FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

CHANGE MANAGEMENT

Change Management

Why this new section of the FIPS 201-2?

- Because we want to work with all the stakeholders to mitigate the impact of any change on the existing infrastructures
- And because we want to be faithful to these two principles:
  - Do no harm; don't break what works
  - Anything we change should not astonish anyone

Change Management

How to achieve these goals?

- Changes will be introduced over 5 to 6 year period to allow time to execute transition plans
- FIPS 201 will contain only requirements that change infrequently. Implementation details should be in the associated Special Publications
- New requirements will be introduced '*optional*' at first, and would become *mandatory* in the following revision
- Backward compatibility will be maintained where possible

Change Management

New sections added to this revision

- Backward compatible changes
- Non-backward compatible changes
- New Features
- Deprecated and removed elements
- FIPS 201 Version Management

Change Management

How we will proceed?

- CM FIPS 201 sections as well as CM sections in the PIV SPs will be written in concert with stakeholders with a particular attention to Users and Implementers
- Workshops, public comments and contributions are the main road to raise attention onto CM issues

Change Management

Example of CM problems:

- The draft FIPS 201-2 document introduces new features (e.g., match on card and two possible card authentication keys) and makes some data objects mandatory instead of optional (e.g., CAK). What are the **recommended migration mechanisms** as well as the **potential impact** to the relying party infrastructure?
- How does a terminal find out if the card presented is compliant with FIPS 201-1 or FIPS 201-2?