AMENDMENT #2
FOR
ITB NUMBER ACQ04001

DATE AMENDMENT ISSUED: March 18, 2004

The state of Ohio, through the Department of Administrative Services, Information Technology Governance Division, for the Department of Public Safety, is issuing this amendment for the Invitation to Bid entitled:

BMV Drivers License and Identification Card Printer ITB

DATE ITB ISSUED:	**February 9, 2004**
OPENING DATE:	****March 4 30, 2004****
OPENING TIME:	**11:00 A.M.**
OPENING LOCATION:	**Department of Administrative Services** **IT Governance Division Bid Room** **30 East Broad Street, 40th Floor** **Columbus, Ohio 43215**

The attached pages represent the Invitation to Bids (ITB) amendment for the ITB listed above. Please use replacement pages contained in this document to replace the page(s) previously issued by the State.

Specifications and requirements that have been revised are surrounded by double asterisks, bold type and when applicable, strikethrough.

Each DL/ID card must be of such material and design to prevent its reproduction or alteration without being readily detected. The State has selected several security features from those listed in the *Personal Identification – AAMVA International Specification – DL/ID Card Design* dated 09/25/2003. The common security element, as prescribed by AAMVA, must be included in Zone 4 of the card.

- For driver license documents, the background color of Zone 1 of the card must be predominantly pink and the color of the background, which may be a printed image, must be matched as closely as possible to a 30% tint of Pantone reference 198. This is a specific requirement of ISO/IEC CD 18013-1 for ISO compliant driver licenses.

- For non-driver license identification card documents, the background color of Zone 1 of the card must be predominantly green and the color of the background, which may be a printed image, must be matched as closely as possible to a 30% tint of Pantone reference 368.

- The reproduction of the portrait of the holder of the license is depicted on the left side on the portrait side of the card as shown by the position of Zone III in Attachment 10.

Additional security features will be included on the card but are not specified here in order to protect the knowledge of all security features. The bidder provided printers, cards, and supplies must be capable of all of the following security features.

Printing

a. Deliberate Errors/known flaws - A feature is purposely made with an intentional mistake known only to the manufacturer or inspection officials.

b. Duplex Patterns - A design made up of an interlocking pattern of small irregular shapes, printed in two colors and requiring very close register printing in order to preserve the integrity of the image.

c. Fine line background (Guilloche pattern) - A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.

d. Fine line foreground - A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.

e. Front to back (see through) register - A design printed on both sides of a card that forms an interlocking image when held to a light source.

f. Ghost Image - Half tone reproduction of the original image that is typically printed in the same area as, and behind, personal data.

~~**g.** Layered printing (on lamination) - Printing separate elements of the secure design on different layers of the laminated card body materials so that no single layer contains all of the security features and the entire product is only apparent after lamination.~~

~~**h.** Micro optical imaging - Text, line art, gray scale images and multi-reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.~~

i. Micro-printing / nano-printing - Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Difficult to duplicate.

~~**j.** Moiré pattern (anti-scan/VOID pattern) - A new pattern formed by the super positioning of two patterns who periodicities are not identical. Security designs can be developed so that a scanner or copier will only display part of the pattern and/or word VOID or COPY appears instead of the pattern.~~

k. Non-standard type fonts - Special type that is not available on the commercial market and is reserved for security card use only.

l. Rainbow printing - A subtle shift of color across a document. Accurately designed patterns cannot be easily copied. It is often used with a fine line or medallion pattern in the background of a card.

m. Security code High-resolution color printing systems print a security code within the body of the color printed photo image. The code can be printed in a non-proportional font that can imbed characters on the edge or bottom of the printed picture.

Inks

a. Chemically Reactive - Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.

b. Infrared fluorescent - Forms a visible image when illuminated with light in the infrared / red visible part of the spectrum.

c. Infrared dropout - Forms a visible image when illuminated with light in the visible part of the spectrum, but cannot be detected in the infrared region.

d. Metallic, pearlescent, and iridescent - Inks that fluctuate in brilliance depending on the angle of illumination of the viewing. Difficult to mimic the luster and hard to copy or scan.

~~**e.** Metameric - The use of a pair of ink colors that differ in spectral composition but match one another under certain lighting conditions. Under incandescent light that may appear the same, but under colored light they appear as different colors.~~

f. Optically variable (color shifting) - This overt security ink can be printed as a semi-transparent or opaque color shifting security feature. Advanced multi-layer light interference structures create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc.

~~**g.** Phosphorescent - Contains a pigment that glows when exposed to a light source of appropriate wavelength. The reactive glow decays after the light source is removed.~~

h. Tagged - Contains taggants or compounds that are not naturally occurring and that can be detected using special equipment that reacts to electromagnetic energy identifying the grouping or type.

