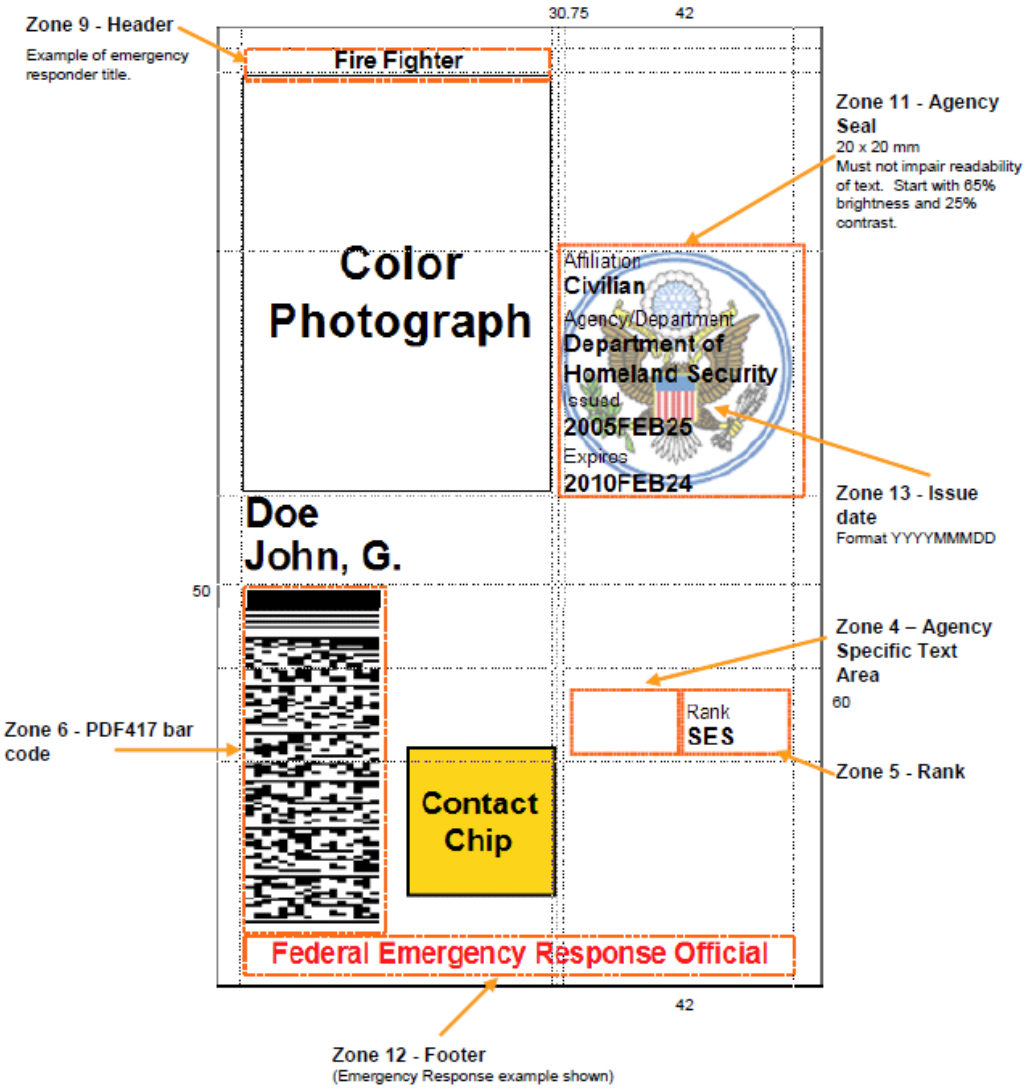
FIPS 201-1 Revision

Card Topology

The case against Calibrated "EYEBALLS"

