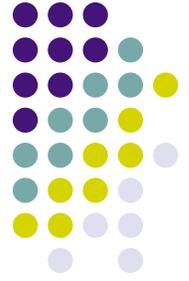# SHA-2 Migration
Background

- Secure Hash Algorithm (SHA) is a one-way function applied to a variable-length piece of data to produce a fixed-length value.

- SHA ensures no two pieces of data yield the same value (called a "collision").

- Treasury PIV-reliant applications currently rely upon SHA-1, which employs 80 bits of "security," to provide strong proof of authenticity and integrity of data.

- Examples:
  - Who is authenticating to my PIV-enabled Windows domain?
  - Who authored this document?
  - Who signed this PIV certificate?
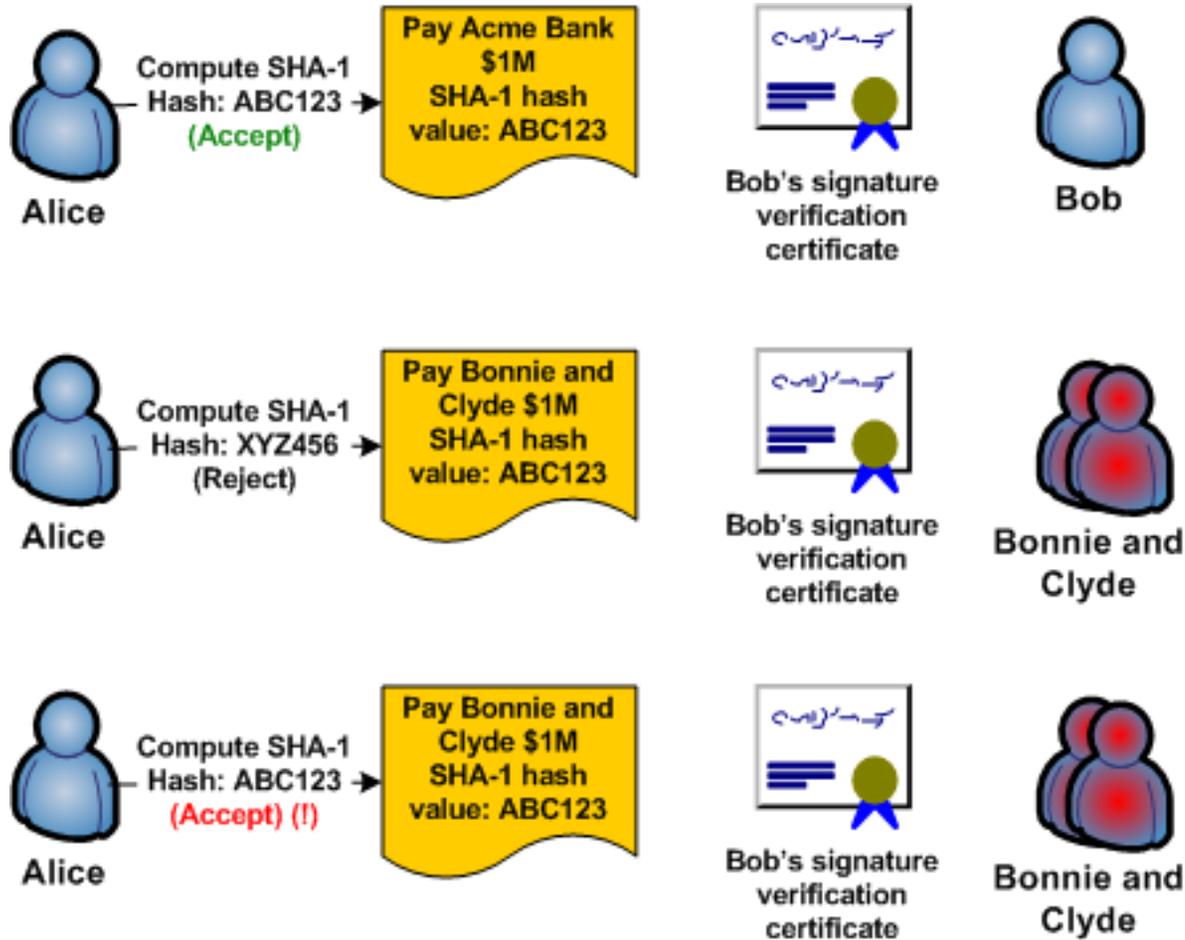
SHA-2 Migration
The need to move
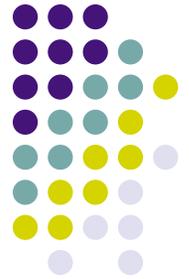
- Weaknesses recently discovered in SHA-1 dramatically lower its security strength to the point where it is theoretically possible to produce a collision.

- This in turn puts trust at risk for Treasury's PIV-reliant applications.

- The Federal community is migrating to SHA-2, which employs up to 256 bits of security and strengthens the PIV PKI trust model
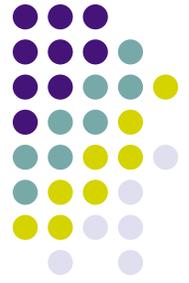
SHA-2 Migration
## Hashing in Action: The good, bad and ugly

SHA-2 Migration
Requirements and Recommendations

- Treasury and Federal PKI policies require SHA-2 signatures on certificates and CRLs generated after **December 31, 2010**

- NIST recommends that Agencies stop using SHA-1 as soon as possible, and requires Agencies to use SHA-2 exclusively after **2010**.

  - http://csrc.nist.gov/groups/ST/hash/policy.html

- Treasury PKI PMO is planning to migrate Treasury's PKI to SHA-2 in advance of this date. Treasury expects GSA MSO to also migrate before then, though no dates have been set.

SHA-2 Migration
What does this mean to me?
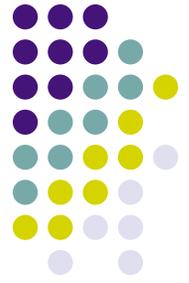
- Not all PIV-reliant applications support SHA-2

- The Treasury PKI PMO plans to migrate the PKI development environment in advance to ensure Bureaus are afforded the opportunity to test.

- Following the development migration, Bureaus can acquire test certificates to integrate and use within their environments:
  - For PIV cards, through the HSPD-12 PMO and PIV test card program
  - For devices, through their local PKI RA and Treasury PKI PMO

- Bureaus that have deployed applications reliant on PIV certificates are strongly recommended to test capability in advance of the Treasury PKI PMO's production migration.

- Bureaus should test several conditions wherever applicable; for example:
  - Capability to **accept** SHA-2 signed PIV certificates and CRLs
  - Capability to **process** SHA-2 signed data
  - Capability to **produce** SHA-2 signatures