points to the minimum, while freeing staff time to focus on your core business.

VI. Charting a Timeframe for a PII Tokenization Project

Because tokenization involves coordination with an enterprise-level licensed product, it typically has a technically detailed installation period involving close collaboration between your staff and the vendor. That said, depending on the vendor's order book, a period of three months is normally sufficient for implementation.

VII. About PPS

Background

In 2003, the Princeton Payments Solutions group was formed to address the specific needs of the ERP Community with respect to complex payment environments. CardConnect, released in 2010, is the latest version. In 2004, PPS was the first company to encrypt data within an ERP system and pass the PCI audit standards with our CardSecure solution. Subsequently, responding to customer requests to remove SAP from PCI scope, and to address growing security concerns about personal information, PPS developed CardSecure's Token feature to take ERP systems completely out of PCI scope. Tokenization is now a highly desirable approach to securing personally identifiable information (PII). PPS clients include General Electric, Adobe, Brother, and Becton-Dickinson.

PPS Personnel

PPS staff are fully engaged with the security community focusing on card payment/processing issues. They meet regularly with Visa and MasterCard on security issues, and participate in the PCI Security Council. Their collective experience includes decades of experience in bank operations, bank software development, and bank card technology. They enjoy personal relationships with various technical groups within the bank processing community, underpinning PPS's innovative approaches to ERP card payment issues. In addition to technical expertise, PPS's credentials include advanced degrees in both business and economics. PPS staff understand your business challenges, offering payments and security expertise to address them.

www.prinpay.com

+1 609-919-0700

askus@prinpay.com