VOLTAGE SECURITY - Technology Overview

Information Encryption for Email, Files, Documents and Databases

Voltage solutions are built upon two innovations of cryptography - Identity-Based Encryption (IBE) and Format-Preserving Encryption (FPE). These innovations open up new ways to securely communicate, new ways to protect sensitive employee and customer data to prevent identity theft and enable many many different ways of encrypting information.

Voltage Identity-Based Encryption

Information Encryption for Email, Files, Documents and Databases

Fundamentally, the reason to use encryption is to protect data so that only a specific person (for example, bob@b.com) or a machine (for example, www.voltage.com) can access it. However, until now, encryption techniques have relied on long, randomly generated keys that must be mapped to identities using digitally-signed documents, called certificates. The management of these certificates, and the need to fetch a certificate before encrypting to a person or machine, has made encryption very difficult.

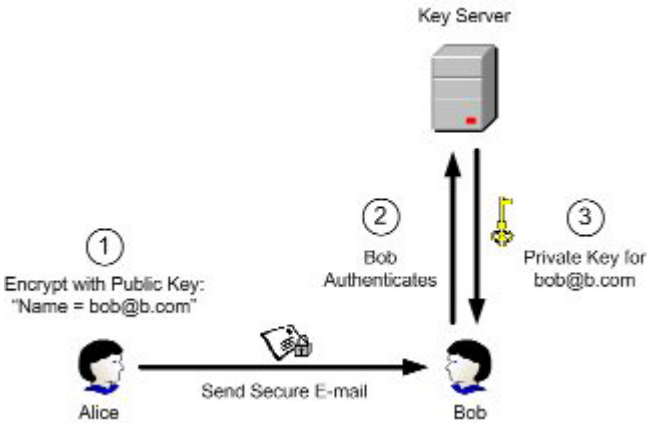
Identity-Based Encryption (IBE) takes a completely new approach to the problem of encryption. IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the mapping of identities to decryption keys.

The design of an Identity-Based Encryption system was a long-standing open problem in cryptography. Voltage now offers a platform based on the first secure, practical IBE system, the Boneh-Franklin IBE Algorithm.

How Voltage Security Identity-Based Encryption Works

Information Encryption for Email, Files, Documents and Databases

Identity-Based Encryption (IBE) dramatically simplifies the process of securing sensitive communications. For example, the following diagram illustrates how Alice would send a secure email to Bob using IBE:



Step 1: Alice encrypts the email using Bob's e-mail address, "bob@b.com", as the public key.

Step 2: When Bob receives the message, he contacts the key server. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements.

Step 3: After authenticating Bob, the key server then returns his private key, with which Bob can decrypt the message. This private key can be used to decrypt all future messages received by Bob.

Note that private keys need to be generated only once, upon initial receipt of an encrypted message. All subsequent communications corresponding to the same public key can be decrypted using the same private key, even if the user is offline. Also, because the public key is generated using only Bob's email address, Bob does not need to have downloaded any software before Alice can send him a secure message.

The Math Behind IBE

The mathematical foundation of IBE is a special type of function called a "bilinear map." A bilinear map is a pairing that has the property:

Pair(a • X, b • Y) = Pair(b • X, a • Y)

The operator "•" is multiplication of a point on an elliptic curve by integers. While multiplication itself (e.g., calculating **a•X**) is easy, the inverse operation (finding **a** given **X** and **a•X**) is practically impossible. Two examples of bilinear maps are the Weil Pairing and the Tate Pairing.

The IBE algorithm consists of four operations:

Setup, which initializes a key server
Encrypt, which encrypts a message for a given user
Key Generation, which generates a private key for a given user
Decrypt, which given a private key, decrypts a message

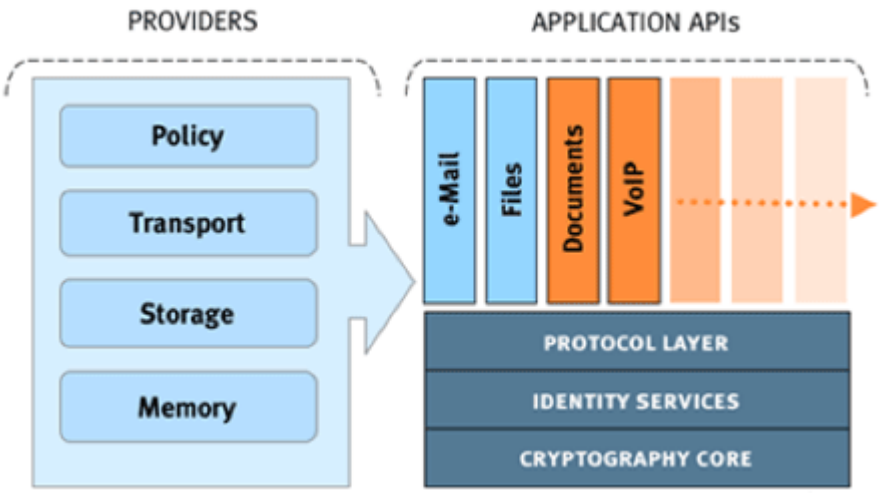
Building Applications Using Voltage Identity-Based Encryption

