protegrity

Solutions Overview

Secure.Data™ for Oracle® Database

A Solution to Facilitate Compliance with New Privacy and Security Requirements on Sensitive Information Stored in Oracle Databases

- ✓ **Penetration tested by Oracle's European Security Practice.**
- ✓ **Certified for interoperability with Oracle9*i* Application Server Release 2.**
- ✓ **Built for interoperability with Oracle Applications.**
- ✓ **Interoperable with nCipher's FIPS 140 level 3 certified nShield™ Hardware Security Module.**
- ✓ **OPSEC™ certified for interoperability with Check Point™ VPN-1™/Firewall-1™.**
- ✓ **RSA SecurID® ready.**

About Protegrity, Inc.

Protegrity's information-privacy solutions and services provide businesses with a powerful and flexible means of protecting the confidential information contained in enterprise relational databases. The Secure.Data™ solution is the only system in the world to encrypt and secure database information at the data-item level and is designed to be fully deployable into production environments. It is also the only third party data protection and privacy enforcement technology integrated with Oracle®, IBM® DB2® UDB, IBM® Informix®, Microsoft® SQL Server™, and Sybase® ASE databases, thus now providing organizations with the means to meet new global privacy and data protection legislation that calls specifically for the cryptographic protection of stored data. Working closely with these database vendors, Protegrity® has developed the Secure.Data suite of products to address the rapidly evolving ebusiness requirement for stored data protection, such as credit card numbers, PIN numbers, patient records, and other personnally identifiable data and/or mission critical corporate information. Secure.Data operates independently of and transparently to applications, protecting the privacy of this nonpublic information against both internal and external threats. Protegrity, which was established in 1996, is based in Stamford, Connecticut, U.S.A. and its R&D and European sales offices in Sweden. More information is available at www.protegrity.com

Acknowledgements:

Author: Thomas McGough

Contributors: Ulf G. Dahl
Ulf Mattsson
Tom Molin
Patrik Nilsson
Christian Olsson

Document No. PWP0011

Fourth Edition: September 26, 2002

Website: www.protegrity.com

Americas and Asia-Pacific
Protegrity Incorporated
1177 Summer Street
Stamford, Connecticut 06905-5529, U.S.A.
Tel: +1 203-326-7200
Fax: +1 203-326-7250
Email: sales@protegrity.com

Europe, Middle East And Africa
Protegrity Nordic AB
Box 5050, Nääs Fabriker
SE-448 51 Tollered, Sweden
Phone: +46-31-755-2520
Fax: +46-31-755-2524
Email: nordic@protegrity.com

CONTENT

I. Introduction

By now, we have all seen the headlines: "*Hacker Steals Thousands of Credit Card Numbers from XYZ, Inc*". Data theft is a very real problem facing organizations today. Studies like the seventh annual joint U.S. FBI/Computer Security Institute (CSI) Computer Crime and Security Survey released on April 7, 2002 identifies that U.S. companies and government agencies report losing more money from theft of proprietary information than any other type of attack on their computer systems. Seventy-five percent of the companies do not report intrusions to law enforcement because of negative publicity, and 72% said that they don't because they do not want to give competitors an advantage. Historically, the theft of proprietary information and the mechanisms to protect it have been in existence since the owners of data became aware of the power and sensitivity of information. Julius Caesar is considered to have been one of the first to use encryption to secure private communications (The Caesar cipher was an early algorithm used by Caesar to communicate with his army). Bring today's hacker into Caesar's world and rather than focus on intercepting and deciphering the individual messages en route to the army, he would head for Rome, break into Caesar's palace and steal all of the plain-text scrolls that he could get his hands on.

In today's world, databases hold the sensitive/confidential information. Although security mechanisms have been adapted to support the evolution of communication, they still take the outside-in approach toward security. The focus is on securing the perimeter, leaving sensitive information on the inside exposed to anyone who gains or has access to the inside. As the headlines indicate, hackers regularly penetrate perimeter defenses and focus their efforts where the reward is greatest; the database. Credit card numbers, social security numbers, personal information required to be protected by Privacy legislation, trade secrets, proprietary source code, and other sensitive information often lies totally unprotected in databases. This data is accessible by a savvy hacker or trusted insider.

In order to fully understand this problem, it is also important to remember that it is often much easier to access these databases from the inside of a protected network. Looking at the Caesar example, rather than trying to get past the superior perimeter and interior security of the palace, it would have been a lot easier to pay Brutus a large sum of money for the same information contained in the plain-text scrolls. Relational databases are at risk even if an institution has established perimeter controls like a firewall and network security.

This is validated by today's security figures. While statistics vary, a conservative estimate would indicate that 30% to 70% of security incidents come from inside the firewall. Recent surveys conducted by the FBI and Computer Security Institute suggests that the greatest risk to corporate security arises from internal sources. The 2002 CSI/FBI computer security issues and trends study confirms the trend. Ninety percent of respondents detected computer security breaches within the last 12 months. Eighty percent acknowledged financial losses due to computer breaches. Forty-four percent were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses. As in previous years, the most serious financial losses occurred through the theft of proprietary information occurring in 20% of the respondents. These originated from both internal and external sources in virtually equal numbers. Client/server architecture and today's distributed computing environments leave the database and the proprietary information unprotected by traditional perimeter solutions.

Whether accessed from the outside or inside, the weakest link in a company's security policy is quite often the database. Protegrity Secure.Data solution was designed to strengthen this weakest link in the security chain. Using strong encryption and advanced key management, Secure.Data hardens database defenses of residing sensitive information with an "inside-out" approach to database security. This section of the document describes the theory and implementation of the last line of defense against the misuse of what we call sensitive data that resides in databases. From this document, the reader will gain a clear understanding of the key concepts, design principles, architecture, and a basic operational model of Secure.Data that together describe our commitment to protecting your most valuable digital assets from unauthorized access of any kind.

The implications of this "inside-out" approach to data security are far-reaching. Secure.Data is designed for organizations in every business vertical. Financial and health institutions have been targeted by new Government legislation and requirements worldwide. Business requirements for selective protection of data in databases are growing at exponential rates. This can be attributed to tangible or intangible forces. On the tangible side:

- Information-privacy legislation which mandate controlling access include:
  - ✓ U.S. Gramm-Leach-Bliley Act, GLBA) extended with the U.S. Office of the Comptroller of Currency (OCC) requirements for the financial services industry.
  - ✓ U.S. Healthcare Insurance Portability and Accountability Act (HIPAA).
  - ✓ U.S. Food & Drug Administration (FDA) 21CFR 11 Electronic Records; Electronic Signatures for Clinical Trials.
  - ✓ European Union (EU) 95/46/EC Directive on Data Privacy (Safe Harbor) and individual EU member state privacy legislation.
  - ✓ Canada's Personal Information Protection and Electronic Document Act (PIPEDA).
  - ✓ Australia's Privacy Act.

- Industry initiatives which mandate controlling access include:
  - ✓ American Express Merchant Services Data Security Standards.
  - ✓ MasterCard Site Data Protection Service.
  - ✓ VISA U.S.A. Cardholder Information Security Program (CISP).
  - ✓ VISA 3D Secure specifications for cardholder data protection.
  - ✓ U.S. Software and Information Industry Association (SIIA) - A method for securing credit card and private consumer data in e-business sites.
  - ✓ ISO/IEC 17799:2000 - Information technology -- Code of practice for information security management.

All the above require the protection, segregation and audit of sensitive data at rest within the database. Secure.Data satisfies this and all of the other critical security and privacy requirements.

