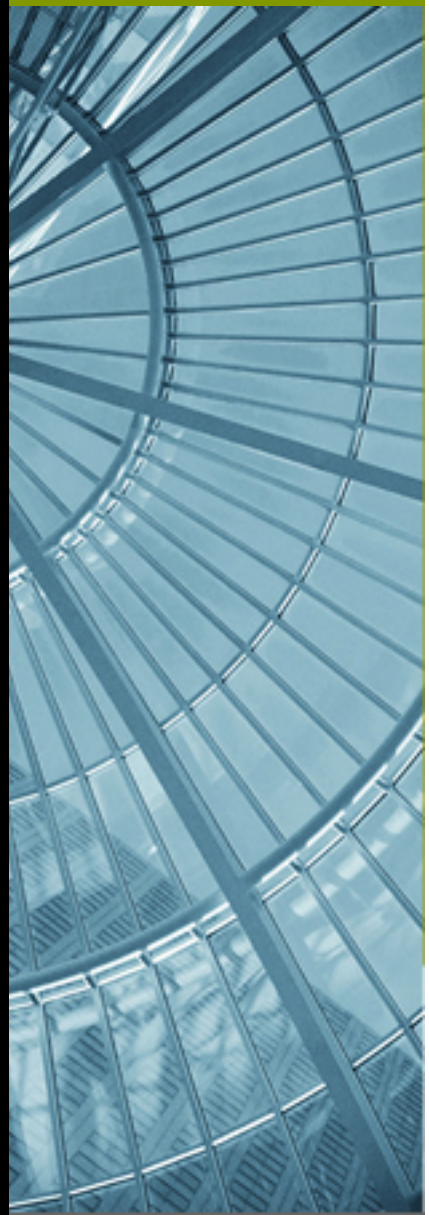


Protection of Data Privacy from the Power of the Administrator

Barbara Banks, Sr. Staff Engineer
Adaptive Server Enterprise
December 12, 2007

Sybase, Inc.

- Sybase is a leading provider of enterprise infrastructure and mobile software
- Adaptive Server Enterprise (ASE)
  - Sybase's award-winning data manager
  - High-performance, mission critical database management system
- Customer base
  - ASE manages some of the world's most critical data, especially in the vertical markets of financial services, government, telecommunications, healthcare and defense.
  - Powers over 50% of Wall Street trades
  - 20,000 enterprise customers worldwide

Agenda

- Sybase Encrypted Columns project
  - Objectives of ASE Encrypted Columns
  - Feature architecture and implementation
    - Protection of data privacy from power of administrator
- Customer response
- Ongoing work

Protection of Data Privacy

- Generic data privacy is the main objective
- Why is it important?
  - Compliance with legislative mandates, recommendations and expectations
    - Affects all businesses storing personally identifying information
  - Public trust in e-business
    - Customer often bears the risk of fraud
  - Employee trust in employer

Sybase – Native Encrypted Columns

- Since the late 1990's Sybase provided column level encryption through the use of a third party software encryption product
  - Solution didn't scale to large numbers of customers
- 2003 - Decided to write our own solution based on column encryption as an intrinsic data property
  - 2005 - First release of product with basic encryption functionality
  - 2007 – Extended functionality, to protect data privacy from power of the administrator
- Wide scale adoption by Sybase customers
  - Licensed feature; revenue generating