Information Encryption for Email, Files, Documents and Databases

The Voltage IBE Toolkit is a set of tools that enable developers to quickly and easily incorporate Identity-Based Encryption into their applications. Using the Toolkit, you can secure an email, file, or other arbitrary data in less than 15 lines of code, without the need for certificates; all you need to know is an email address. Applications built using the Toolkit seamlessly integrate with the Voltage Enterprise Privacy Management Platform, enabling developers to take advantage of its centralized administration, advanced policy management, and key distribution architecture.

The Toolkit provides high-level interfaces for rapid application development as well as lower-level cryptographic APIs for advanced security operations. The Toolkit is suitable both for ISVs looking to integrate robust security into their products as well as enterprises wanting to secure internal applications.

The Toolkit supports all major cryptographic algorithms and is FIPS 140-2 Level 1 certified. It offers a C interface and is supported on Windows and Linux, with additional platform support planned. The Toolkit is offered at no charge, with source code provided.



Voltage IBE Toolkit Benefits

Identity-Based Encryption
The Voltage IBE Toolkit is the only commercially available SDK that implements IBE. IBE enables data to be secured to any user, machine, or entity without the need for certificates or pre-enrollment, enabling an extremely lightweight encryption system.

Platform Integration
Applications built using the Toolkit can transparently leverage the Voltage Enterprise Privacy Management Platform for key management, authentication, and transport. Existing IBE keys can be used for new applications, and data can be secured in formats compatible with existing Voltage applications.

Rapid Application Development
The Toolkit offers high-level APIs that require no knowledge of cryptography or data security algorithms. An email message or file can be encrypted in just a few function calls.

Source Code Provided
Well-documented source is provided, enabling easy debugging. The source code may be modified or extended to suit the specific needs of an application.

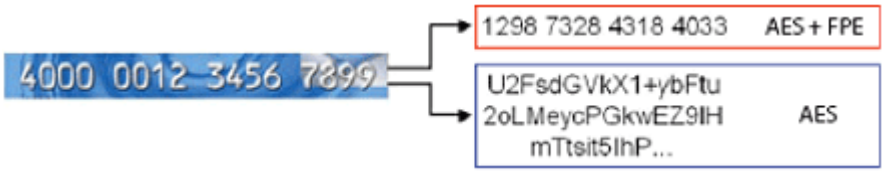
FIPS Certification
The Toolkit's Cryptographic Module has been awarded FIPS 140-2 Level 1 certification by NIST. The certifiation specifically validates the following algorithms: DES, Triple-DES, AES, DSA, SHA-1 and Random Number Generation. Voltage's FIPS 140-2 certification is available online at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt522.pdf

Voltage Security Format-Preserving Encryption (FPE)

Preserving Critical Business Functions by Maintaining Data Format

Format-Preserving Encryption (FPE) is a fundamentally new approach to encrypting structured data, such as credit card or Social Security numbers, that makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. It uses a published encryption method with an existing, proven encryption algorithm to encrypt data in a way that does not alter the data format. The result is a strong encryption scheme that allows for encryption with minimal modifications to the way that existing applications work. FPE is a mode of standard AES, recognized by NIST.

Traditional algorithms turn small, structured data elements, such as 16-digit credit card numbers, into larger, binary fields. As a result, implementing these algorithms typically required massive re-engineering of databases and applications in order to accommodate the modified data sizes and formats.



Where older encryption technologies radically alter the structure of data, Voltage Format Preserving Encryption (FPE) maintains data format integrity, significantly minimizing changes to existing applications.

With FPE, encrypted data will retain its original format, on a character-by-character basis, so that encrypted data "fits" in existing fields, eliminating the need for database schema changes.
For example, a 16-digit credit card number can be encrypted, with the output guaranteed to also have 16 digits; the credit card checksum can even be maintained. FPE also preserves referential integrity, which enables encryption of foreign and indexed keys and ensures consistency across data stores.

FPE can also be used for cryptographic masking or de-identification of data. By preserving data formats, sizes, and referential integrity, FPE provides an efficient method for "sanitizing" data without the need for massive masking or lookup tables. Additionally, because it is a two-way encryption algorithm, FPE enables both reversible and non- reversible data masking.

Properties and benefits of FPE:

- Supports data of any format, including numeric and alphanumeric
- Eliminates changes to database or application schemas —data "fits" in existing fields
- Guarantees referential integrity
- Enables encryption of primary and foreign keys
- Provides reversible and non-reversible data masking