II. Value Statement Summary on Securing and Controlling Access to Digital Assets

Working closely with Oracle, Protegrity has developed Secure.Data for Oracle Databases to address the rapidly evolving requirements for stored data protection. Secure.Data is the most advanced "out-of-the-box" automated database access control solution with extensive key management capabilities for selectively encrypting, securing and controlling access to database information at the data-item level. Secure.Data is application transparent, which allows for fast integration, cost-effective security and privacy mandate compliance. It is an effective last line of defense protecting against unauthorized and un-auditable access:

- Selective and highly secure, column-level **data item encryption.**
- Cryptographically enforced **authorization.**
- Comprehensive and secure software and hardware **key management.**
- **Secure audit and reporting** facility.
- Enforced **segregation of duties.**
- **Centralized** console for control, administration and management of data **security policies and procedures.**

The Secure.Data database protection system (see Figure 1) actively encrypts data within enterprise databases, securing information at the data-storage level. Secure.Data automates the encryption of sensitive data in selected columns of a database and provides role-based access control to allow users to retrieve protected data based on roles and functions within an organization. The Secure.Data suite includes Secure.Data Manager™ the main administration module where database privacy rules and policies are established, and the Secure.Data Server™ component that actively enforces encryption and access control security procedures.

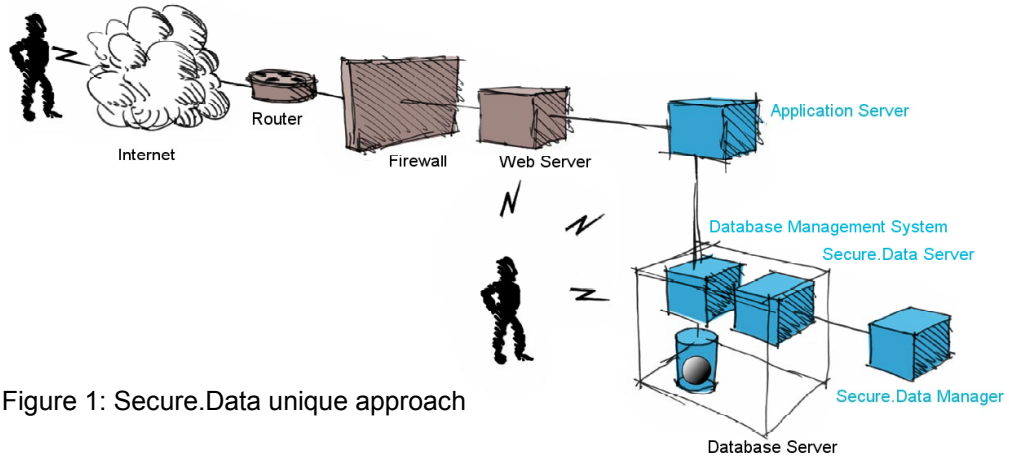

Figure 1: Secure.Data unique approach

.

Secure.Data is:

- An out-of-the-box security solution that completely protects the database, is easily implemented in one to three days, and work with no changes to underlying applications.
- Selective encryption of data where it is most vulnerable – at rest in databases.
- Designed to seamlessly run within an Oracle environment providing organizations with a readily deployable comprehensive encryption software key-management solution. This key-management solution includes monitored and protected access to encryption keys.
- The only "out-of-the-box" software solution to encrypt and control access to database information at the data-item level ensuring optimal performance.
- The only solution that operates independently of, and transparently to, applications, protecting the privacy of nonpublic information against both internal and external threats.
- Designed to be fully deployable into production environments in a matter of days.
- Including data migrations tools for a uniformed and single data migration approach across different database platforms and applications.
- Secure.Data is the only third-party "out-of-the-box" data access control and privacy-enforcement product for e-businesses that operates in distributed environments across:
  - All of the major relational databases
    - I**BM DB2 UDB** - Certified by IBM for the Solution Advantage IBM Server Proven® Program and IBM Start Now Solutions Proven.
    - **IBM Informix** - Beta version.
    - **Microsoft SQL Server 2000** - Performance tested by the Microsoft® SQL Server™ Test Laboratory and Certified for Microsoft® Windows® Server 2000.
    - **Oracle Database** - Penetration tested by Oracle's European Security Practice.
    - **Sybase ASE** - Performance tested by Sybase R&D.
  - Leading Web/Application Server platforms such as:
    - **Microsoft Commerce Server** - Built for the Microsoft® Solution for Internet Business (MSIB) and passed the Microsoft® Commerce Server 2000 Integration Test.
    - **Oracle Application Server** - Certified for interoperability with Oracle9*i* Application Server Release 2.

- Leading Web- and Internet-enabled database applications such as:
  - **Bowman Internet Systems** – OEM solution in Bowman's web-based ServicePoint™ Case Management Information System for SQL Server 2000.
  - **Oracle Applications** - Built for interoperability with Oracle Applications.
  - **PeopleSoft** - Certified for interoperability with PeopleSoft Financials and HR on SQL Server 2000.
- Leading security software such as:
  - **Check Point** - OPSEC™ certified for interoperability with Check Point™ VPN-1™/Firewall-1™ user-authority for Oracle databases.
  - **nCipher** - Integrated with nCipher's FIPS 140 level 3 certified Hardware Security Module (HSM) for Oracle.
  - **Pointsec Mobile Technologies** – Endpoint security system.
  - **RSA Security** - RSA SecurID® ready for Oracle databases.

Further certifications are in the pipeline. Check with your local Protegrity representative for the latest list.

Secure.Data security solutions were implemented together with Oracle enabling organizations to achieve the following benefits:

Prevent losses and liabilities to the company and executive management

- Ensure data integrity in all the protected databases by preventing unauthorized access leading to destruction, loss or misuse of critical information assets.
- Safeguard the company public relations and the trust of its customers from damaged reputation and the cost of battling negative publicity that may occur with a disclosure of critical corporate information or consumer personal information.
- Enable protection of senior management from the risk of business liability by ensuring the safety and value of corporate and personal information accordingly to industry standards and government security and privacy requirements.

  With these key Secure.Data functions:

  - ✓ Selective encryption of data where it is most vulnerable – at rest in databases.
  - ✓ Strong Role Based Access Control (RBAC) to facilitate granular access control to sensitive data.
  - ✓ Secure and separated auditing of all access to critical data.
  - ✓ Segregation of duties that provides security control over all users in an environment – even technical administrators – to ensure that only authorized individuals see protected information.

Enable new e-business initiatives

- Bring customers together to do business with new revenue-producing applications that allow sharing, analysis and communication of information, while ensuring that the full security and protection of critical information assets always is maintained.
- Fulfill a market need. Create safe IT products and services for organizations that need IT solutions and are concerned with the confidentiality of sensitive data.
- Expand business models into networked or Web-enabled environments without the risk of disclosing critical sensitive information assets.

  With these key Secure.Data functions:

  - ✓ Role-based access controls that allow for open sharing of information with business partners, customers, and other internal/external users without the risk of disclosure of Critical Information Assets.
  - ✓ Built to work with leading web platforms such as Oracle9*i* Application Server.

- ✓ Secure.Data Manager supports stronger two-factor authentication with RSA SecurID®.
- ✓ Working in combination with Secure.Data, Check Point® UserAuthority™ allows sharing of VPN-1™ and FireWall-1™ authentication information with Secure.Data Server.
- ✓ Centralized data-security policy management to minimize costs for new business applications.
- ✓ Segregation of information access policy and administration to fulfill varying security requirements and allow for checks-and-balances in multiple client environments.

Facilitate "out-of-the-box" compliance with new privacy and security requirements

- Acquire the baseline functionality called for in various global privacy and data protection legislation requirements that require cryptographic protection of stored data such as the GBLA, HIPAA, the U.S. FDA 21 CFR 11, EU Privacy Directive/Safe Harbor, Canada's PIPEDA and other industry mandates such as VISA U.S.A. CISP.
- Satisfy internal IT audit requirements in accordance with new audit requirements and protect against both external and internal security threats.
- Effectively and timely apply required security functionality across multiple applications and database platforms without lengthy, expensive and problematic development for each environment.

With these key Secure.Data functions:

- ✓ Absolute control of access to Critical Information Assets.
- ✓ Selective encryption of data in storage, protecting information from unauthorized access.
- ✓ Allows for increased protection of encryption keys using nCipher's FIPS-140 level 3 certified HSM.
- ✓ Centralized application of privacy rules through which a single Secure.Data solution protects information access from any application or source in the enterprise.
- ✓ Self-protected and secure audit trail that tracks all activity around the most confidential data and provides trusted, intuitive information for reviews of security compliance.