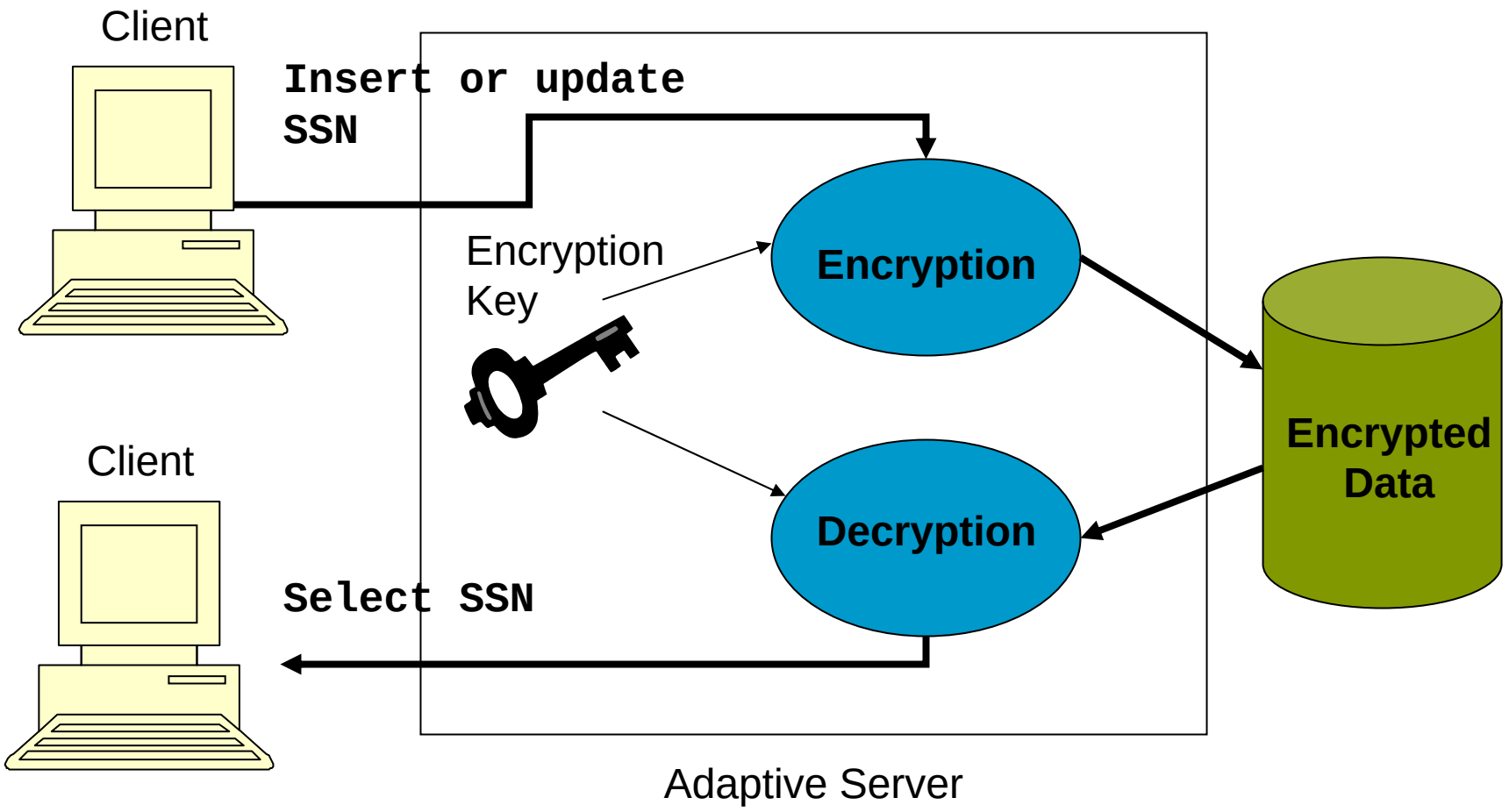
Encrypted Columns - Objectives

- Protect data “at rest”
  - in the database
  - in backup tapes
  - in replication queues
- Provide data privacy through encryption as a column-level attribute
- Deployable with no application changes
- Optimize performance
  - Minimize the number of decryption operations through efficient searches and joins

Encrypted Columns - Objectives

- Robust key management
- Ease of use
  - Functionality usable through new SQL commands and extensions to existing SQL
- Provide Disaster Recovery
  - Ability to securely migrate/replicate keys and data
- Protection of privacy from power of administrator
  - Separation of roles for administration of data and keys
  - Provide key copies for end users, encrypted by a password unknown to the admnistrator

