Securing Data Today and in the Future

Ulf Mattsson
CTO Protegrity

ulf.mattsson@protegrity.com
Ulf Mattsson

- 20 years with IBM Development & Global Services
- Inventor of 22 patents – Encryption and Tokenization
- Co-founder of Protegrity (Data Security)
- Research member of the International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security
- Member of
  - Cloud Security Alliance (CSA)
  - PCI Security Standards Council (PCI SSC)
  - American National Standards Institute (ANSI) X9
  - Information Systems Security Association (ISSA)
  - Information Systems Audit and Control Association (ISACA)
Cloud Security Debate

Encryption is better equipped than tokenization to secure data in the cloud.

October 01 2010

AGAINT

Ulf Mattsson
CTO, Protegrity

One of the biggest challenges of tokenization is a lack of transparency. Faster, decreases administrative risk, exposure of data by replacing sensitive data with non-sensitive data. That said, analysts take shortcuts and make other mistakes. Tokenization provides an alternative that is better equipped than encryption to protect data.

ISSA | PREEMINENT TRUSTED GLOBAL INFORMATION SECURITY COMMUNITY

Next Generation Tokenization for Compliance and Cloud Data Protection

By Ulf Mattsson – ISSA member, New York Metro, USA Chapter

This article will discuss how next-generation tokenization protects data as it flows across systems while minimizing PCI compliance costs.

Cloud Computing – Assessing Data Security Risks and Solutions

Ulf Mattsson
CTO
Protegrity

Making Sense of the Sony Breach

April 2011 by Ulf Mattsson, CTO, Protegrity Corporation
Guidance from Cloud Security Alliance

Security Guidance for Critical Areas of Focus in Cloud Computing

Top Threats to Cloud Computing V1.0
“Cloud – Like a Parking Garage”
Risks Associated with Cloud Computing

- Handing over sensitive data to a third party
- Threat of data breach or loss
- Weakening of corporate network security
- Uptime/business continuity
- Financial strength of the cloud computing provider
- Inability to customize applications

Source: The evolving role of IT managers and CIOs Findings from the 2010 IBM Global IT Risk Study
“Pass Security Before Entering The Cloud”

Unprotected sensitive information:  

Protected sensitive information  

123456 123456 1234  

123456 123456 1234  

123456 999999 1234  

123456 999999 1234  

Cloud  

Security Check Point  

User  

Secured data  

Sensitive data
“It is fascinating that the top threat events in both 2010 and 2011 are the same and involve external agents hacking and installing malware to compromise the confidentiality and integrity of servers.”


Data Breaches – Mainly Online Data Records

- 900+ breaches
- 900+ million compromised records:

Source: 2010 Data Breach Investigations Report, Verizon Business RISK team and USSS
Compromised Data Types - # Records

- Payment card data
- Personal information
- Usernames, passwords
- Intellectual property
- Bank account data
- Medical records
- Classified information
- System information
- Sensitive organizational data

Source: Data Breach Investigations Report, Verizon Business RISK team and USSS
Industry Groups Represented - # Breaches

- Hospitality
- Retail
- Financial Services
- Government
- Tech Services
- Manufacturing
- Transportation
- Media
- Healthcare
- Business Services

Source: Data Breach Investigations Report, Verizon Business RISK team and USSS
Breach Discovery Methods - # Breaches

- Third party fraud detection
- Notified by law enforcement
- Reported by customer/partner
- Unusual system behavior
- Reported by employee
- Internal security audit or scan
- Internal fraud detection
- Brag or blackmail by perpetrator
- Third party monitoring service

Source: Data Breach Investigations Report, Verizon Business RISK team and USSS
Example of How the Problem is Occurring – PCI DSS

Source: PCI Security Standards Council, 2011
How can the problem be solved?
- Tokenization and other options can reduce the risk

Source: PCI Security Standards Council, 2011
Amazon Cloud & PCI DSS

- Just because AWS is certified doesn't mean you are
  - You still need to deploy a PCI compliant application/service and anything on AWS is still within your assessment scope

- PCI-DSS 2.0 doesn't address multi-tenancy concerns

- You can store PAN data on S3, but it still needs to be encrypted in accordance with PCI-DSS requirements
  - Amazon doesn't do this for you
  - You need to implement key management, rotation, logging, etc.