Secure.Data is the most time and cost effective "out-of-the-box" solution available for the protection of valuable information that resides in relational databases. The advanced technology found in Secure.Data is required as the last line of defense against the compromise of residing sensitive data. Secure.Data can help enable and forge new applications in a world where data accessibility and portability are driven by the Internet and customers who demand flexible, real-time access to information. The Secure.Data solution is able to integrate with, and manage security and privacy on, multiple database platforms, is transparent to the applications and implements compliance in the audit processes of sensitive data.

III. Senior Management/Director Involvement

The commitment and involvement of senior management and boards of directors from the early stages of the GLBA/OCC project to its completion is critical to ensuring that all aspects of the project is carefully considered and that the project are clearly defined, supported, funded and monitored. Many financial institutions will direct their Chief Privacy Officer or other designated officer to establish new reporting mechanisms to keep senior management apprised of progress and to manage risks. These reporting mechanisms will help to keep GLBA/OCC projects on schedule and ensure that adequate resources are available. Quality assurance reviews of sensitive information, benchmarking, and internal audit proceedings also must be established to ensure risks are properly managed. As part of both planning and monitoring, financial institutions have to establish clearly defined measurement objectives and conduct periodic reviews to ensure that these goals and standards are met. The efforts of interdisciplinary teams comprised of the Chief Information Officer, Chief Privacy Officer, Chief Security Officer, experts from IT systems, affected business units, law departments, and corporate communications will help financial institutions to better manage risks, improve public relations and avoid liabilities. These teams will help to facilitate critical phases of the project and emphasize the priority of the project through the entire organization.

IV. Comprehensive IT Inventories of Information-Assets at Risk

Financial institutions or other organizations have to develop current inventories of defined sensitive information, such as nonpublic personal information stored in different types of databases or used in certain applications and networks. This enables many institutions to consolidate, eliminate, manage, or integrate technology projects on an enterprise-wide basis. Effective planning serves as a catalyst for modernizing database systems, integrating and managing sensitive information in new systems with relevant legacy systems. Comprehensive inventories of sensitive information stored in databases also foster better risk evaluation and decision-making, ensuring that IT systems are consistent with current business strategies.

The risks to physical assets are well understood, however they are not as clear when considering data assets. For example, the source and range of possible damages that could accrue to a delivery truck are well known. There is a considerable record of the prior loss. Mechanisms employed to mitigate this risk also are well known (insurance, maintenance, trained and competent drivers).

The possible sources of loss or compromise to information assets are substantially larger and the consequences far more complex. For example, information can be stolen more than once and by multiple parties. Additionally, it is often difficult to know if and when an information asset was accessed and if the access constituted a theft.

While the identity of the person who steals a truck may initially be unknown, there is generally a high probability that it will eventually be determined and the truck recovered. In the theft of an information asset, it may be difficult to establish direct evidence that a theft occurred; it is equally hard to identify the thief. Finally, while a truck can be returned and any damage repaired, what does it mean to return stolen data?

By most accounts, the problem is very serious. Recently, a well-known .com music store was forced to report the loss of 300,000 credit cards, with associated authentication information, and an attempted extortion by the thief. The result of this compromise was the public disclosure of 25,000 of these numbers by the thief with sufficient information to support fraudulent transactions.

While the full extent of the problem is not known, it is believed that significant break-ins occur daily. Several organizations that practice the art of hacking routinely claim that they can penetrate any commercial system and obtain valuable information assets.

On a weekly basis we are now hearing about compromises where proprietary corporate data is extracted through the organizations' web connections. In the case of the .com music store there was apparently significant loss both direct and consequential. The merchant stands to lose the value of completed transactions because the cards posted on the Internet contained sufficient information to authenticate cardholder identity, thus meeting card association requirements. The credit card issuing banks must deal with the legal documentation required to absolve each legitimate cardholder of EVERY fraudulent transaction committed against their card. This is on top of having to reissue 300,000 new cards. Each new card will estimate a cost of US$3-12. Perhaps the least effected on an individual basis is the cardholder. Nonetheless, they must deal with the paperwork generated by the issuing bank for each transaction and wait for the replacement of the card. They may also suffer by the disclosure of tampered nonpublic information where the consequences are difficult to calculate.

The .com music store mentioned above may suffer the most even though it experienced none of the financial loss of the merchants or the administrative loses associated with cleaning up the fraudulent transactions or issuing new cards. The e-store nevertheless has lost its MOST VALUABLE asset: its client's trust; and it is the CEO who bears the ultimate responsibility for this loss. Some percentage of his clients WILL do their shopping elsewhere. One aspect of the Internet is that, to a large extent, all merchants within a class of business are virtually indistinguishable. The lack of distinguishing attributes forces extreme pressure on price and service (note the extensive use of free shipping). Ultimately this makes it easy for the consumer, with the click of his mouse, to choose a new merchant, perhaps one that realizes a valuable distinguishing attribute might in fact be security. Digital loyalty —-a recently coined term — suggests e-merchant's awareness regarding consumer trends and loyalty. Merchants using

the Internet to reach their customer-base now are beginning to realize that the privacy and integrity of information entrusted to them is a number one priority.

By visualizing the outcomes of loss of or damage to information-assets as well as the legal and public relations consequences, you can determine the financial value of these assets. This dollar value in turn dictates the specific investment that is necessary to protect the privacy and integrity of your customer and consumer nonpublic personal information.

V. Key Concepts in Secure.Data for Oracle

There are a number of key concepts that are essential to understanding the design and implementation of Secure.Data using the Oracle databases. This section will briefly outline each one of these concepts.

Security Policy Management

Policy management in Secure.Data refers to the creation and application of "the policy", a collection of security and privacy rules that can be used to enforce data protection, and audit right down to the column level in targeted databases. Secure.Data is built on existing standards for policy management:

Role Based Access Control (RBAC) – The role-based model of access control is the foundation of Secure.Data 's policy design. Using the RBAC methodology, Secure.Data is able to bring granular user access to the field/column level within protected databases. Roles are created that allow you to define each user's unique data-access privileges. These roles are then used to apply defined security controls to requests executed by a particular database user or a group of database users. Individualized roles can be assigned to specific users or more generic role-types can be created to accommodate larger functional groups of users.
Note: Secure.Data's RBAC is designed to supplement, but not replace; existing RDBMS access controls of sensitive information.

Access Control Definition Facility (ADF) – ADF is a complete RBAC facility that enables the security administrator to create and maintain users' functional and organizational roles and their associated access privileges. To make the relationships between roles and information in the RDBMS both flexible and easy to use, the notion of the role is mapped into the columns of an RDBMS through an additional layer of abstraction. In Secure.Data, the ADF is called the Secure.Data Manager™.

Access Control Enforcement Facility (AEF) – AEF is central to the architecture of Secure.Data. An effective AEF is tightly coupled to the RDBMS engine used by the application and in general, it must receive security policies (and updates) via secure transmission from ADF. In Secure.Data, the AEF, Secure.Data Server™, controls real-time access to all protected elements of the database at the appropriate level of granularity. Discretionary Access Controls (DAC) provide a role-based means of restricting access to objects based on the identity of subjects/users and the roles to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. The Discretionary Access privilege granted to objects is based on the identity of a USER--an active entity, generally in the form of a person that causes information to flow among objects or changes the system state. The least privilege principle requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control (MAC) – MAC provides a workgroup-based means of restricting access to objects/rows based on the sensitivity (as represented by a label) of the information contained in the objects. MAC also requires formal authorization (i.e. clearance) of subjects to access information of such sensitivity.

Granular Data Protection

Granular Data Protection, also referred to as "Selective Database Encryption", allows users such as Security Administrators of Secure.Data, to target and automatically encrypt only the data that needs to be protected and audited. With Secure.Data, columns of data can be protected without protecting the entire table or database that contains this data. This approach allows Secure.Data to minimize the overhead associated with using encryption to protect information. Encryption/decryption operations are only performed when columns of a protected table are included in database queries.