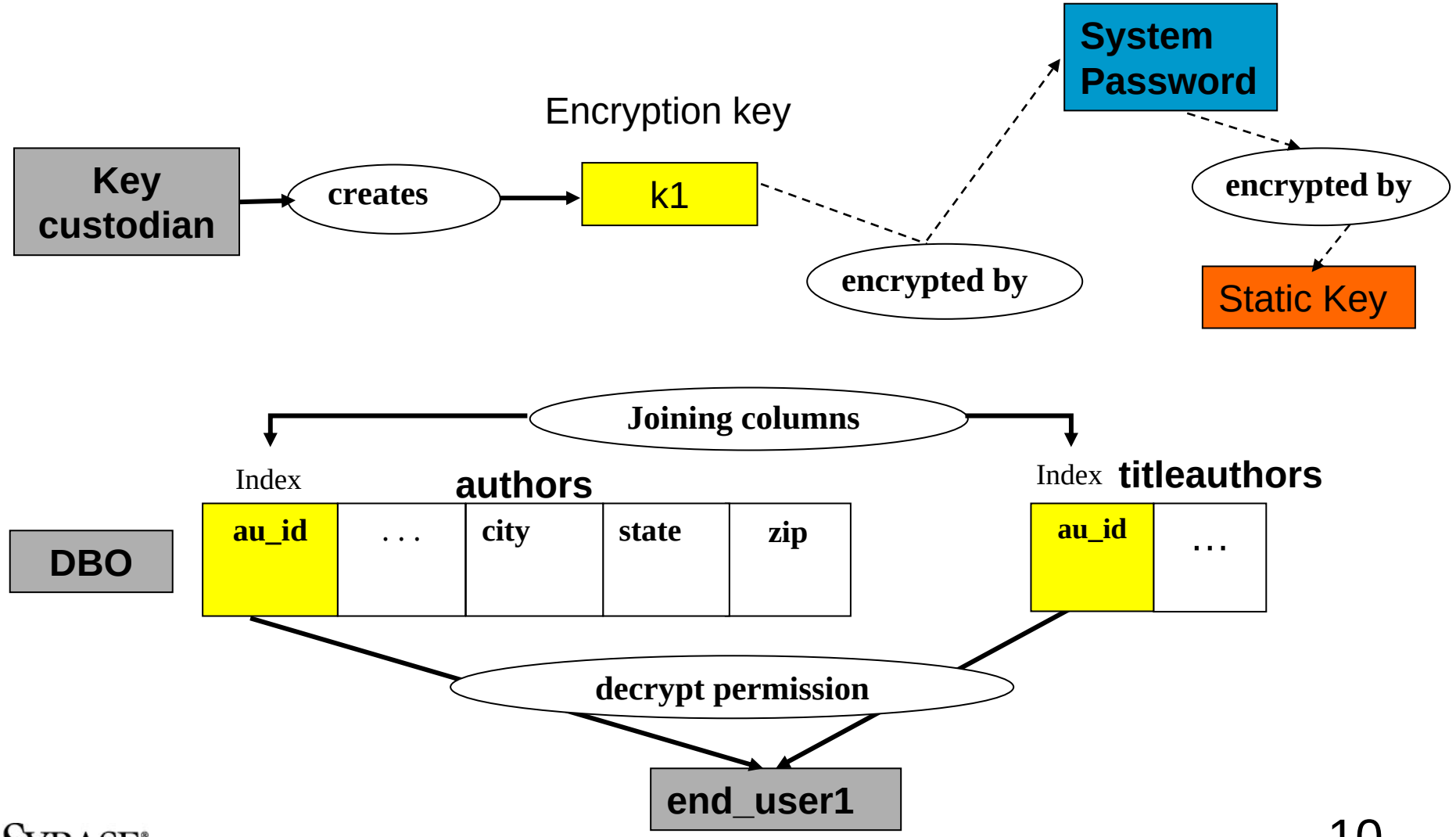
Encryption in Adaptive Server



Encrypted Columns user interface

- Create Encryption Key(s)
  - Stored encrypted in system catalog
- Alter table to encrypt data column(s) with named key(s)
- Grant decryption authorization to users or roles
  - New SQL permission
  - Separates roles of those allowed to see data in the clear and those who can only see it in ciphertext form
- Continue using same old SQL
  - ASE automatically encrypts and decrypts column data on INSERT, UPDATE, SELECT; in WHERE clauses