Ron Martin, HHS,

Current and Proposed Front



Current and Proposed Back

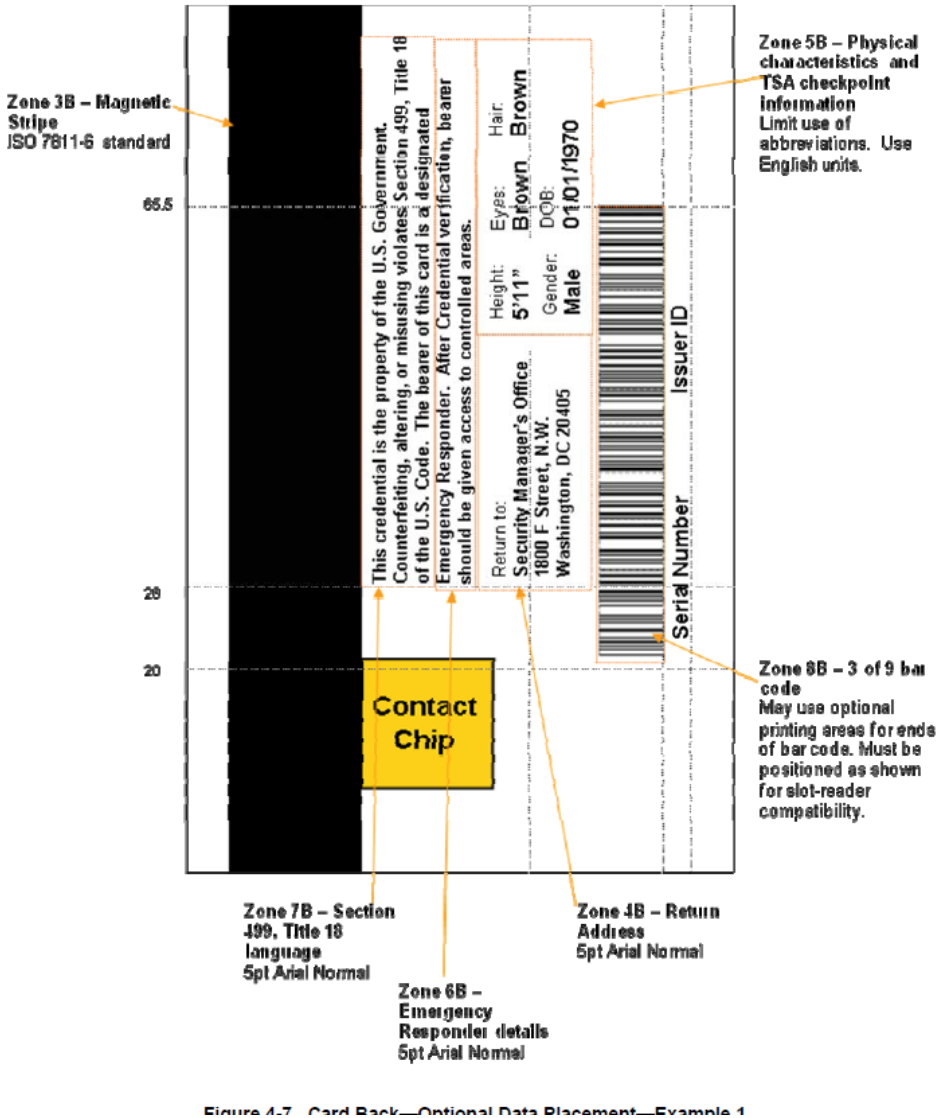


Figure 4-7. Card Back—Optional Data Placement—Example 1

SP800-104
A Scheme for PIV Visual Card Topography

The purpose of this document is to provide additional recommendations on the Personal Identity Verification (PIV) Card **color-coding for designating employee affiliation**. Compliance with this document is voluntary; however, a department or agency shall not claim compliance unless it **adheres to all requirements of this document**. This document is not intended to contradict requirements specifically identified in the Federal Information Processing Standard 201 (FIPS 201) or its associated documents, nor to limit options permitted by FIPS 201 except as explicitly stated herein. The recommendations in this document complement FIPS 201 in order to increase the reliability of PIV card visual verification.

Concern

OMB suggest that all legacy technologies be removed from the PIV card; The **Specification allows legacy technologies**

Centralized card personalization vendors and Local card production Printers **cannot duplicate the card specifications**

Agencies **will need** additional credentials to (NON-PIV) for logical and Physical Access

Color Designation

Color Designation specified not attainable

For the green bar the NIST document specifies **153,255,153.** As you may be aware printing with a CMY process doesn't translate to a RGB value that is seen on a computer monitor.

we've experimented with RGB values to get a green that looks closer to what the NIST 800-104 on a computer screen may look like. We've backed off the R and B values to 120, (**120,255,120**) .

