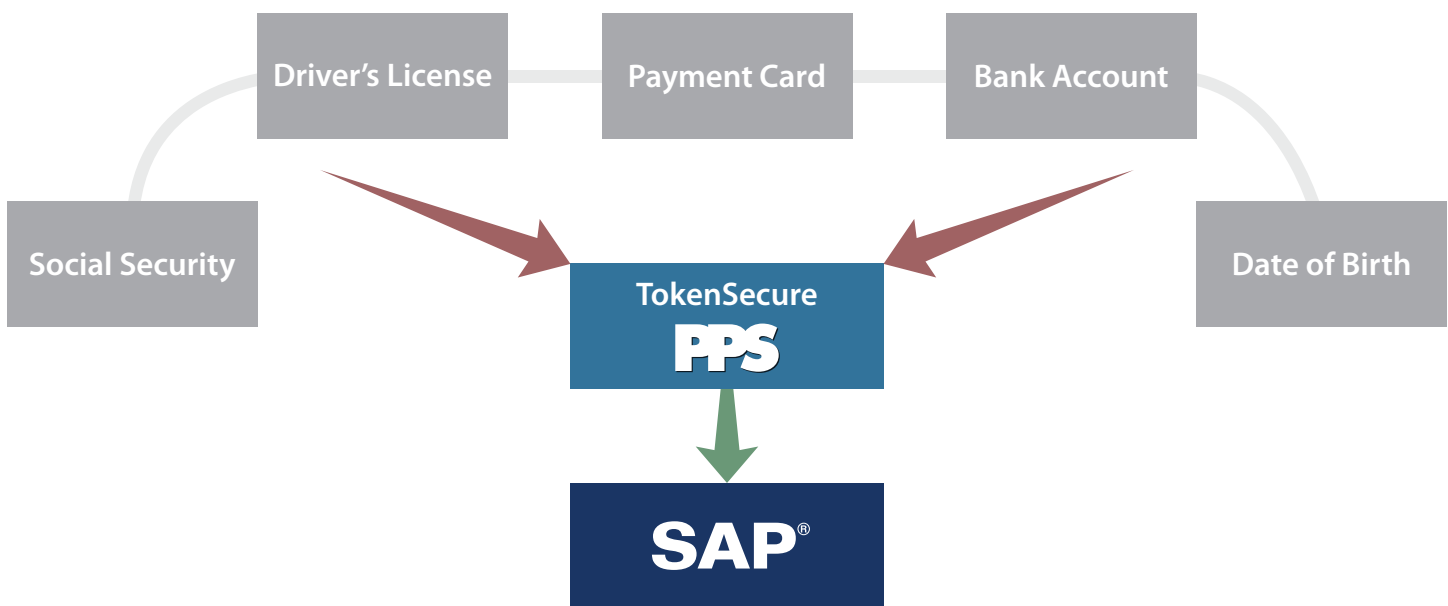


TokenSecure PII

Encryption for SAP involves two groups of data. The secure storage of the first group of data – credit card data – has been mandated by the card associations since 2004. The second group is categorized as personally identifiable information (known as PII), and includes social security numbers, driver's license details, and bank account data. The protection of this second group of data has been reinforced by a Massachusetts mandate, 201 CMR 17.00, and the Texas Personal Information Data Privacy Notification and Encryption Laws: Business and Commerce Code Chapter 521.

Normally, encryption at the database level is a common activity, and many good solutions on the market accomplish this. Unfortunately, SAP does not normally work with encryption libraries other than its own, and SAP's encryption does not meet the PCI data security requirements, nor is it designed to work with PII data. This situation makes it challenging for companies who use SAP to meet the PCI-DSS requirements and the new state laws that mandate the protection of PII data. This is an introduction to TokenSecure as a solution for the protection of personal information within the SAP environment.