Encrypted Columns Schema



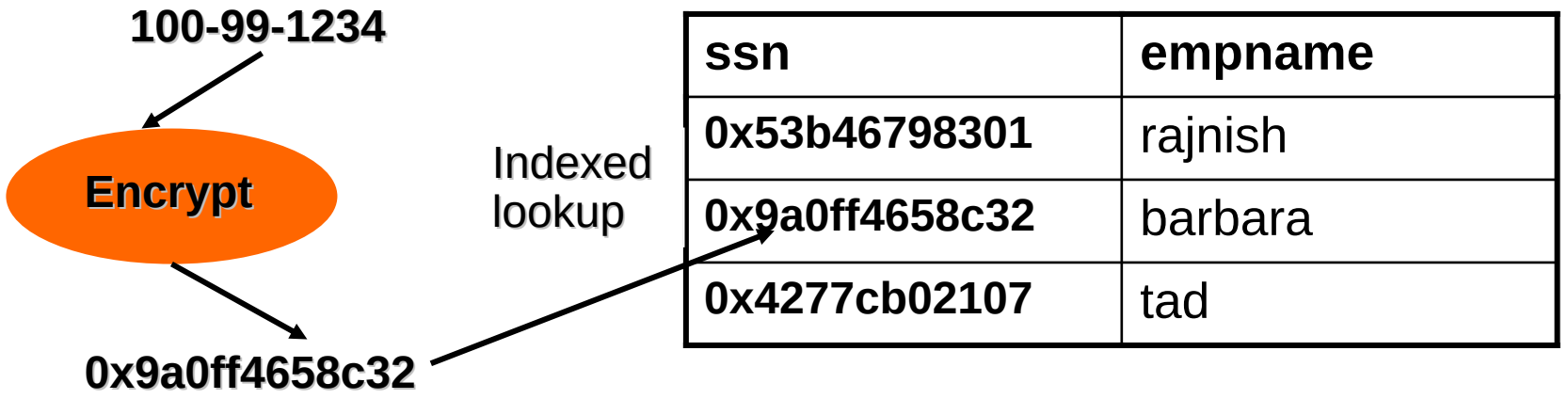
Decrypt permission and application transparency

- When application user lacks decrypt permission, what is the correct behavior?
  - Issue an error?
  - Return ciphertext data?
  - Return a null?
- Solution
  - Return a default value

Optimization

- ASE matches encrypted data based on the ciphertext value, where possible.
  - Reduces the number of decryption operations per query
  - Allows the user of indexes on encrypted columns

select * from emp where ssn = '100-99-1234'



ssn	empname
0x53b46798301	rajnish
0x9a0ff4658c32	barbara
0x4277cb02107	tad

Optimization (cont'd)

- **Joins across tables are optimized the same way**
  - Providing the same key is used on joining columns

select * from emp e, dept d where e.ssn = d.ssn and dname = 'sales'

ssn	dname
0x53b46798301	eng
0x9a0ff4658c32	eng
0x4277cb02107	sales

ssn	empname
0x53b46798301	rajnish
0x9a0ff4658c32	barbara
0x4277cb02107	tad

Protection of Privacy from Power of Administrator

- Core issue
  - Authorize administration without data access
- Example - Service Provider
  - Provides service for out-sourcing data processing applications
  - System administrators are employed by service provider
  - Customers -- as end users -- must have confidence that sensitive data retains privacy.
- Example - In-house application
  - DBO has inherent power to see all data
  - Schema owner is often DBO for convenience