Granular Data Protection refers to the unique ability of Secure.Data to encrypt different physical columns of data with different encryption keys. With multiple keys in place, intruders are in many cases prevented from gaining full access to any database since a different key protects each column of encrypted data. In Secure.Data, columns are encrypted by database extension functions that convert plain text objects into cipher text objects. For all queries meeting the access-control criteria, Secure.Data provides transparent and automatic crypto services on the fly, supplying plain text to the authorized user only. Data being accessed remains encrypted in the source database.

The granular data protection provided by Secure.Data is portable. The encryption rules for a particular type of sensitive data can be bound to one or more physical columns of data in a database. As security and privacy requirements evolve and business requirements change, these rules can easily be applied to new columns of data with minimal effort. This flexibility can help organizations respond quickly to ever-changing requirements for data protection.

Internal Threat Protection

Internal Threat Protection (ITP) refers to a set of features as well as a general philosophy of Secure.Data: All parties not specifically granted access to data protected by Secure.Data must be prevented from accessing that data in any possible way. This philosophy is carried out using a combination of security best practices, sophisticated self-protection mechanisms, and the ITP functionality itself.

ITP is a functionality that provides additional protection from potential internal threats. Items protected by Secure.Data can be given an added layer of security from unauthorized database administrator access (unauthorized access could be from either an external hacker who has gained database administrator access to the protected database, or from an internal database administrator who is not permitted to access data through the Secure.Data policy). This added layer of security is accomplished through the use of intelligent integrity checks performed on protected data, user passwords, and key database objects.

Dual Control Duties

The Dual Control Duties (DCD) feature provided by Secure.Data automatically implements the security industry best practice of "Separation of Duties" also called "Segregation of Duties". The notion of separation of duties has been around for a long time and is often associated with the security policies of financial institutions such as banks. For example, when responsibilities of database content is decided within an organization, the security administrator may be assigned responsibility for sensitive information and the database administrator could administer all other information.

In Secure.Data, DCD can be defined as the intentional division of responsibility between the custodian of data (i.e. the database administrator) and the security administrator who creates and maintains security policies for sensitive data (i.e. Privacy Officer). The DCD function helps to ensure the security and confidentiality of data is guided and managed by senior management and implemented by Secure.Data. In Secure.Data the DCD feature is not optional. Access control, encryption, key management, audit and other self-protection mechanisms are features to enforce it.

The database administrator's role and responsibilities, for example, is defined to allow him/her to do the usual database administrative functions without being able to access and "see" (decrypt) sensitive data within a Secure.Data protected database. Likewise, the database administrator could administer role and workgroup access privileges, add and delete users, etc., yet not have the capability to view or modify sensitive data. Secure.Data is the only solution which enables significantly improved internal physical security, even if the disk or system is misappropriated, the information is unreadable to even privileged users.

The concept of DCD also maps particularly well to some of the new legislative and corporate requirements in the area of data security. For example, the GBLA specifies “Segregation of duties for managing access to Customer/Consumer information”.

Data Migration in the database

In the context of Secure.Data, data migration refers to the process by which clear-text data is transformed into cipher-text. The data migration services provided by Secure.Data allow existing databases to be secured with minimal administrative effort. Application-based toolkits do not provide these services and require manual script generation and superior database knowledge to perform the same data migration abilities provided out of the box with Secure.Data.

The Secure.Data SQLDirector™ subsystem provided with Secure.Data produces DDL (Data Definition Language) scripts that facilitate data migration. Using these scripts, data in protected tables is backed up and the affected columns are converted to a data type that supports encryption. The data is then converted to cipher text using the specified encryption rules and put back into the changed tables.

VI. Secure.Data Design Principles

Secure.Data is a database security solution substantiated by over 10 years of extensive research and development. From its inception, the product has been developed under a distinct set of guiding design principles. This section gives you a brief outline of these principles.

Use of Cryptographic Standards and Best Practices

Security and Privacy is paramount in the development of all Secure.Data products. Security best practices and, more importantly, cryptographic including audit best practices, overshadow all of the other principles considered in this section.

Key lengths and algorithms - Secure.Data employs 56-bit DES and 168-bit Triple DES and Diffie-Hellman key-exchange technology.

Within Secure.Data Manager and Secure.Data Server, Diffie-Hellman key-agreement implementation process operates as follows: Both sides calculate the common D-H key which is thereafter used to 3DES-encrypt messages. The 3DES keys are stored on Secure.Data Server and Secure.Data Manager.

Key Management - Secure.Data ’s strength versus other solutions lies in the sophisticated and automatic key management system used to protect all keys from potential exposure. Follows is a brief explanation of some of the components of the key management system utilized by Secure.Data.

Automatic Key Management in Secure.Data Manager and Secure.Data Server

Master keys are generated, split into several parts and backed up. Separate keys are used for policy data encryption and application data encryption. The keys are encrypted, stored in a database and backed up. All communication, external and internal, is encrypted by the use of Diffie-Hellman protocol to negotiate encryption keys. Unique encryption keys are used for each pair of Secure.Data Manager and Secure.Data Server.

Optional Hardware Encryption

Combining nCipher technology with Secure.Data for Oracle8*i* has enabled Protegrity and nCipher to offer an "out-of-the box" application transparent database access control solution with nCipher's FIPS 140 level 3 certified nShield™ Hardware Security Module, to deliver enhanced key management capabilities. For organizations that need to protect sensitive information, Secure.Data brings together the most advanced "out-of-the-box" automated database access control solution with a combined hardware and software key management architecture not found in any other product.

Benefits of the optional nCipher HSM Integration

- ✓ Management of the Secure.Data master key inside the nShield HSM, delivering a significant improvement in the manageability and scalability of the software key hierarchy.
- ✓ Secure backup and recovery of the master key using nCipher smart card based key management.
- ✓ Protection of the master key by FIPS 140 Level 3 cryptographic hardware, allowing for the secure generation, storage, disposal, archival and recovery of the master key.
- ✓ Protection against off-line attacks employing a stolen master key and a copy of the database.
- ✓ Transparent failover support with multiple HSMs to support redundancy, including backup site configurations for disaster recovery.

Performance

If the number one design principle for Secure.Data is "make it secure", then number two automatically would be "make it fast". Encryption and decryption by nature is a resource intensive operation that requires careful design considerations and expertise when balancing high-level security with optimal performance. The delivery of Secure.Data encryption is optimized and secure, to produce the fastest high-level security solution available for the protection of sensitive data stored in relational databases.

The performance design philosophy can also be seen in our implementation of granular data protection. With granular data protection, only the items that require explicit protection are processed by the Secure.Data cryptographic services. This conserves a tremendous amount of precious database and machine-level resources.

Application Transparency

Functionality of applications that access data protected and audited by Secure.Data is not impeded and does not require any modification. This philosophy is the foundation for much of the functionality and behavior found in the Secure.Data solution. Application transparency is a key issue for most organizations, particularly organizations that have large sums of money invested in application code that accesses databases now warranting protection. It is prohibitively expensive and far too time-consuming for these organizations to re-write applications using tool-kits in order to enable data protection services.

Secure.Data for Oracle accomplishes application transparency by providing a *view* that corresponds with the original physical table being protected. Without any changes to the application or any knowledge from the end-user, all queries to the original table are now being handled by the Secure.Data controlled view. All access to the underlying (encrypted) data is handled by this implemented view.

In a database environment protected by the Secure.Data encryption services, direct or indirect access to a view with an attached security policy causes the data-server always to consult the policy function for verification. The policy function returns only authorized data, dynamically modifying the external user's data access. Fine-grained access control such as this is transparent to both external users and applications; it allows an organization to have different access conditions per external user, per group of external users, and it offers flexible policy implementation, to allow customers to fine-tune their security policies based on their specific needs.

Consistency Across Heterogeneous Environments

Secure.Data for Oracle is one solution in a suite of products that bears the Secure.Data name. The Secure.Data platform currently supports Oracle, IBM DB2 UDB, IBM Informix, Microsoft SQL Server, and Sybase ASE databases. Each of these products is designed to look, feel, and behave in a similar manner. The skills and knowledge required to operate Secure.Data in one environment translate directly into the other environments that we support.