- If you deploy a server instance in EC2 it still needs to be assessed by your QSA (PCI auditor)
  - Organization's assessment scope isn't necessarily reduced

- Tokenization can reduce your handling of PAN data

Tokenization Use Case Example

- A leading retail chain
  - 1500 locations in the U.S. market

- Simplify PCI Compliance
  - 98% of Use Cases out of audit scope
  - Ease of install (had 18 PCI initiatives at one time)

- Tokenization solution was implemented in 2 weeks
  - Reduced PCI Audit from 7 months to 3 months
  - No 3rd Party code modifications
  - Proved to be the best performance option
  - 700,000 transactions per days
  - 50 million card holder data records
  - Conversion took 90 minutes (plan was 30 days)
  - Next step – tokenization server at 1500 locations
Evaluating Options
## Evaluating Field Encryption & Tokenization

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Strong Field Encryption</th>
<th>Formatted Encryption</th>
<th>Tokenization (distributed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnected environments</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Distributed environments</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Performance impact when loading data</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transparent to applications</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Expanded storage size</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transparent to databases schema</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Long life-cycle data</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Unix or Windows mixed with “big iron” (EBCDIC)</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Easy re-keying of data in a data flow</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>High risk data</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security - compliance to PCI, NIST</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Best  ●  ●  ●  ●  Worst
Choose Your Defenses – Different Approaches

Applications
- Web Application Firewall
- Database Activity Monitoring
- Data Loss Prevention

Web Application Firewall
- Database Activity Monitoring
- Data Files
- Database Log Files
- Database Server
- Encryption/Tokenization

Database Server
- Database Log Files
- Database Columns
- Data Files
- Encryption/Tokenization
Choose Your Defenses – Cost Effective PCI DSS

- Firewalls
- Encryption/Tokenization for data at rest
- Anti-virus & anti-malware solution
- Encryption for data in motion
- Access governance systems
- Identity & access management systems
- Correlation or event management systems
- Web application firewalls (WAF)
- Endpoint encryption solution
- Data loss prevention systems (DLP)
- Intrusion detection or prevention systems
- Database scanning and monitoring (DAM)
- ID & credentialing system

Source: 2009 PCI DSS Compliance Survey, Ponemon Institute
Best Practices - Data Security Management

- Application Protector
- File System Protector
- Database Protector
- Tokenization Server
- Secure Archive
- Policy
- Audit Log

Enterprise Data Security Administrator
## Vendors/Products Providing Database Protection

<table>
<thead>
<tr>
<th>Feature</th>
<th>3rd Party</th>
<th>Oracle 9</th>
<th>Oracle 10</th>
<th>Oracle 11</th>
<th>IBM DB2</th>
<th>MS SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database file encryption</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Database column encryption</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Column encryption adds 32-52 bytes (10.2.0.4, 11.1.0.7)</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Formatted encryption</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Data tokenization</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Database activity monitoring</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Multi vendor encryption</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Data masking</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Central key management</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>HSM support (11.1.0.7)</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Re-key support (tablespace)</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

**Best**: ●

**Worst**: ○
## Vendors Providing Strong Encryption

<table>
<thead>
<tr>
<th>Feature</th>
<th>Vendor A</th>
<th>Vendor B</th>
<th>Vendor C</th>
<th>Oracle</th>
<th>Vendor D</th>
<th>Vendor E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software solution</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>HSM support</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Database support</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>File encryption support</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Performance</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>FIPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Availability</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Central key management</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Best: ● ● ● ● ● ●  Worst: ○ ○ ○ ○ ○ ○
# Column Encryption Solutions – Some Considerations

<table>
<thead>
<tr>
<th>Area of Evaluation</th>
<th>3rd Party</th>
<th>Oracle 10 TDE</th>
<th>Oracle 11 TDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance, manage UDT or views/triggers</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Support for both encryption and replication</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Support for Oracle Domain Index for fast search</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Keys are local; re-encryption if moving A -&gt; B</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Separation of duties/key control vector</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Encryption format specified</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Data type support</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Index support beyond equality comparison</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>HSM (hardware crypto) support (11.1.0.6)</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HSM password not stored in file</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Automated and secure master key backup procedure</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Keys exportable</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