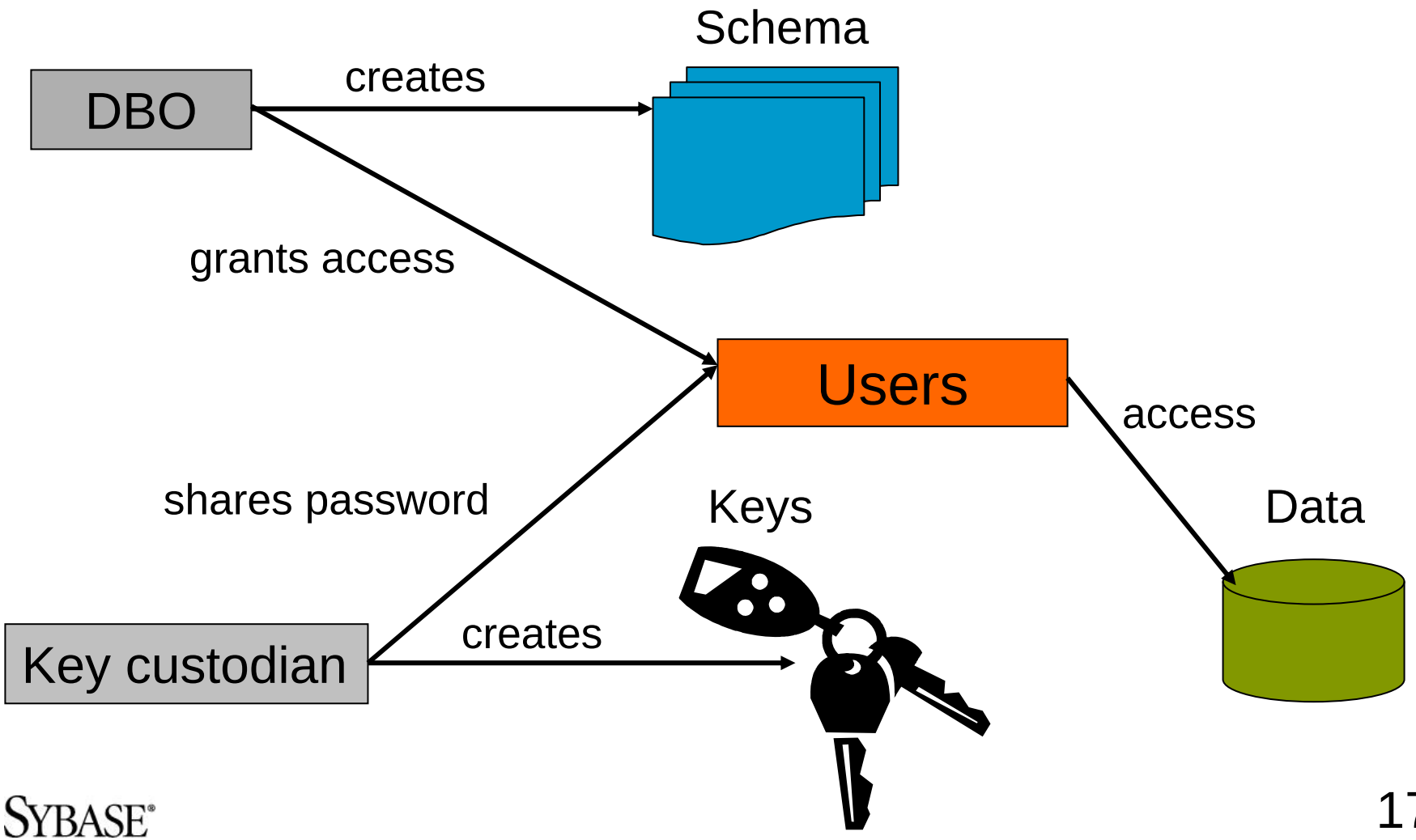
Limits on power of administrator

- Auditing
  - Good, but only after the fact
- Trust the administrator
  - Requirement, but not sufficient to satisfy auditors
- Limit need for System Administrator by creating less powerful administrator roles
  - Vest security in specialized roles