The goal has been to get a color bar that is close to the same color as "seen" on a computer screen.

Side-by-Side Card Comparison

Oberthur printed card

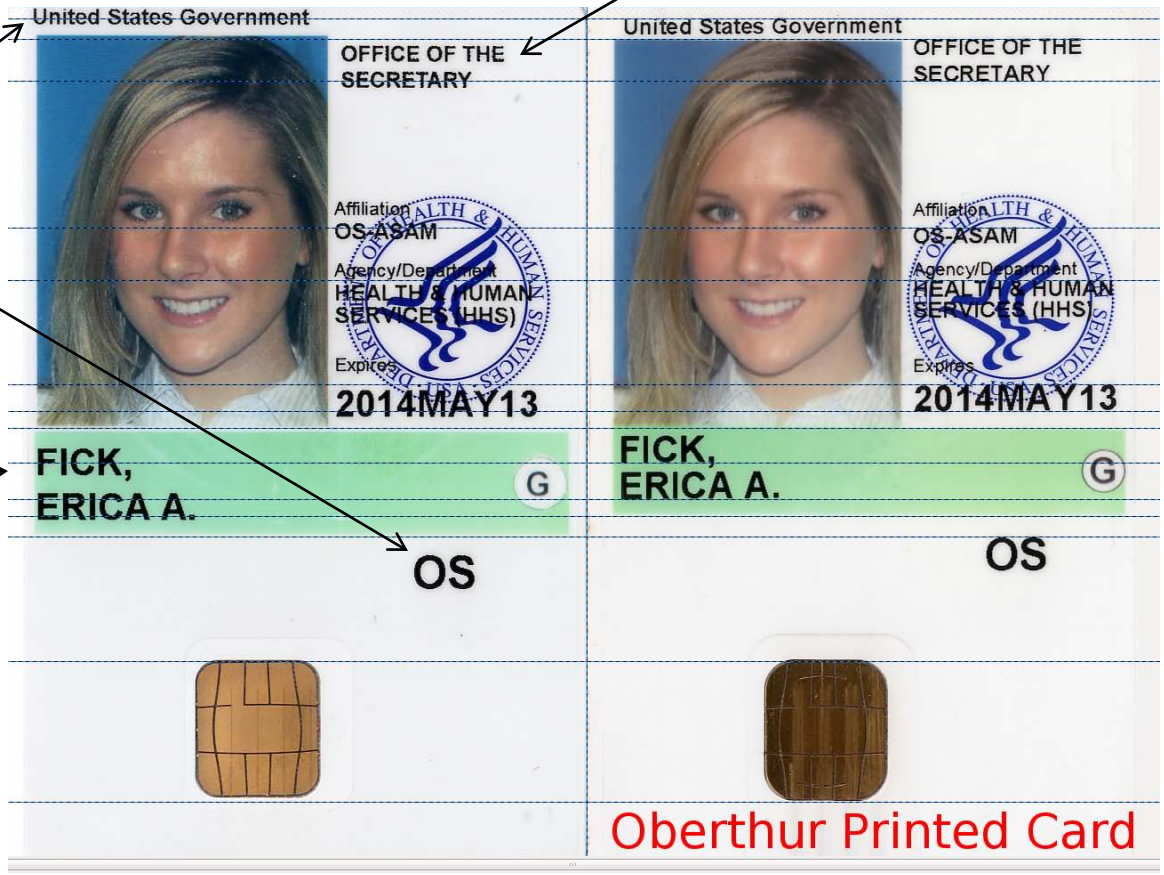
Locally printed card

Vertical Spacing and Alignment

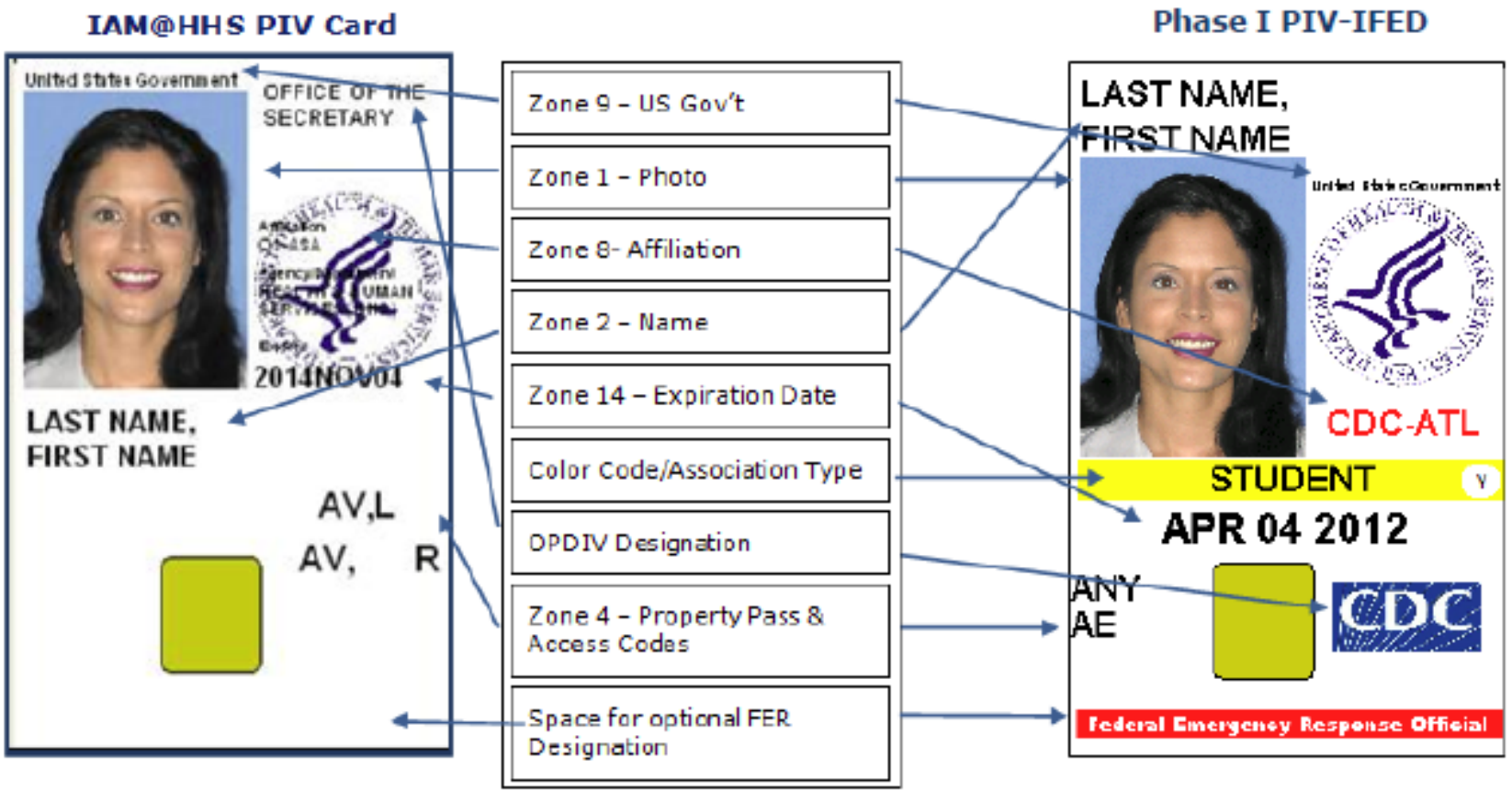
OPDIV Spacing

Field Alignment

Name Alignment and Spacing



NON-PIV Visual Differences



PHASE I NON-PIV CARD

Phase I

Capability

Standardized smart card for use by populations not eligible for PIV credentials

Use Cases

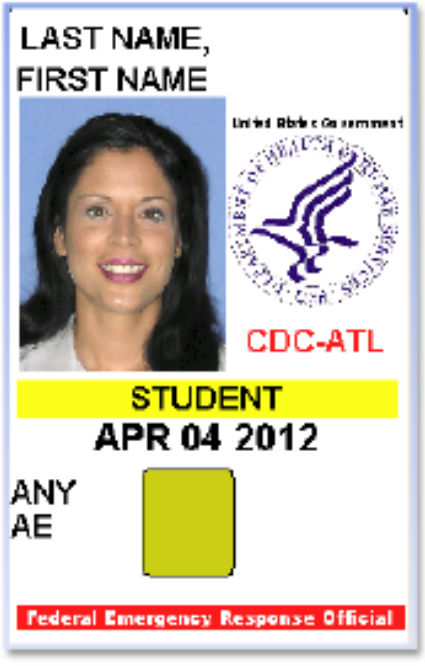
1. **Students** – Individuals who work at an HHS entity for a short period of time, such as during a summer break or break between school terms.
2. **Interns** – Staff hired as part of an Intern program with a known duration of less than 180 days.
3. **Temporary staff** – Staff hired, or contracted, to work for a period of time of less than 180 days.
4. **Visiting Professionals** - Fellows, Medical Staff, Student Doctors or Student Nurses who need access to physical and logical systems (i.e., patient records).
5. **Visiting Staff** - Auditors and visiting scientists, or other visiting staff who, due to the short term nature of their jobs, need immediate access to physical and logical systems.
6. Members of the **Medical Reserve Corps, the National Disaster Medical Service or the US Public Health Service Commissioned Corps** that are detailed to HHS.