Secure.Data products are designed to provide a homogeneous policy management on different database platforms, and maximum data protection with audit compatibility across the environments that Secure.Data support. Additionally, interfaces, methodologies and functionality are kept similar wherever possible.

VII. Secure.Data Components Overview

A Secure.Data solution installation (Figure 2) consists of four main components. The Server and Manager components can be used in different combinations depending on the size and architecture of the targeted organization. Each of these components will be briefly outlined in this section and described in more detail in this document.

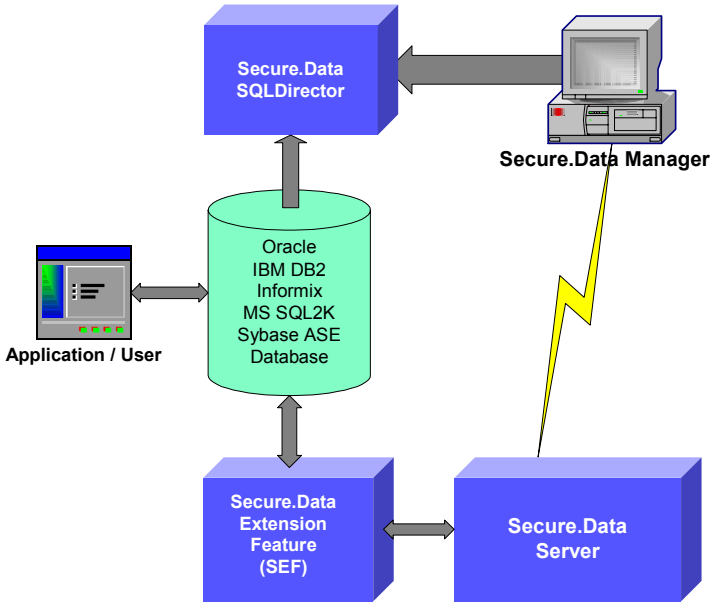

Figure 2: Secure.Data Components Overview

Secure.Data Manager

Secure.Data Manager is the central point of control for security administration and security management of an organization's security policies and procedures regarding sensitive information residing in databases. This component of the Secure.Data product suite is where the security administrator/officer defines external user settings; assigns external and internal user roles, user relations to workgroups and data-access privileges; specifies the data to be encrypted and audited; and selects algorithms, encryption keys and other security parameters. Once defined in Secure.Data Manager, the security policy or updates to the policy are communicated in a secure way to the Secure.Data Server environment for enforcement and execution at the database level. All activities and transactions within the Secure.Data Manager are automatically logged and stored in an encrypted form, ready for audit review.

Secure.Data Server

Secure.Data Server is the active component of the Secure.Data suite of security software and performs real-time security processing for targeted sensitive information residing in the database. Secure.Data Server plugs into the database as a security middleware component. As the run-time portion of the security system, Secure.Data Server enforces and executes the security procedures and policies that have been defined in and pushed from the Secure.Data Manager. All activities and transactions within Secure.Data Server are automatically logged and stored in an encrypted form, ready for audit review.

Optional nShield Hardware Security Module

nCipher's nShield hardware security platform provides transaction acceleration and secure key management and storage capabilities for a broad range of security sensitive applications. nShield meets the Federal Information Processing Standard (FIPS) 140-1 Level 3 for key security and tamper-resistant physical hardening. FIPS 140 is the industry benchmark for companies that need to secure sensitive data, and is recognized not only by regulatory agencies across the world, including the US and Canadian Governments and the European Union, but also by industry initiatives such as Visa's CISP and 3-D Secure specifications.

Secure.Data Extension Feature

The Secure.Data Extension Feature (SEF) provides cryptographic and authorization services to the targeted and protected database. The SEF is tightly coupled with the database and is largely dependent on the database architecture in its design. In the case of Oracle the SEF is implemented as an external program, a database view and its triggers, normally on the same machine.

SQLDirector

The SQLDirector is a subsystem that provides scripting support to aid in the implementation phase of Secure.Data policy rules into the targeted database environment. Scripts generated by the SQLDirector allow for the creation and maintenance of cryptographic support and general policy implementation within the database.

This utility supports the notion of dual control or separation of duties by enforcing the partitioning of policy creation/enforcement and the application of policy against the actual database. Scripts from this utility are saved to disk, reviewed by the database administrator, and then executed against the protected database.

VIII. The System in Operation

The following operational diagram outlines how the Secure.Data solution operates in a two-database scenario: The generic login and SELECT (read) query are depicted in the diagram below (Figure 3). This example depicts a user logging into the database to extract information with a custom report generation application that includes strong authentication by hardware token.

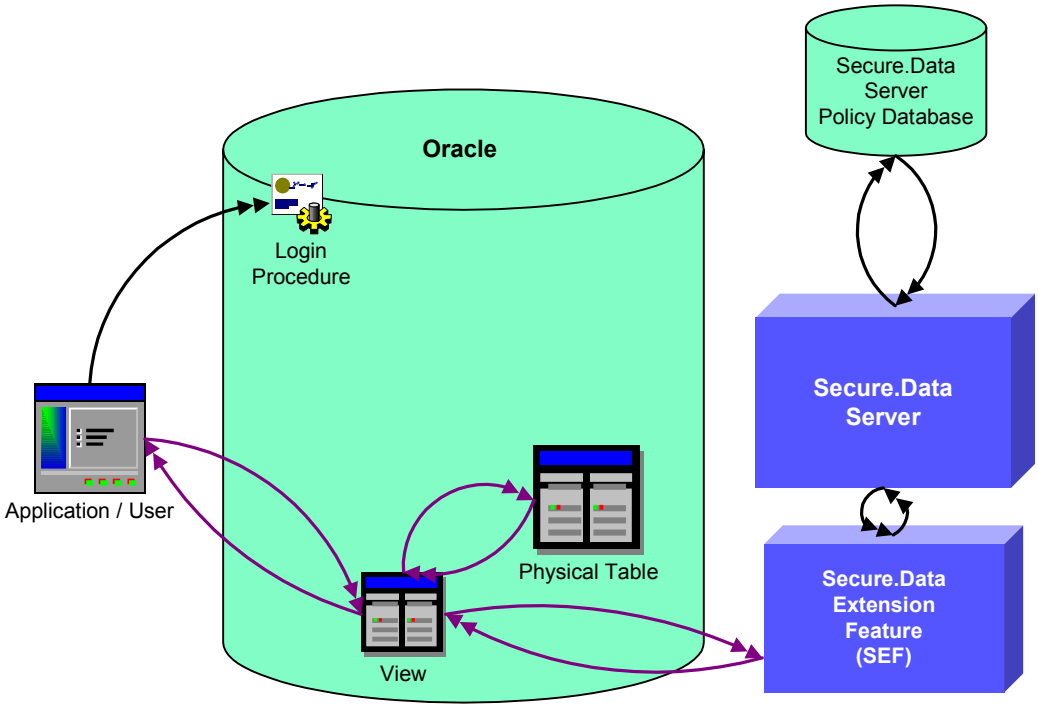

Figure 3: The System in Operation

The external user authenticates to the application. The application makes a connection to the database and logs in the external user. The external user executes a SELECT (or read) query against the database. Without application or user knowledge, Secure.Data has created a view to protect information in the base table with the same name as the original physical table. The user's query hits this View. Oracle then sends the SELECT query to the SEF. The Secure.Data Security Extension supplies the user information to the Secure.Data Server that queries the policy for information relevant to this external user. Assuming that the external user has the appropriate rights to read the requested information, the data is decrypted and returned from the SEF to the view. The result set is returned to the external user (application).

IX. Secure.Data Components in Detail

Secure.Data Manager

The Secure.Data Manager is the central point of control for the administration and management of the security policies and procedures. It provides a graphical user interface that can be run on any Windows workstation. Through the Secure.Data Manager, the Security Officer can define user settings, roles, privileges, sensitive data, encryption algorithms, audit selection, keys, and other security parameters. The Secure.Data Manager also provides a mechanism for importing objects and user records.

