STATE OF COLORADO
Department of State
1700 Broadway, Suite 200
Denver, CO 80290

Jena M. Griswold
Secretary of State
Judd Choate
Director, Elections Division

Voting Systems Trusted Build Procedures

Trusted Build

A software build (also referred to as a compilation) is the process whereby source code is converted to machine-readable binary instructions (executable code) for the computer. A **trusted build** (or trusted compilation) is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. The primary function of a trusted build is to create a chain of evidence which allows stakeholders to have an approved model to use for verification of a voting system. Specifically, the build will:

- Demonstrate that the software was built as described in the manufacturer's Technical Data Package (TDP).
- Show that the tested and approved source code was actually used to build the executable code used on the system.
- Demonstrate that no elements other than those included in the TDP were introduced in the software build. The vendor or source from which each commercial-off-the-shelf (COTS) product was procured must be included in the TDP.
- Document for future reference the configuration of the system certified.
- Demonstrate that all COTS products are unmodified by requiring the Voting Systems Testing Laboratory (VSTL) to independently obtain all COTS products from an outside source.

Trusted Build Procedure

A trusted build is a three-step process:

1. The build environment is constructed,
2. The executable code and installation media are created, and
3. The VSTL verifies that the trusted build was created and functions properly.

In each step, a minimum of two witnesses from different organizations are required to participate. These participants must include a VSTL representative and a manufacturer representative. Before creating the trusted build, the VSTL must complete the source code review of the software delivered from the manufacturer for compliance with the standards and must produce and record file signatures of all source code modules. Hashes shall use a current Federal Information Processing Standard (FIPS) 140-2 level 1 or higher validated cryptographic module. After the trusted build is completed, there shall be no other "final" build. As the final step, the trusted build must be submitted to the Secretary of State.

Constructing the Build Environment

The VSTL shall construct the build environment in an isolated environment controlled by the VSTL, as follows:

- The device that will hold the build environment shall be completely erased, in accordance with Department of Defense or National Institute of Standards and Technology (NIST) approved methods. The VSTL shall ensure a complete erasure of the device.
- The VSTL, with manufacturer observation, shall construct the build environment.
- After construction of the build environment, the VSTL shall produce and record a file signature of the build environment.
- A clone of the build environment computer's main storage media shall be created. File signatures shall be taken by the VSTL for verification purposes.

Creating the Executable Code and Installation Media

After successful source code review the VSTL shall:

- Check the file signatures of the source code modules and build environment to ensure they are unchanged from their original form.
- Load the source code onto the build environment and produce and record the file signature of the resulting combination.
- Produce the executable code, and produce and record file signatures of the executable code. A clone of the computer's main storage on which the executable code was created shall be created, with the file signatures verified by the VSTL.
- The VSTL shall create installation media from the executable code, and produce and record file signatures of the installation media.

Verification of the Created Media

Upon completion of all the tasks outlined above, the VSTL shall perform the following tasks:

- Install the executable code onto the system submitted for testing and certification before the completion of system testing.
- Produce and record file signatures of each voting system file resident on each device.
- Verify that all media to be included in the Trusted Build and submitted to the Secretary of State functions properly.

Installation of the Trusted Build

Members of the Voting Systems team will use the Trusted Build media to install the voting system software and firmware on the components of each county's voting system. An affidavit will be provided to the county that details the following:

- Date of installation
- Component type and serial/tag number(s)
- Applicable software module names and version numbers
- Name and signature of the person performing the installation