~~**i.** Thermochromatic - Ink that exhibits a sharp, reversible color change when exposed to heat, i.e., finger rubbing or hot air.~~

j. Ultraviolet fluorescence - Invisible inks that emit visible color under exposure to ultraviolet light. Colors can be formulated that are not commercially available, making resistance to counterfeiting higher.

Substrate Inclusion

a. Core inclusion - The manufacture of card stock with different layers. A colored core material may be placed inside to create a colored edge along the card.

b. Embedded thread, fiber or planchette - Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided.

c. Opacity mark - Similar to a watermark, it is a plastic that contains a unique translucent mark.

d. Security bonding - The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.

e. Ultraviolet features - Card bodies are made UV dull or possess a controlled response to UV light so they exhibit fluorescence that can be distinguished in color from the “blue” used in commonly available fluorescent materials.

Optically Variable Devices

a. De-Metalized OVD - A combination of metal and transparency on the same foil or laminate. High-resolution OVD has selective de-metallization, either transparent or opaque, as defined above.

b. Non-transparent OVD - Printed opaque, OVD's advanced multilayer light interference structures create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. similar to what is seen on many global identification documents including driver licenses, banknotes, passports, and visas. The color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications.

c. Personalized OVD - OVD that is personalized for each card based upon biographical data, portrait, or signature of the cardholder.

d. Transparent OVD - Printed on transparent lamination overlay material, advanced multilayer light interference structures create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. When incorporated into a driver license design, feature will not interfere with photo or data information. Transparent OVD color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications, i.e., driver licenses, passports, visas, etc. The OVDs are digitally mastered and created using computer-guided lasers or electron beams.

Additional Features

a. Biometric feature (template) - A biometric template of the customer’s physical characteristics.

b. Covert variable pixel manipulation - Covert dot matrix images that are converted to visible text with a special reader or lens.

c. Digital Seal - A method of securing and validating data by electronic means using digital signature technology. The issuing authority "signs" the information contained in the Machine Readable Technology (MRT).
d. Embedded Image (e.g., digital watermark) - An image or information that is embedded or encoded within a primary visual image.
e. Laminates (security) - Transparent layers or films with an integrated security feature(s) are applied to the card with an adhesive or fused by heat. Available in a number of forms, security laminates are designed to be tamper evident and carry other security features to the card.
~~f. Laser encoded optical image - Image and text files are placed to an optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions.~~
~~g. Laser engraving - The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photos, characters, bar codes, OCR, etc.~~
~~h. Laser perforation - Holes are made with the laser beam of images or objects. The image is visible when held up to a light source. It has a tactile feel with conical holes that are larger at the entrance than exit.~~
i. Machine-readable technology (MRT) - Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other information.
~~j. Magnetic media fingerprinting - Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.~~
~~k. Optical media fingerprinting - Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.~~
~~l. Optical watermark - Fine line images that are engineered into optical WORM medial with a very high resolution (12,000 dpi). The watermark is overwritten with a laser-encoded optical image, locking together a preformatted document security feature with a laser encoded personalization security feature.~~
m. Overlay - An ultra-thin film or protective coating that may be applied to the surface of a card in place of a security laminate and which may contain optically variable features.
n. Overlapping data - Variable data, such as digitized signature, seals or text can be placed over another field such as a photo image. Both fields must be altered if a substitution is to take place making it more difficult.
o. Redundant data - Display of data in more than one location on the card. A visual inspection may determine if all of the fields match. Usually, the data is displayed in a variety of colors and fonts to further deter alteration.
~~p. Retro reflective device - Optical constructions that reflect light such that covert logos become visible over the entire document when viewed using a focused light source or retro reflective viewer.~~
q. Security threads - Metal or plastic, these threads are seen on currency. With special metallized film, demetallized text is invisible in reflected light and therefore is difficult to copy. When viewed in transmitted light, the opaque aluminum letters are clearly visible.
r. Thin film interference filters - Multiple layer structures that produced color effects by interference.
~~s. Tactile feature- A feature which is apparent to touch or feel without requiring a special instrument. This could include texture, flexibility, or weight of the document and/or a feature incorporated in the card structure or card components.~~

2.4.2 Two-Dimensional Barcode

The PDF417 symbology (see ISO/IEC 15438 *Automatic Identification and Data Capture Techniques - International Two-dimensional Symbology Specification - PDF417*) must be used for the Driver's License and Identification Cards. The following PDF417 symbology variants as defined in the ISO/IEC 15438 *Automatic Identification and Data Capture Techniques - International Two-dimensional Symbology Specification - PDF417* must NOT be used.

- Compact PDF417
- MicroPDF417
- MacroPDF417