A single Secure.Data Manager can control the security policy for all company database management systems. Alternatively, a hierarchy of Secure.Data Managers can be set up for each level of the security administration hierarchy. The Secure.Data Manager stores the defined security policy in an encrypted policy database. This policy information can be "pushed" to any or all of the Secure.Data Servers that are configured in the enterprise via a 3DES encrypted network connection.

The extensive audit procedures (referred to as SafeAudit™) in Secure.Data are configured and viewed in the Secure.Data Manager. All information relevant to the protection and use of secured data can be monitored from the Manager. Changes to the policies that enforce data protection as well as the queries against protected data can be tracked at a granular level. Audit logs are always stored in encrypted format and are monitored for evidence of tampering. Real-time audits of all security policies and privileges ensure non-repudiation of all transactions involving sensitive information and enable an organization to enforce audit policies enterprise-wide. While other systems produce logs of all system activities, SafeAudit focuses on the most useful information for security managers - activity around protected sensitive information.

The Secure.Data Manager also produces reports from audited information. Using the Report Directory in the Manager, security administrators can view, print, and export reports into different formats. The underlying report generation engine in Secure.Data is Seagate Crystal Reports™ (version 7).

Secure.Data Manager provides single factor authentication with enforced minimum passwords and alpha-numeric restrictions. The Secure.Data Manager also supports stronger two-factor authentication with RSA SecurID®.

The Secure.Data Manager initialization process provides system self-protection in the form of integrity checks against its policy database. This integrity check automatically provides an additional layer of security for the solution by detecting any kind of tampering with the policy database content. The Secure.Data Server executes similar checks on startup.

The Internal Threat Protection (ITP) feature further enhances the overall security of the Secure.Data system. ITP, configured from both the Secure.Data Manager and the Server, is a collection of functionality designed to prevent unauthorized access to protected data by a database administrator. ITP is enforced with a series of extra controls placed on views, triggers, users, etc. These controls can be recalculated and checked at a predefined interval. If tampering is detected including unauthorized changes to user passwords, the system will either go into lock out mode or generate log alerts depending on the configuration.

Secure.Data Server

Secure.Data Server enforces and executes the security procedures and policies that have been defined in Secure.Data Manager. It is the run-time component of the Secure.Data solution that plugs into the implemented database via the Secure.Data Extension Feature (SEF). Each Secure.Data Server maintains its own encrypted database containing relevant policy information. The policy created in the Secure.Data Manager, is distributed to Secure.Data Servers via a 3DES encrypted TCP/IP connection.

Security administrators typically administer Secure.Data Servers with database administrators handling the database specific requirements. It is important to point out that the responsibility of control and administration of protected data can only be executed from the Secure.Data Manager (usually by a security administrator/officer). This enforced Dual Control Duties (DCD) ensures the highest possible level of data security including key management control as well as protection against the execution of DDL (Data Definition Language) queries against the database by the security administrator/officer.

The Secure.Data Server and the Secure.Data Manager maintain separate policy databases. In the case of the Manager, the policy database may be located on any ODBC compliant RDBMS server including the server hosting the database that is to be protected by Secure.Data. The Secure.Data Server's policy database must be located on the database server to be protected. The minimum recommended size for both of these databases is 10 MB. All data stored in any Secure.Data policy stores is encrypted and can only be decrypted by Protegrity Global Services (this includes auditing information).

The Secure.Data Server has an initialization process that is similar to the one in the Secure.Data Manager. This initialization process provides a series of integrity checks on the policy database as well as on all Secure.Data components (internal and external to the database). If any of these checks fail for any reason, the server will safeguard protected data by locking itself until the problem has been isolated and fixed.

Secure.Data Server is comprised of two services (Windows platforms) or Daemons (Unix platforms. See Figure 4):

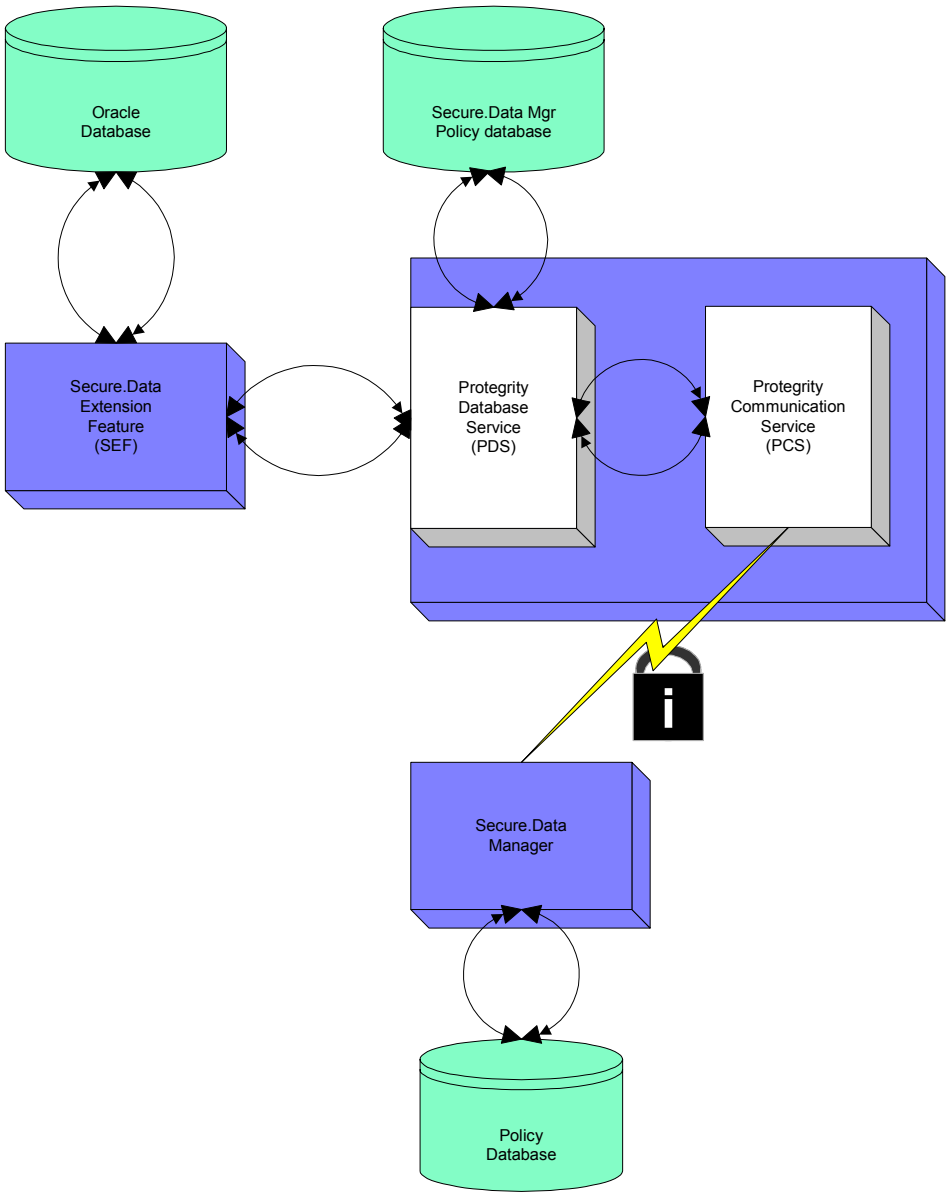

Figure 4: Secure.Data Server is comprised of two services or Daemons

The Protegrity Communication Service (PCS) – As the name implies, this service provides all communications between the Manager and the Server. The TCP/IP protocol is used and data is encrypted using 3DES before transmission. This service remains idle unless a communications session is initiated from the Secure.Data Manager.

For the sake of performance, Secure.Data employs a symmetrical keying implementation to provide encryption services. Symmetrical keying requires the maintenance and exchange of private (secret) keys.

The PCS uses a Public Key Distribution System called Diffie–Hellman when exchanging any private keys. The Diffie-Hellman implementation in Secure.Data is based on SSLeay by Eric A. Young.