**Best** ✔️ ✔️ ✔️ ✔️ ✔️ **Worst**
Oracle Domain Index

Enc, Foreign and Primary Keys in the where clause

Select * from test2 with sub-select in the where clause

Enc in select and where clause, 6 tables containing encrypted columns.
Choose Your Defenses – Total Cost of Ownership

- **Cost of Aversion – Protection of Data**
- **Expected Losses from the Risk**
- **Total Cost**
- **Optimal Risk**

- **Strong Protection**
- **Weak Protection**

- **Total Cost of Ownership X**
Case Studies – Retail Environments

- **Point of Sale**
  - ‘Information in the wild’
    - • Short lifecycle / High risk

- **E-Commerce**
  - Temporary information
    - • Short lifecycle / High risk

- **Branch Office**
  - Operating information
    - • Typically 1 or more year lifecycle

- **Aggregation**
  - Decision making information
    - • Typically multi-year lifecycle
    - • High volume database analysis
    - • Wide internal audience with privileges

- **Operations**
  - Archive
    - • Typically multi-year lifecycle

- **Analysis**
  - Encryption service
Quality of Systems Testing vs. Data Exposure

Quality of Testing (Analytics ...)

High

Low

Quality Of Data

High

Low
Data Security Life Cycle – Reversible Protection

Data Quality & Exposed Details
- 3rd Party Interface Testing
- Data Entry
- Partner Interface
- Two-Way Masking

Unprotected sensitive information:  
Protected sensitive information
Data Protection – Reversible or Not

Data Quality & Exposed Details

- 3rd Party Interface
- Testing
- Data Entry
- Partner Interface

High

Low

Fire Fighting
Two-Way Masking

Development Testing Staging Production Operational Analytics Archive

Unprotected sensitive information: Protected sensitive information
Limit Exposure to Sensitive Data

Exposure to sensitive data

Development

Testing

Production

Data encoding:
1. Tokenization
2. Encryption
Data Tokens in a Cloud Environment – Integration Example

Tokenization Gateway

Tokenization Gateway

Application Databases

Cloud Environment

Unprotected sensitive information: 990-23-1013

Protected sensitive information: 4000 0012 3456 7899

Data Tokens in a Cloud Environment – Integration Example

Tokenization Gateway

Application Databases

Cloud Environment

Unprotected sensitive information: 123-45-1013

Protected sensitive information: 40 12 3456 7890 7899

Data Tokens in a Cloud Environment – Integration Example

Tokenization Gateway

Application Databases

Cloud Environment

Unprotected sensitive information: 990-23-1013

Protected sensitive information: 4000 0012 3456 7899

Data Tokens in a Cloud Environment – Integration Example

Tokenization Gateway

Application Databases

Cloud Environment

Unprotected sensitive information: 123-45-1013

Protected sensitive information: 40 12 3456 7890 7899
Data Tokens in a Cloud Environment – Integration Example

Unprotected sensitive information:  
Protected sensitive information

: Data Token
Data Tokenization at the Gateway Layer

Unprotected sensitive information: ____________________________

Protected sensitive information: ____________________________

: Data Token
Data Tokenization at the Gateway Layer

: Data Token

Unprotected sensitive information: 
Protected sensitive information: 

035
Data Tokenization at the Application Layer

User

Application

Token Server

Database

Cloud

: Data Token

Unprotected sensitive information: 
Protected sensitive information: 

: Social Security Card

: Visa Card

: Security Admin

: protegrity
Data Tokenization at the Database Layer

Unprotected sensitive information:  
Protected sensitive information

: Data Token
Solving 5 Business Issues with 7 Technical Features

**Business Issues**  ➔  **Business Benefits**  ➔  **Technical Features**

- **Token collisions and duplications**  ➔  **No collisions**
  - Fully distributed approach
  - No synchronization needed

- **High latency**
  - 100 ms
  - Tokenization close to the data

- **Low performance**
  - 20 tokens/s
  - All in memory – no disk operations

- **High cost, size & complexity**
  - 50 mil+ records
  - Small system footprint < 5 million records
  - Supports standard HW/SW for load balancing, HA and DR

- **Algorithm could be breached**  ➔  **No algorithm**
  - Several layers of fully random tables

- **Low performance**
  - 200,000+ tokens/s
  - Minimized latency < 1 ms

- **High cost, size & complexity**
  - 50 mil+ records
  - Low cost & simplicity
Securing Encryption Keys

An entity that uses a given key should not be the entity that stores that key.

