Code signing at the ASF

Mark Thomas, 15 April 2015
Introduction

- Apache Tomcat committer since December 2003
  - markt@apache.org
- ASF Member since June 2007
- Security Team volunteer since late 2007
- Infrastructure volunteer since early 2008
Agenda

- Why the ASF needs a code signing service
- Requirements
- Options considered
- Why we choose Symantec’s service
- What the code-signing service provides
- Projects are using the service
- How to request the code-signing service for your project
Why?
Why the ASF needs a code signing service

• Apache OpenOffice
  – End user software
  – Not your typical ASF user (less technical)
  – Windows unsigned code warnings scare people off
  – Code signing means nice ‘trusted source’ dialogs instead

• Java applets
  – Becoming increasingly difficult to run unsigned code
  – Bypassing the checks is far from user friendly
  – Code signing means much simpler process to accept remote code
Requirements
Code Signing Requirements

- Signing requires a private key
- Signing keys need to be kept secure
- Single ASF key
  - Would have to remain under infra control
  - Any compromise would be very messy
  - Compromise would reflect badly on the ASF
Code Signing Requirements

• Per PMC key
  – Experience suggests not all PMCs would look after it
  – Any mess would be contained within the PMC that screwed up
  – Still reflects badly on the ASF as a whole

• Per release manager key
  – Experience suggests not all RMs would look after it
  – End users would have to trust individual RMs
  – Some projects change RM with every release
  – End-user burden
Code Signing Requirements

- The solutions considered were constrained by some of the ASF’s requirements for releases
- Releases must be built on trusted systems
  - Essentially this means the release manager’s own machine
Options
Options Considered

• Per release manager keys rejected
  – End-user burden
  – Cost
  – Overhead of keeping track of keys

• Per PMC keys rejected
  – Too great a risk of compromise
  – Compromise would reflect badly on the ASF
Options Considered

• Option 1: ASF signing key with build
  – Centralised, trusted build system that would build from svn/git and then sign
  – Requires fully automated build
  – Would have to be custom built

• Option 2: ASF signing service
  – Centralised signing service
  – Release managers submit artefacts for signing
  – Would have to be custom built
Options Considered

• Option 3: Commercial signing service
  – Centralised signing service
  – Release managers submit artefacts for signing
  – Would have to be paid for
Why Commercial?
Why A Commercial Service

- Available sooner
  - Infra didn’t need to build anything

- Lower cost
  - Compared to infra having to build and maintain something
  - Not compared to buying code signing certs for a couple of PMCs

- Lower risk
  - Writing a secure code-signing service is hard

- Minimal resources required from infra to support
Symantec
Features of the Symantec Service

- Each PMC is a separate organisation within the service
- Each release manager has their own account
- Supports a wide range of signing types
  - Windows
  - Java
  - Android
- Web based GUI and SOAP interface
- A signing event can sign one or more files
Features of the Symantec Service

- Each signing event can be traced back to the user that requested it
- Each signing event can be revoked individually
- An unlimited number of test signing events are allowed
- Production signings cost one credit per signing event
- Infra allocates credits to the PMCs as required
Features of the Symantec Service

• Infra has written some client side tools to aid integration with project builds
  – Java
  – Ant task
Projects
Projects Using Code Signing

- **Apache Tomcat**
  - Windows binary (the installer and unistaller)
  - Primarily because I am a release manager for Tomcat
  - There was a low level of user demand
  - Fully integrated into the build process (ant release)

- **Apache Commons**
  - Because Tomcat needed Commons Daemon binaries signed

- **Apache OpenMeetings**
  - JARs used for Java Applet
How
How To Request Code Signing

• Open an INFRA Jira ticket for the code signing component
  – Need Apache IDs for release managers

• Infra will register the PMC and release managers with Symantec

• Expect a bunch of e-mails from Symantec

• End result will be a personal certificate to access the web interface
Questions