GLOBAL 2007

Обучение Java

Тема **Безопасность в JAVA**

Часть **Архитектура поставщиков безопасности**

Автор **ASKIL (omendba@gmail.com)**

27.02.2007

Поставщик безопасности предусматривает: алгоритмы и программы, реализующие их.

Приведем простой пример: дайджест сообщения. Он может быть осуществлен специфическим алгоритмом, типа MD5 или SHA. Алгоритм вообще обеспечивается как конкретный класс. Однако можно получить два класса, реализующие алгоритм SHA, от различных поставщиков, но результаты будут одинаковыми для обоих классов.

Цель интерфейса поставщика безопасности состоит в том, чтобы предоставить легкий механизм, где определенные алгоритмы и их выполнение могут быть легко заменены. Поставщик безопасности позволяет нам изменять выполнение SHA алгоритма, который находится в использовании, и представлять новый алгоритм.

Следовательно, типичный программист только использует классы, чтобы выполнить необходимые действия.

Компоненты архитектуры

Архитектура имеет следующие компоненты безопасности:

• Родные классы

Эти классы идут с Java как часть ядра API.

• Классы алгоритмов

Набор классов, которые осуществляют алгоритмы. Данные классы обеспечиваются поставщиком платформы Java и сторонними организациями.

• Классы поставщиков

Набор классов с алгоритмами от поставщика.

• Классы безопасности

Классы поддерживают список классов поставщика и взаимодействуют с каждым из них, чтобы просмотреть, какие методы они поддерживают.

Основные алгоритмы безопасности

Класс	Название алгоритма
AlgorithmParameters	DSA
AlgorithmParameterGenerator	DSA
CertificateFactory	X509
KeyFactory	DSA
KeyPairGenerator	DSA
KeyPairGenerator	RSA
KeyStore	JKS
MessageDigest	MD5
MessageDigest	SHA-1
MessageDigest	MD2
SecureRandom	SHA1PRNG

Signature	DSA
Signature	MD2/RSA
Signature	MD5/RSA
Signature	SHA-1/RSA