Source: http://csrc.nist.gov/groups/SNS/cloud-computing/
Hiding Data in Plain Sight – Data Tokenization

Unprotected sensitive information:

Protected sensitive information:
Deploy Defenses

Matching Data Protection Solutions with Risk Level

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Number</td>
<td>25</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>20</td>
</tr>
<tr>
<td>CVV</td>
<td>20</td>
</tr>
<tr>
<td>Customer Name</td>
<td>12</td>
</tr>
<tr>
<td>Secret Formula</td>
<td>10</td>
</tr>
<tr>
<td>Employee Name</td>
<td>9</td>
</tr>
<tr>
<td>Employee Health Record</td>
<td>6</td>
</tr>
<tr>
<td>Zip Code</td>
<td>3</td>
</tr>
</tbody>
</table>

- **Low Risk** (1-5) - Monitor
- **At Risk** (6-15) - Monitor, mask, access control limits, format control
- **High Risk** (16-25) - Replacement, strong encryption

---

[Protegrity logo]
Please contact me for more information

Ulf Mattsson

Ulf. Mattsson AT protegrity. com
Summary

1. With the rising cost of data security breaches and their increasing frequency, companies are starting to reevaluate how they protect their data.

2. External and internal breaches have highlighted the need for companies to understand the flow of data within the enterprise and the need to take a more granular approach in terms of how it is secured.

3. This session will discuss recent breaches and review different options for data protection strategies in a cloud and outsourced environment.
US Laws - Privacy and Data Security Risks in Cloud

- HIPAA Restrictions on Health Data
  - Covered entity would risk a HIPAA violation by using such a provider for data storage.

- Breach Provisions Under HITECH Act
  - To the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act.

- Gramm-Leach-Bliley Act - GLBA
  - GLB's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties

- State Information Security Laws
  - For example, California requires businesses that disclose personal information to nonaffiliated third parties to include contractual obligations that those entities maintain reasonable security procedures

- State Breach Notification Laws
  - Over 45 U.S. states and other jurisdictions have data security breach notification laws that require data owners to notify individuals whose computerized personal information has been subject to unauthorized access

- Massachusetts regulations
  - Must determine whether the cloud provider maintains appropriate security measures to protect the data to be stored
US Legislation
US Laws - Privacy and Data Security Risks in Cloud

- **HIPAA Restrictions on Health Data**
  - Covered entity would risk a HIPAA violation by using such a provider for data storage.

- **Breach Provisions Under HITECH Act**
  - To the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act.

- **Gramm-Leach-Bliley Act - GLBA**
  - GLB's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties

- **State Information Security Laws**
  - For example, California requires businesses that disclose personal information to nonaffiliated third parties to include contractual obligations that those entities maintain reasonable security procedures

- **State Breach Notification Laws**
  - Over 45 U.S. states and other jurisdictions have data security breach notification laws that require data owners to notify individuals whose computerized personal information has been subject to unauthorized access

- **Massachusetts regulations**
  - Must determine whether the cloud provider maintains appropriate security measures to protect the data to be stored
Best Practices and Regulations
Case Study: Global Investment Banking and Securities

Investment banking division
- Encryption of Deal related attributes and other MNPI data (i.e. company name, company identifier, etc)
- Prevented development and technology people to identify entities involved in deals

Compliance department
- Compliance has TWO copies of Deal data – one for the Conflicts Process and one for the Control Room
- Encryption KEYS are DIFFERENT in Banking and Compliance

Encryption of compensation data

Encryption of firewall rules
- Managed in a standalone application

Platforms:
- Oracle, DB2, SQL Server, UNIX, Linux and Windows
Best Practices from NIST on PII Data - SP800-122