7. **Contractors** - Contractors engaged on a contract of less than 180 days.
8. Users who require an HHSID in order to access to systems such as EHRP and EWITS.

Benefits

- Providing smartcards for the PIV-ineligible populations
- Leveraging the existing PIV processes, infrastructure and investments, including the Smart Card Management System and workstations currently in place across the United States.
- Providing a uniform, department-wide approach
- Means to achieve FICAM compliance
- Providing the baseline for future PIV-IFED capabilities

Credential Characteristics

- Leverages current PIV cardstock
- Capable of satisfying Common Policy Identity proofing requirements



Phase I Example

PHASE II NON-PIV

Phase II

Capability

Cardholders that require additional cards with different UPNs and/or SMTPs

Use Cases

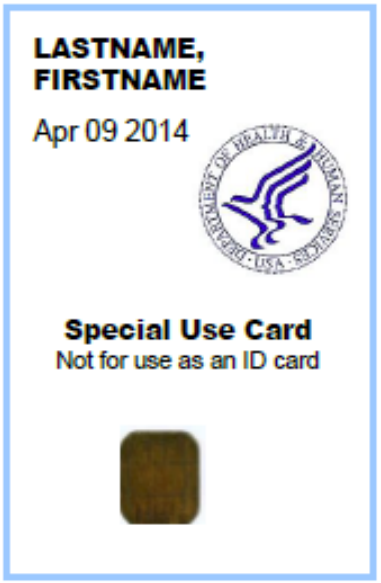
1. **System Administrators** who require more than one logical profile/UPN.
2. Contractors who are associated with more than one OPDIV.
3. HHS Employees of one OPDIV who are detailed to, or work part-time for, another OPDIV.

Benefits

- Addresses key cardholder business requirements for use of additional profiles
- Means to reduce user password-based access
- "Parent-child" relationship with PIV record can enhance security
- Leverage PIV processes and data across OPDIVs

Credential Characteristics

- PIV interoperable smart card.
- Capability limit to "needed" certificates (e.g., if used solely for authentication, only contains authentication certificate)
- Certificate lifetimes match certificates on primary card.
- May be directly requested by card holder after smart card authentication



Phase II Notional – for Illustrative Purposes Only

PHASE III NON-PIV

Phase III

Capability

Cardholders that require additional cards with the same UPN

Use Cases

1. **Specialized laboratory environments** where objects cannot be freely moved in or out of the laboratory.
2. PIV card has been **lost, stolen or damaged** and who need immediate access to HHS physical and/or logical resources.
3. High priority PIV-cardholders who must minimize the time without access to their logical resources due to a damaged or forgotten PIV card.
4. Multiple login sessions using a single logical identity (i.e., Issuer Role Holders).

Benefits

- Reduce wait time for replacement cards
- Tool for highly-restrictive facilities/environments

Credential Characteristics

- Email encryption certificate is duplicate of original PIV card
- Issuer specified badge/certificate lifetimes that may be limited to a few days.
- Certificate lifetimes match certificates on primary card.
- May be directly requested by card holder after smart card authentication

Phase III Notional – for Illustrative Purposes Only