In Secure.Data, the Manager and Server each create one public and one private key, and then send the public key of this key pair to each other. Encryption keys are created from the receiver's public key and the sender's private key and are used to ensure the security of all information exchanged between the Server and the Manager.

Protegrity Database Service (PDS) – The PDS is the central component of the Secure.Data system. It provides any requested policy or audit information from the Server database to either the Secure.Data Extension Feature (SEF) or the Secure.Data Manager. Internal Threat Protection (ITP) is also enabled and enforced by the PDS.

As seen in the System in Operation section, the Secure.Data Extension Facility requests an external user's policy information when the external user establishes a connection to the protected database. It is the PDS that services this request. The PDS will provide all policy information (access times, rights to individual objects, etc.) to the SEF, which builds a "user area" in memory with this information. This cached user area is queried when subsequent requests to the database are initiated by this user.

The PDS executes the real-time audit mechanisms provided by SafeAudit. The information requested for audit is obtained, monitored, and stored by this service. When requested by a security administrator, audit information is passed to the communication service for transmission to the Secure.Data Manager.

All of the Secure.Data services can be started automatically if a token file is made available to the system. A token file consists of a database username and password for the Secure.Data Server database and a crypto services username and password (all are in encrypted format).

Secure.Data Extension Feature

The Secure.Data Extension Feature (SEF) is the component that is the most database dependent. It is beholden to the architectural design and available functionality provided by the RDBMS environment to perform its duties. In Oracle, the SEF is actually implemented as VIEW's and TRIGGER's using the Data Cartridge facility of Oracle. Throughout the Secure.Data product line, this component is often referred to as the database "plug-in" or "snap-in". The SEF is the critical component in the Secure.Data system that provides the mechanism to extend the existing database security controls with the extra layer of protection found in Secure.Data.

Secure.Data Server resides in each Oracle environment and performs all real-time processing for the selected and protected information. Secure.Data Server plugs into the database as a data security middleware component and as the run-time portion of the security system. Secure.Data Server enforces the security and privacy procedures and policies that have been defined in Secure.Data Manager. Application users are authenticated and all access to protected data is authorized through the Secure.Data Server utilizing the encrypted security policy stored within the database server environment.

When an external user attempts to access protected data, Secure.Data Server will verify the authority in the security policy before granting the client access to the data. If the data is encrypted the Secure.Data Server will decrypt the data before providing it to the client application. Correspondingly, if the client has access to change or add encrypted data, Secure.Data Server will encrypt the data before storing it in the physical database table.

The Secure.Data implementation uses two distinct features of the Oracle relational database engine: the ability to execute functions, written in C, that exist in a shared library; and the trigger functionality. SEF is implemented as a Data Cartridge (for more information on Data Cartridge see the Oracle manuals). The TRIGGER's and VIEW's call these functions, which in turn contain calls to the Secure.Data Server.

The SEF is database specific and provides a different technical solution for each of the databases that are supported by Secure.Data. Although these solutions vary greatly in terms of technical design aspects, every effort has been made to ensure consistency across database platforms.

The SEF can be viewed as the data processing workhorse of the Secure.Data system. All application data related operations such as encryption, decryption and type conversion are performed by this component. In a run-time scenario, the SEF is called upon to process any queries against protected information in the database. The bulk of these operations are centered on verifying that the user executing the query has the proper permissions to perform the operation that they are trying to perform (i.e. Select, Insert, Update, Delete). If the executing user has the proper credentials the SEF will provide the necessary encryption or decryption functionality. In some cases, the SEF can also provide query optimization by rewriting parts of queries that search on protected data.

The cryptographic services provided by the SEF use industry standard DES and 3DES algorithms to protect data. AES (Advanced Encryption Standard) and other algorithms will be available in future releases. The SEF also participates in Secure.Data 's strong key management system. Application data keys used by the SEF are generated within this key management system and are destroyed immediately after use for maximum security.

SQLDirector

The Secure.Data SQLDirector subsystem is provided to help both the security administrator and the database administrator to implement Secure.Data security policies within targeted databases. SQLDirector has a graphical user interface and is currently invoked from within the Secure.Data Manager. Access to this utility requires administrative access to the Secure.Data Manager.

In order for Secure.Data to provide transparent encryption and decryption services, some modifications to the protected tables are required. The original table is renamed and its content is protected by access control and encryption. Original clear-text values will be converted to cipher text. In this process, a View is created that will provide access to qualified external users to the data protected by Secure.Data.

By accessing both the Secure.Data policy database and the targeted database dictionary, the SQLDirector can generate DDL (SQL) scripts that implement data item protection against specific columns within the database. SQLDirector supplies all of the DDL scripts necessary to create data protection controls as well as migrate existing data into encrypted format. SQLDirector uses ODBC to make the connection to both the target and the Secure.Data policy databases.

Scripts generated by the SQLDirector include provisions for backing up the tables (and data) selected for protection. In the event of a script failure, original tables can be restored from these backups. The SQLDirector utility can also be used to generate restore scripts for protected tables. These restore scripts will enable the ability to completely "back-out" Secure.Data protection from the specified table(s). The restore process includes the migration of protected data back to its original form and data type.

X. Strong Internal Security and Privacy Controls

All institutions or organizations must focus attention on protecting critical information such as nonpublic personal information defined by the new requirements and the company core business values. Establishing better safeguards to detect fraudulent, malicious, and negligent acts from both internal and external sources lead to true and absolute access control to sensitive information. Control points include satisfactory internal audits that cover facilities, personnel, policies and procedures, access control, level of information protection, separation of duties, granularity of audit logs separated from ordinary log files, managing encryption keys, databases, telecommunications, system software and application software. Important precautions to protect information security and privacy included instituting enhanced security access restrictions, background checks on employees and

contractors, enforcing appropriate separation of duties between security officers and database administrators, and generating effective audit trails on defined sensitive information only. Financial institutions should also develop contact lists to get advice on how best to respond and escalate to intrusions/attacks and to instantly alert others about intrusions/attacks on sensitive information stored different database systems.

A financial institution internal auditor provides a very important control mechanism for detecting deficiencies and managing risks in the implementation of the GLBA and other privacy requirements. Many institutions have not treated information technology audits as critical and do not focus adequate attention on assessing the audits. Internal auditors should be involved early in the implementation of any solution for compliance, participate in the contingency planning process, and independently validate tests and contingency plans. Together with the Chief Privacy Officer, they should also review the defined sensitive information for protection as well as the access authorization and escalation plans.

XI. How to achieve enhanced true and absolute access controls to defined stored information:

Once an intrusion is detected, effective response begins with planning damage assessment and recovery activities. Time is money, and management must quickly determine which system and database have been affected and whether any data have been altered or copied. By pinpointing exactly which computer system or databases have been compromised, management can prioritize the sequence of recovery efforts in a manner that may require immobilization of the entire network or databases. In general, to minimize the time spent in response to an intrusion, management should prioritize the sequence of actions from containment and elimination through system or database restoration and, finally, to corrective actions. By having the priorities stated, the board should review, approve, and monitor Internet banking technology projects that may have a significant impact on financial institutions risk profile. Security measures and controls should include management controls that provide effective segregation of duties and restrictions on accessing data.

- Centralized management to remove unauthorized users from all Protegrity-secured databases (reduces risk of exposure or breaches to security).
- Monitor specific users who have temporary authorization to access sensitive information.
- Detect unauthorized access attempts across different databases.
- Provides a secure way to identify particular job functions and safely delegate those functions to a security administrator. This allows security administrators to properly assess and manage the security of a database without risking the damage that could be caused by more powerful database administrator utilities.
- Avoid random access by disclosure of root-access codes.
- Define who should have access to all company information and include an accountability policy.
- Management should decide individual responsibility over the encryption keys.
- Management should define access rules to back-up files.