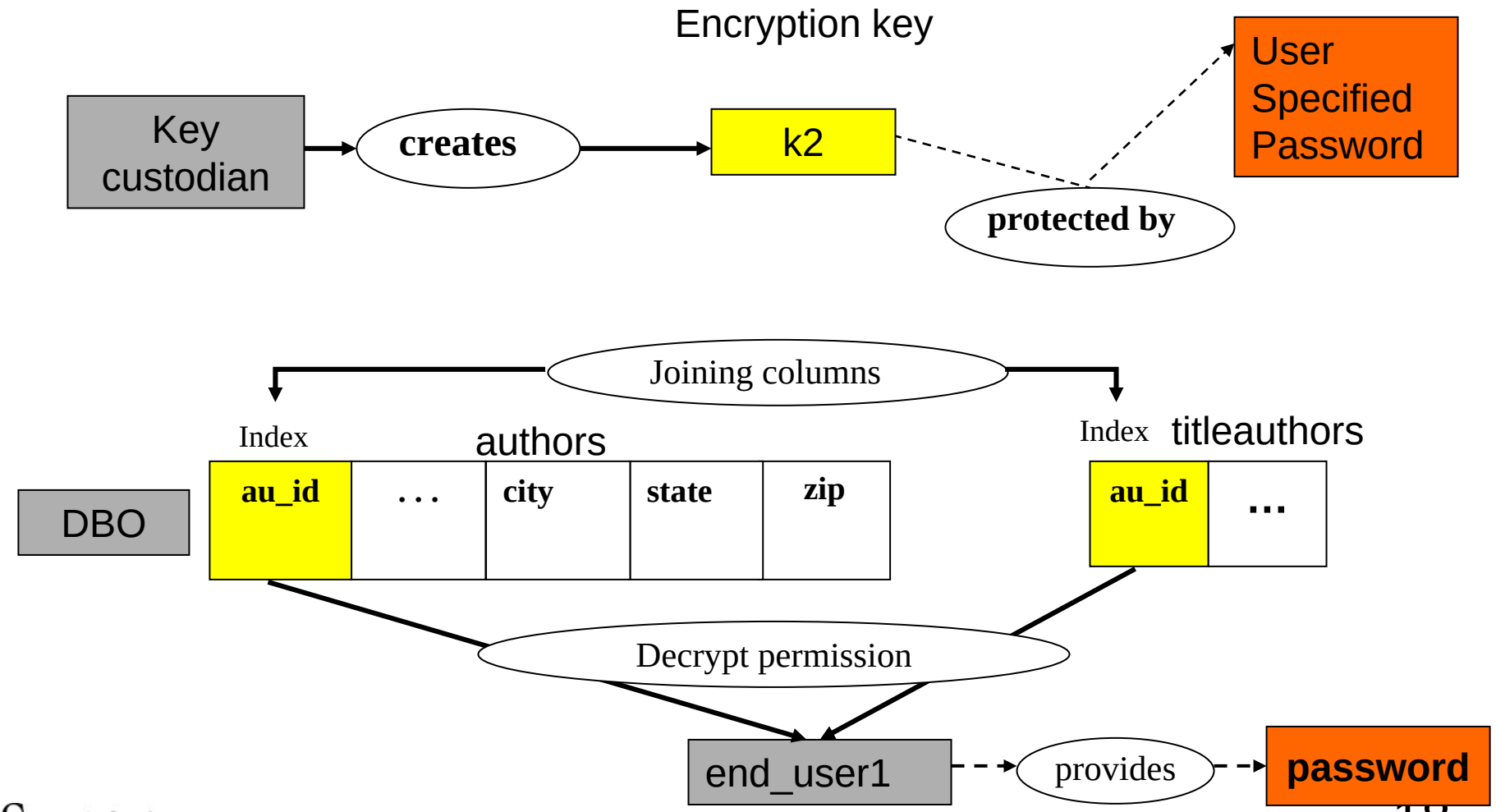
ASE solution for protection of privacy

- New keycustodian_role, a system role
  - Sole responsibility is key management
- Protection of keys using private passwords
  - Passwords do not need to be shared with administrators
  - Private password can be user's login password – allows applications to run without change
- Key copies allow multiple users access to the same key through their own password
- Keys can be recovered from lost passwords

