THALES

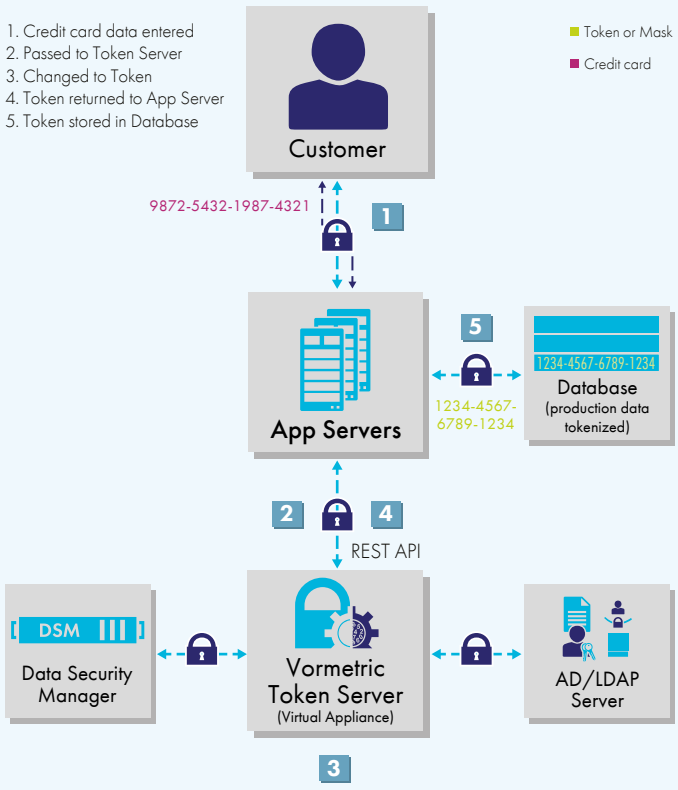
www.thalesesecurity.com

ANONYMIZING DATA FOR SECURITY AND COMPLIANCE

- Create tokens in numeric, text and date formats for single or multiple use applications
- Use LDAP user groups to decide what information is displayed to specific groups – For instance call center operators versus call center managers
- Deploy token server appliances in your virtual format of choice - OVF, ISO, Microsoft Azure Marketplace or Amazon AMI
- Non-disruptive – Restrict access to sensitive assets without changing database schemas

‹Thales e-Security›

VORMETRIC VAULTLESS TOKENIZATION WITH DYNAMIC DATA MASKING



Typical Tokenization Workflow

THE CHALLENGE:

For today's security teams, it seems virtually everything is proliferating, including the volume and sophistication of threats, the amount of data and repositories that need to be secured, and the number of mandates and tools that have to be supported.

All this proliferation continues to place increasing demands on security teams—but these teams don't see their time, staffing, or budgets undergoing any commensurate expansion. To contend with these realities, many security professionals have explored the use of tokenization, which has the potential to provide a convenient way to protect sensitive assets in databases and big data architectures, including those hosted on premises and in the cloud.

While tokenization offers the potential to address a wide range of security and compliance objectives, traditional tokenization tools have been far too complex and costly, and introduced too much of a performance hit on applications. More than ever, security teams need to be able to leverage the benefits of tokenization—and they need to do so in a consistent, efficient, high performance, and cost-effective manner.

‹Thales e-Security›

VORMETRIC VAULTLESS TOKENIZATION WITH DYNAMIC DATA MASKING

THE SOLUTION: VAULTLESS TOKENIZATION

The Vormetric Data Security Platform features tokenization capabilites that can dramatically reduce the cost and effort associated with complying with security policies and regulatory mandates like the Payment Card Industry Data Security Standard (PCI DSS). With Vormetric Vaultless Tokenization with Dynamic Data Masking, your organization can efficiently address its objectives for securing and anonymizing sensitive assets and cardholder records—whether they reside in the data center, big data environments or the cloud.

BENEFITS

- Reduce PCI DSS compliance effort and scope by minimizing servers requiring audit and control
- Fully leverage cloud, big data and outsourced models – Replacing sensitive data with tokens enables use without risk or compliance overhead
- Easily enable call center and other applications.
- Minimize data security staff training and overhead with a common platform used for other data security applications

"Technologies like tokenization reduce compliance scope by replacing sensitive data with a non-sensitive token that looks and acts like the original. This means you get data protection without the need to change your databases. Once sensitive data is replaced with the token, these systems are no longer subject to compliance, meaning a lot less work for IT and compliance teams"

. Adrian Lane, Analyst and CTO, Securosis

DYNAMIC DATA MASKING

Administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field. For example, a security team could establish policies so that a user with customer service representative credentials would only receive a credit card number with the last four digits visible, while a customer service supervisor could access the full credit card number in the clear. LDAP based groups, such as those available from Active Directory, and easily be used to establish and enforce the policy.

ESTABLISH TOKENIZATION WITH MINIMAL DISRUPTIONS AND EFFORT

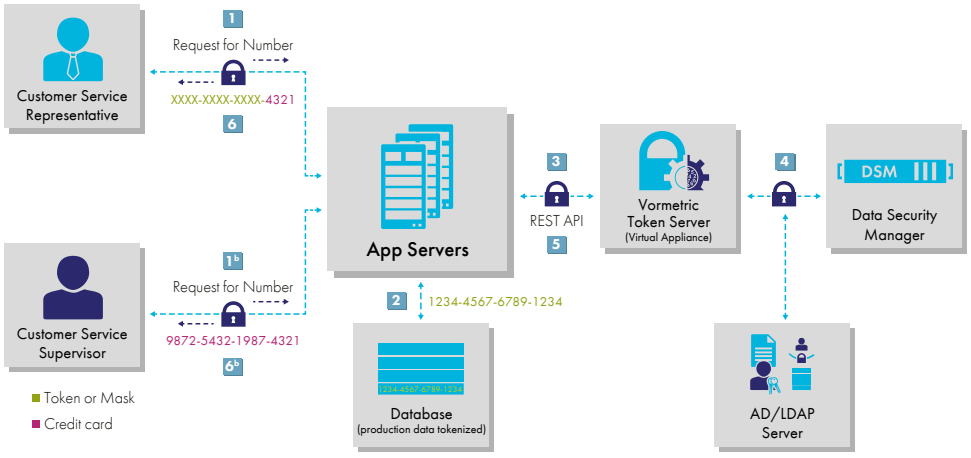
Designed for performance at scale, the solution includes REST APIs for tokenization requests and an easy to use user interface for defining policy and usage of dynamic data masking that minimizes changes required to applications.

- Application layer tokenization simplifies integration to existing implementations
- Easily established data masking policies enable new uses for existing data sets without increasing audit scope or extensive application rewrites
- Non-disruptive – changes to database schemas and implementations do not require extensive changes or down time

Visit us at: **www.thalesesecurity.com** to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Dynamic Data Masking Workflow

1. CSR requests credit card number
2. Token extracted from Database
3. Token and User passed to Token Server
4. LDAP inquiry shows CSR role, only last 4 digits may be viewed
5. Last 4 digits de-tokenized, the rest masked, and the number returned to the App Sserver
6. Masked number passed back to CSR



Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thalesesecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thalesesecurity.com

© Thales - July 2017 • PLB6804