XII. How to achieve separate, unified, and intelligent auditing

All database auditing is an essential requirement for all security and privacy implementation especially when it comes to the new legal and security requirements like the GBLA and VISA U.S.A. CISP. Companies should define their auditing strategy based on their knowledge of the application or database activity around sensitive data, an effort that would protect their own employees from being wrongfully suspected in any internal breach situation. Auditing does not have to be an "all or nothing" exercise, it has to be selective. Intelligent auditing saves time and reduces performance concerns by focusing on sensitive data only. By intelligently protecting data through encryption and limiting the accumulation of audit logs to only the sensitive information, more critical security events are highlighted and reviewed.

The Protegrity Secure.Data solution for database security ensures that the proper focus is placed on protecting the information granularly stored in Oracle, IBM DB2 UDB, IBM Informix, Microsoft SQL Server, or Sybase ASE databases and provides a unified and protected audit log. In particular, the reality in many cases is that auditing capabilities of databases are often ignored due to application performance enhancement, unmanageable database logs, the requirements of saved disk space or other time-consuming efforts. However, inadequate auditing reduces proper accountability and increases damaging escalation of breaches and forensic analysis to estimate the restoration consequences and costs. Effective audit trails are crucial to immediately understanding actions taken against certain sets of sensitive data. Logging events directly associated with the defined data in the database is essential to monitoring access and activities. Other benefits are:

- Targeted and independent monitoring and auditing capability of selected and protected information.
- Ability to have a separate (dual control), unified audit log from all Protegrity-secured databases monitoring all transactions — read, insert, update and delete — to protected information.
- Logs track only the activity around protected data, providing management with a clear and concise review and control of the protection of confidential information. Decreases prep-time during privacy and security auditing.
- Allows enhanced separation of audit trails where all console and server transactions are monitored.
- The ability to manage multiple databases centrally enables the auditing capability. Centralizing the auditing process allows the security group to identify and evaluate security events across databases. This provides an enterprise-wide snapshot of database events and protects the audit logs in a secured repository.

VISA U.S.A. CISP Audit requirements

Audit is a resource with extensive experience in identifying risks and evaluating the adequacy of controls to mitigate the exposures rising from the risks. In the Visa security program it is stated that: at the highest level, Members, Member agents, and merchants should communicate and periodically reinforce ethical and control imperatives with their management and staff. Account and Transaction Information is an asset that requires a system of control. Account and Transaction Information is frequently stored on databases that can be accessed from the Internet by consumers. Prudent control over an organization's Account and Transaction Information assets is good business practice. Access to sensitive transaction data and parameters stored both locally or centrally should be controlled and limited to authorized personnel only. Developing, maintaining, monitoring, and supporting an Account and Transaction security program requires participation by multiple disciplines in the organization as defined in the VISA U.S.A. CISP requirements.

XIII. Technical Considerations

Platform Support

Secure.Data Server

Secure.Data for Oracle supports Oracle 8*i* and 9*i*.

The Secure.Data for Oracle product line supports the following operating systems:

	Oracle9*i*	Oracle8*i*	Oracle8*i* w/ nCipher
▪ Sun Solaris 2.6, 2.7 & 2.8	x	x	x
▪ HP-UX 11.0		x	
▪ IBM AIX 4.3	x	x	
▪ Microsoft Windows 2000	x	x	
▪ Microsoft Windows NT4 Server		x	
▪ Linux (Future Implementation)			

Secure.Data Manager

- Microsoft Windows 2000
- Microsoft Windows NT 4.0

System Requirements

Secure.Data Server

Minimum free disk space: 15mb
Minimum free memory: 20mb

Notes

1. The amount of disk space required is directly proportional to the type of installation, and the amount of data that requires protection. Clean environments that have no existing data to migrate (to encrypted format) require less disk space than environments that have existing data because Secure.Data will create a backup copy of any existing data in tables to be protected. Another consideration with respect to disk space is that column widths for protected data will include overhead for encryption padding. This affects ongoing operations as well as the migration of data. The actual amount of overhead for a particular column is available from the Secure.Data Manager in order to account for the proper disk space allocations and maintenance.
2. The amount of memory required to operate Secure.Data Server runtime is directly related to the number of users that are actively connected to the database and are defined in the Secure.Data policy.

Secure.Data Manager

Minimum free disk space: 20mb
Minimum system memory: 32mb

Notes

1. Depending on the options installed, disk space usage ranges from 20 mb up to 130mb.
2. The Secure.Data Manager requires Microsoft Internet Explorer 3.02 or higher for online help.

XIV. References

Privacy Legislation Requirements

United States

The U.S. Gramm-Leach-Bliley Act (GLBA) (TITLE V--Consumer Privacy), regulated by the SEC, FTC, FDIC, OCC, OTS, FRB, NAIC, and NCUA, which covers a broad range of financial services and virtually affects any company who accepts credit cards - compliance July 1st, 2001 www.complianceheadquarters.com/Privacy/Privacy_Research/privacy_research.html

The U.S. Health Information Portability and Accountability Act (HIPAA) - compliance by April 2003 www.hipaacomply.com

The U.S. Food and Drug Administration: Title 21 Code of Federal Regulations (21 CFR Part 11) - Electronic Records; Electronic Signatures – compliance by August 20, 1997 www.21cfrpart11.com and www.fda.gov/ora/compliance_ref/part11/

European Union

The European Union 95/46/EC Directive on Data Privacy - compliance October 1998 - and individual EU member state privacy legislation - various compliance dates http://europa.eu.int/comm/internal_market/en/dataprot/

EU/US Safe Harbor - compliance 11/1/2000 www.export.gov/safeharbor and http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm The following privacy laws are examples of individual EU member state privacy legislations. For a complete list of the EU member state privacy legislations see http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

Germany's Federal Data Protection Act (Der Bundesbeauftragte für den Datenschutz) - compliance May 23, 2001 www.bfd.bund.de

Sweden's Personal Data Act (Personuppgiftslagen - PuL) - compliance October 1, 2001 www.datainspektionen.se

UK's Data Protection Act - Compliance March 1, 2000 www.dataprotection.gov.uk

Canada

Canada's Personal Information Protection and Electronic Document Act (PIPEDA) Compliance 1/1/2001 to 1/1/2004 www.privcom.gc.ca

Australia

Australia's Privacy Act – Compliance by December 21, 2001 www.privacy.gov.au

For other countries – see www.protegrity.com/Security_Links.html

Security Standards and Best Practices Guides

The American Express Merchant Services Data Security Standards
http://home5.americanexpress.com/merchant/resources/fraudprevention/datasecurity.asp

The BITS (the technology group for the Financial Services Roundtable) Voluntary Guidelines for Aggregation Services
www.bitsinfo.org/FinalAggregationBook051601.pdf

The ISO 17799:2000 Service & Software Directory - Code of practice for information security management
www.iso17799software.com

The MasterCard Site Data Protection Service
https://sdp.mastercardintl.com/

The U.S. Software and Information Industry Association (SIIA) - An Electronic Citadel **-** A Method for Securing Credit Card and Private Consumer Data in E-Business Sites www.siia.net/sharedcontent/divisions/ebus/citadel.pdf

The VISA U.S.A. Cardholder Information Security Program (CISP) – Compliance May 1, 2001
http://usa.visa.com/business/merchants/cisp_index.html

The Visa E.U. Account Information Security Programme (AIS)
www.visaeu.com/for_business/e-commerce_security/ais_programme.html

The Visa International Account Information Security Programme (AIS)
www.visa.com/_gds_mod/fb/merchants/gds/main.html

The Visa International 3-D Secure Authenticated Payment Program
http://international.visa.com/fb/paytech/secure/main.jsp

Other References

CSI/FBI Computer Crime and Security Survey www.gocsi.com/press/20020407.html

Protegrity Privacy and Security Link Library www.protegrity.com/Security_Links.html

Protegrity Strategic Alliance Partner: Oracle www.protegrity.com/oracle

Protegrity Strategic Alliance Partner: Check Point www.protegrity.com/checkpoint

Protegrity Strategic Alliance Partner: nCipher www.protegrity.com/ncipher

Protegrity Strategic Alliance Partner: RSA www.protegrity.com/rsa

###