VA Smalltalk Cryptographic Support

Seth Berman
Director Of Engineering
Instantiations, Inc.

instantiations
VA Smalltalk

Crypto Features

- Message Digests
  - MD5, SHA-1, SHA-256, SHA-512….
- Message Authentication Code (MAC)
  - HMAC algorithm
- Symmetric Ciphers
  - AES, Blowfish, IDEA, Triple-DES…..
- Public/Private Key Algorithms
  - Encrypt/Decrypt: RSA
  - Digital Signatures: RSA, DSA
  - Digital Enveloping: RSA
  - Key Agreement: Diffie-Hellman

instantiations
VA Smalltalk

Crypto Features Cont...

- Secure Random Number Generator
- High-Performance Crypto Chains
  - Pipelines cryptographic flows
  - Example: plainText | sha1 | aes-256 | base64 | [socket]
  - Plain Text -> Base64-encoded Cipher Text
  - SHA1 Hash computed
  - Pipeline flows are reversible.
- X509 Certificates
- ASN1 Objects
- PEM/DER encoding in many formats

instantiations
VA Smalltalk

Crypto Internals

- Bindings to OpenSSL 1.0.x
- Memory Management
  - Memory Ownership
    - Prevents freeing of static memory
    - Prevents double-free of native memory
  - GC Finalizer
    - Provides assistance with freeing native memory
  - Reference-Counter
    - Aliased refs are explicitly tracked

instantiations
VA Smalltalk

Crypto Internals

- Asynchronous Callout Engine
  - Smalltalk Process -> Native Thread
  - Allows for Utilization of Multiple CPUs
- OpenSSL internally uses multiple native threads
  - Provides a Service Provider Interface
  - Platforms must implement native thread locks.
  - VA Smallltalk implements these

instantiations
VA Smalltalk

Crypto Internals Cont…

- Slight departure…
  - Most OSObjects are simple accessors to native memory
  - The Crypto Bindings…
    - Mostly contain behavior and High-Level APIs
    - Are generally opaque…their native layout is not exposed.
    - Memory-Managed
    - The result is…they are very pleasant to work with.
- This is in preparation for a VAST Interface layer which allows multiple providers (i.e. BoringSSL, LibreSSL…)

instantiations
VA Smalltalk

Crypto Examples

- Suite of Crypto Coding Examples
  - Provides Story-driven examples
  - User can run, step, debug to learn how they work
  - Assertion based format because these same examples are used as integration tests internally

instantiations
VA Smalltalk

SSL/TLS

- VA Smalltalk's existing SSL/TLS support is now built on the new crypto library.
- Inherits the safer memory management features
- More options exposed for SSL/TLS connections
- Gained TLSv1.2 support
- More options for X509 certs

instantiations
VA Smalltalk