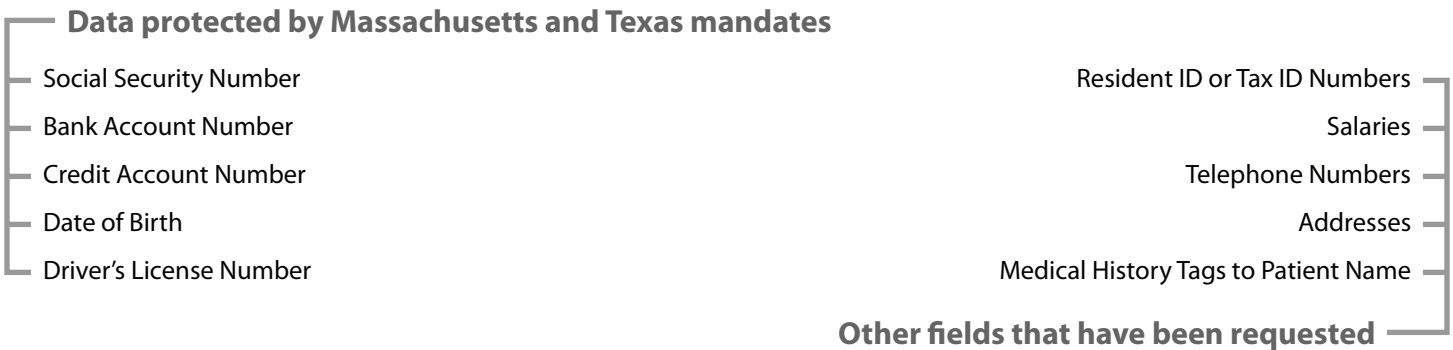
Protection of PII Data in ERP Systems

Over the past few years, a good deal of attention has been given to the protection of credit card data at the merchant level. Various systems have been developed to encrypt the data, and some even remove it completely from most applications and databases.

The same attention is now being directed to personal information that is deemed sensitive. This data, usually collected and monitored in the HR systems, has been referred to as Personally Identifiable Information, or PII. State legislatures, such as Massachusetts, have gotten involved in this issue, by defining PII data and creating legal mandates to protect it. While the requirement seems easier to put in place than the PCI card mandates, states may look to dovetail off the card security infrastructure requirements defined in the PCI-DSS.

The Problem

In most applications and databases, encryption is a straightforward process, but in SAP it can be a challenge. SAP normally allots a fixed length for any one field. Encrypting a data element with a commercial grade algorithm creates a string longer than the field size allotted by SAP. Another issue is the logic checks built into SAP to check data values. Giving a scrambled value will trip these checks and stop the application from doing its job.

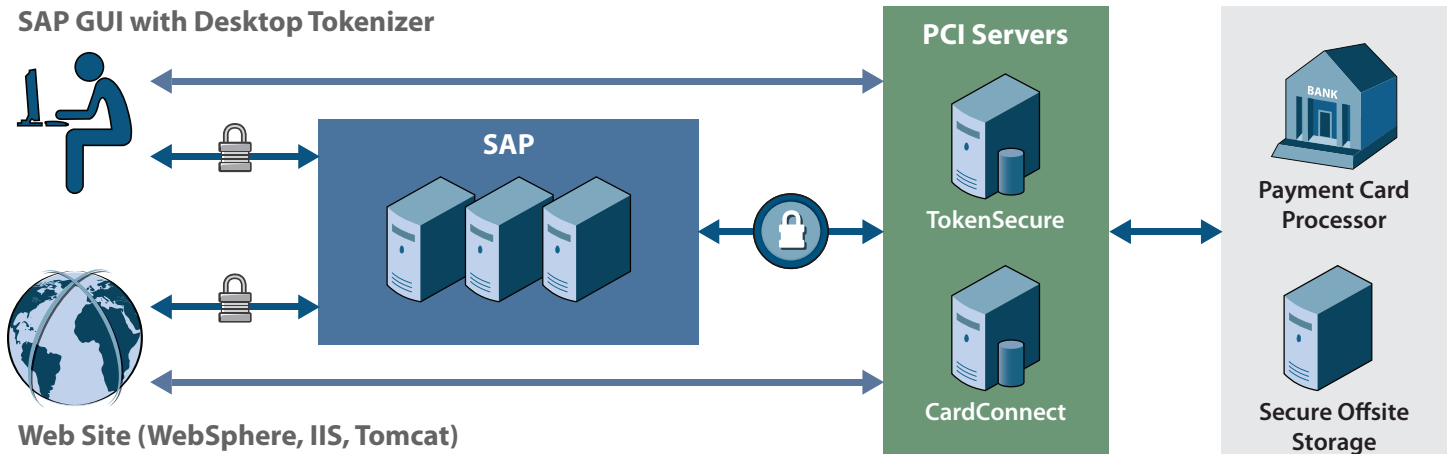


The Solution

The solution is to encrypt data externally, and feed a token or surrogate value back in to SAP that will fit in the space allotted by SAP, and pass the application logic checks. There are a number of tokenization offerings in the marketplace, but for an SAP facility certain factors should be taken into consideration before investing time and effort in a solution. Following are some of the most important:

1. Tokens must fit into space allotted for each data type by SAP.
2. Tokens should be designed to pass logic checks within SAP.
3. Special characters must be supported.
4. Country specific data types and double byte must be supported.
5. Masking techniques should provide a choice of identifiers before and after token values, including the choice of no masking in certain situations.
6. Token formatting options to allow users differentiate token values from real values, and provide enough information to allow confirmation (such as: 'last 4 of social').
7. Systems will need a quick load capability that circumvents the ERP system and works directly with the database, especially important for large installations that have millions of accounts.
8. Assurance that each token's value is unique, even if that value is expunged from the system and re-introduced later.
9. Availability of tools to tokenize data before entry into the target system, especially important for credit or debit card values, as this removes the target system from the scope of a PCI audit.
10. A management system that allows different access permissions to be assigned to users (i.e. give HR access to personnel data and Treasury access to banking data).
11. Solutions for Date of Birth – this presents unique challenges.

The TokenSecure Infrastructure - Options



Option 1: TokenSecure Encryption for on-site storage

The first option for PII data protection is an onsite encryption engine with key management and key rollover. The encryption engine will protect the data and store it in a secured onsite server, separate from the SAP application servers. The PPS solution adds a token layer that creates surrogate values to be used by the application for its day-to-day processes. This architecture enhances the security of your data, and allows personally identifiable information to be encrypted, using token or surrogate values specifically designed to fit into the space allotted by SAP.

Option 2: TokenSecure Encryption for off-site storage

The second option is to create the security capability described above but have it hosted at an off-site facility. Having the data off-site is not an advantage as far as the PII laws to date, but if card processing and data is now off-site for PCI purposes this may be considered a comparable function.

TokenSecure with CardZapper

Description

TokenSecure enables tokenization of payment card numbers within SAP. Tokens replace card numbers when the card number is entered into SAP. Tokens are then stored within the respective fields in the SAP database. The PII value or payment card number is encrypted, and then stored on the PPS TokenSecure server that is segregated from the SAP network.

The token incorporates the first 2 and last 4 digits of the card number, masking the rest of the value from SAP's display screens and reports. The token is de-tokenized for essential purposes, such as to check the card's validity. Selected users can be authorized to view the plain card number in SAP, however most sites restrict viewing the card to password-protected screens within the TokenSecure GUI.

Utility programs allow for the initial mass tokenization of each SAP table, with a back-up option. Key rollover to replace the encrypted value for each token occurs on the TokenSecure server, so the rollover has no impact on SAP performance.

CardZapper functionality can be added to TokenSecure to further protect data that lives on test and development systems. Most sites routinely refresh Test and Development systems with production data, a major security risk unless sensitive data is scrubbed

immediately. This tool eliminates that threat by replacing the production data, now stored in a non-production environment, with dummy payment card numbers, sanitizing the test system without causing problems with SAP's database.

PPS SAP Background

In 2003, the Princeton Payments group was approached by SAP AG to assist in the definition and creation of the first SAP-certified payment card interface (PCI). PayWare ERP was the first implementation and has since been a leader in complex SAP payment environments. Users of PayWare ERP include Becton Dickinson, General Electric, Brother International, Reliant Energy, Johnson & Johnson and SAP itself.

In 2004 PPS was the first to encrypt data within SAP and pass the PCI audit. For the past five years PPS has been installing PCI-DSS compliant encryption and tokenization systems. Users include Adobe, Brother, General Electric and Reliant Energy.

PPS has also introduced other payment technologies for:

- Automated reconciliation of bank deposit detail and fees
- Chargeback monitoring
- Payment infrastructure for returns, clearing A/R invoices and pre-payments
- Electronic checks, ACH, card swipe and terminal payments

Laws Protecting PII

US Federal Laws

- Title 18 of the United States Code, section 1028d(7)
- US 'Safe Harbor' Rules (EU Harmonization)
- Health Insurance Portability and Accountability Act (HIPAA), is to protect a patient's PII.

US State Laws

- California
 - » California Online Privacy Protection Act (OPPA) of 2003
- Massachusetts
 - » 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth
- Texas
 - » Texas Personal Information Data Privacy: Business and Commerce Code Chapter 521 [7]

Canadian Laws

- Privacy Act (governs the Federal Government agencies)
- Personal Information Protection and Electronic Documents Act (PIPEDA) of (2001 government entities)

For further information please contact Princeton Payment Solutions.

Contact: Alex Chapman
Email: achapman@prinpay.com
Phone: +1 (203) 952-5715
www.prinpay.com