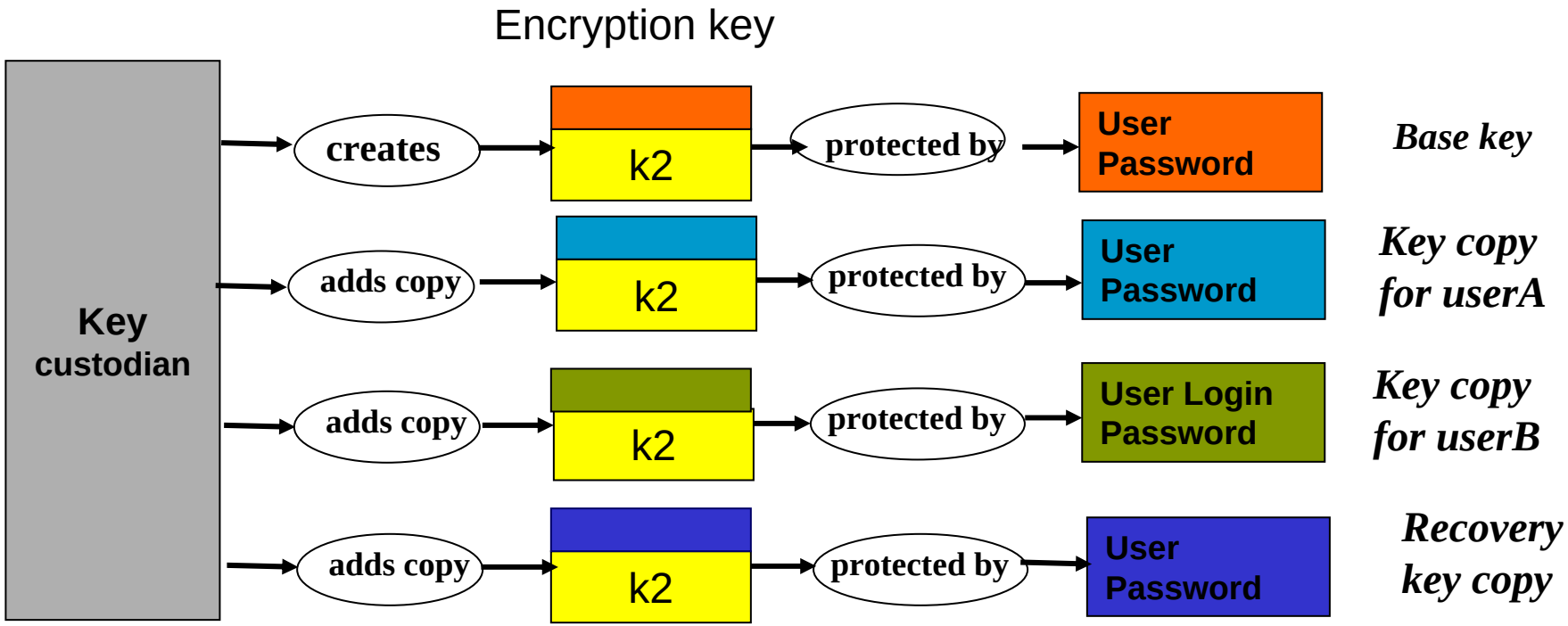
Separation of Roles



Encryption with private password



Encryption key copies



Customer Response

- One customer profile
  - Business provides outsourced administration of employee benefits
  - Approx 5 million self-serve users across clients. Need to handle as many as 10,000 users simultaneously
  - Each client company has 30 – 40 tables. Number of rows ranges from 500,000 to 10 million
  - Encryption and indexing of primary key columns (user SS#)
  - Performance was equivalent to pre-encryption performance, even during peak times

Ongoing work

- Dual control and split knowledge of key protection
  - Payment Card Industry (Data Security Standard) requirement
  - Requires 2 passwords to access key
- Centralized external key store
  - Enterprise-wide key management and distribution
- Efficient range searching of encrypted data
  - Avoid table scans and decryption of every row when searching on a range of data or on case insensitive data.

More Information

- Corporate website
  - **http://www.sybase.com**
- Presenter contact email:
  - **bbanks@sybase.com**
- ASE 15.0.2 user manual: Using Encrypted Columns in Adaptive Server®
  - **http://sybooks.sybase.com**
    - Select “Adaptive Server Enterprise” product set
    - Select Adaptive Server Enterprise 15.0.2
    - Select Core Documentation Set
    - Select New Features Adaptive Server Enterprise 15.0.2, and go to Chapter 2.


SYBASE®