Examples of PII Data

1. Name
2. Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number
3. Address information
4. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address
5. Telephone numbers
6. Personal characteristics, including photographic image
7. Information identifying personally owned property
8. Information about an individual that is linked or linkable to one of the above

Source: National Institute of Standards & Technology - NIST (http://csrc.nist.gov/)
SEC Adopted Regulation S-P to Address Privacy

1. Like GLB (Gramm-Leach-Bliley Act), compliance with Regulation S-P (17 CFR Part 248) is mandatory since July 1, 2001

2. Regulation S-P provides the means of implementing GLB

3. Every broker, dealer, and investment company, and every investment adviser registered with the SEC must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information

4. Insure the security and confidentiality of customer records and information

5. Protect against any anticipated threats or hazards to the security or integrity of customer records and information

6. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer
[1] Establishes a Federal Breach Notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.

[2] Ensures that new entities that were not contemplated when the Federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.

[3] Provide transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record.

[4] Shutting down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual’s health information without their authorization.

[5] Requires that providers attain authorization from a patient in order to use their health information for marketing and fundraising activities.


• Health Insurance Portability and Accountability Act (HIPAA) of 1996
• Health Information Technology for Economic and Clinical Health Act (HITECH Act), of 2009
Example: HIPAA – 18 Direct Identifiers

1. Names
2. Geographic subdivisions smaller than a state, including
3. All elements of dates (e.g., date of birth, admission)
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal locators (URLs)
15. IP address numbers
16. Biometric identifiers, including fingerprints and voice prints
17. Full-face photographic images and any comparable images
18. Other unique identifying numbers, characteristics or codes
The Massachusetts law is the first in the nation to require specific technology when protecting personal information. Both "data at rest" and "data in transit" over a public network, such as the Internet, that contain personal information must be encrypted.

- Personal information is defined as a Massachusetts resident's name in combination with one of the following:
  
  **Social Security number**, **Driver's license number** or state-issued identification card number and Financial **account number** or **credit/debit card number**
## Visa Best Practices for Tokenization Version 1

Published July 14, 2010.

<table>
<thead>
<tr>
<th>Token Generation</th>
<th>Single Use Token</th>
<th>Multi Use Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm and Key <strong>Reversible</strong></td>
<td>Known strong algorithm (NIST Approved)</td>
<td>✓</td>
</tr>
<tr>
<td>One way <strong>Irreversible</strong> Function</td>
<td>Unique Sequence Number</td>
<td>✓</td>
</tr>
<tr>
<td>Hash</td>
<td>Secret per transaction</td>
<td>✓</td>
</tr>
<tr>
<td>Randomly generated value</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Best Practices Summary

- Reduce attack surface and compliance scope
  - Separation of System Components
- Separation of Duties: DBA, Risk Manager, etc.
  - Get the DBA off the hook – Not a Suspect
- Security can be highly transparent to developers
- Less documentation necessary
# Making Data Unreadable – Protection Methods (Pro’s & Con’s)

<table>
<thead>
<tr>
<th>IO Interface</th>
<th>Granularity</th>
<th>Protection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Layer</td>
<td>Granularity</td>
<td>AES/CBC, AES/CTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Formatted Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Tokenization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Masking</td>
</tr>
<tr>
<td>Application</td>
<td>Column/Field</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Record</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Database</td>
<td>Column</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Table</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Table Space</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>OS File</td>
<td>IO Block</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>Storage</td>
<td>IO Block</td>
<td>○</td>
</tr>
<tr>
<td>System</td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
</tr>
</tbody>
</table>

Best  ●  ○  ○  ○  ○  Worse
De-identified information can be assigned a PII confidentiality impact level of *low, as long as the following are both true:*

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information.
- The data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.

*Source: National Institute of Standards & Technology - NIST (http://csrc.nist.gov/)*
Mapping the Cloud to Compliance – PCI DSS

Cloud Service Models

- **Applications**
- **Data** / Meta-data / Content

SaaS – Software as a Service

Middleware

PaaS – Platform as a Service

Hardware

IaaS – Infrastructure as a Service

Compliance Model – PCI DSS

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Source: http://csrc.nist.gov/groups/SNS/cloud-computing/