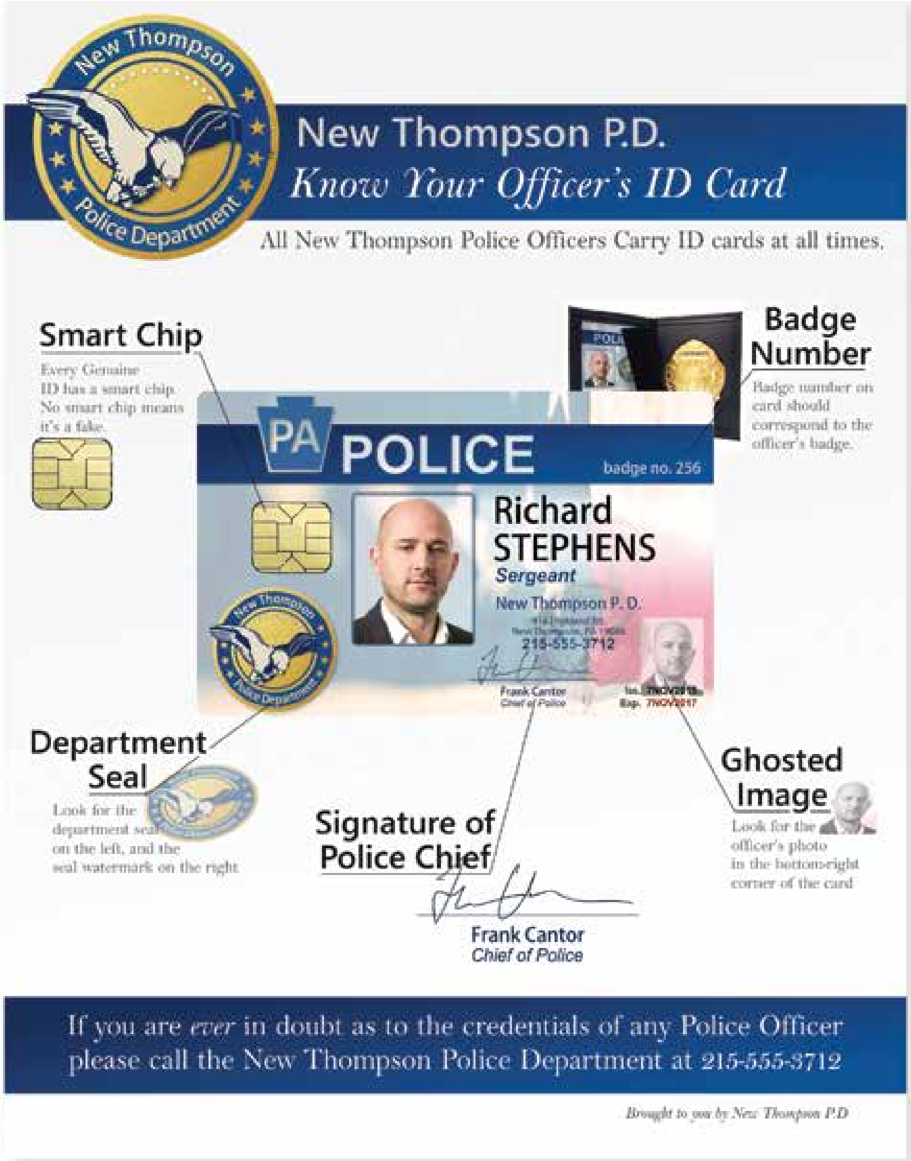
Eight Tips for Designing and Using Smart ID Cards for Police Officers


New Thompson Police Department
New Thompson P.D.
Know Your Officer's ID Card
All New Thompson Police Officers Carry ID cards at all times.
Smart Chip
Every Genuine ID has a smart chip. No smart chip means it's a fake.
Badge Number
Badge number on card should correspond to the officer's badge.
PA POLICE
badge no. 256
Richard STEPHENS
Sergeant
New Thompson P. D.
215-555-3712
Frank Cantor
Chief of Police
Department Seal
Look for the department seal on the left, and the seal watermark on the right
Signature of Police Chief
Frank Cantor
Chief of Police
Ghosted Image
Look for the officer's photo in the bottom-right corner of the card
If you are ever in doubt as to the credentials of any Police Officer please call the New Thompson Police Department at 215-555-3712
Brought to you by New Thompson P.D

By David Allen, Head of User Experience, and David Finkelstein, President, InstantCard

In an era of skilled fraudsters and hackers, police executives everywhere face growing security challenges. One of the most basic challenges is ensuring that officers' photo ID cards cannot be forged or falsified. Swindlers today have access to advanced computer and printer technology, so it's crucial to include security features that make ID card falsification virtually impossible. The public should have complete confidence that when an officer—especially a plainclothes or off-duty officer—shows an ID card, it can be readily verified as genuine.

Police departments also need to strictly control who can access departmental computers, mobile data terminals (MDTs), and facilities. In addition, departments need to store emergency medical information in a place easily accessible to an EMT who's assisting an injured officer.

The following eight tips for secure and useful ID cards can ensure that officers' cards meet all of these needs.

Make the ID cards "smart."

A smart card is a secure ID card that has a tiny, embedded chip. The card connects to a card reader either by direct physical contact or through a short-range wireless connection, typically radio-frequency identification (RFID).

Smart card technology is designed to offer the highest security and more functionality. Smart cards are extremely secure and are useable for a myriad of applications, such as opening locked doors and signing on to electronic systems.

A smart police ID card must

- be virtually impossible to forge or falsify;
- instill confidence in anyone to whom it is presented; and
- control access to sensitive areas or computer data.

For high-level security, a smart card allows a department to use two-factor authentication to identify officers and personnel. It's called "two-factor" because there's typically a private key stored in each card and a public key that is available to anyone. These keys are unique to each ID card. When an officer presents a smart ID card as proof of identity, the mathematics of private and public passwords can confirm that the card is indeed the original. The card is not falsifiable because there's no way for anyone to counterfeit or know the card's private key.

This high-level identity verification may be used for the department's access control. For instance, police ID cards can be used to grant computer or MDT access and access to secure areas within the department. This creates a record of each login or entry that can be reviewed if there's ever a question about who has accessed sensitive areas.

Smart cards also provide digital signatures with every exchange, which are far more secure than passwords.

Many facilities, computers, and networks are already set up to accept smart cards to control user access. However, police departments require particularly secure programs to implement smart card technology. Qualified systems integrators can install the appropriate software to securely enable these advanced functionalities.

Put the chief's signature on the card.

A signature is not easily forged. The agency executive's signature on the card adds greater credibility to the ID card program.

Add a "ghosted" image.

For even greater security, add a second faint photo of the officer on the ID card. It's "ghosted" because it's the same as the main photo of the officer—just smaller and fainter. A ghosted image prevents someone from simply pasting their photo onto a genuine ID.

Alert the community about the ID program via posters, the web, social media, and other publicity avenues.

People should know when they are or aren't seeing an authentic ID. Officers' ID cards should immediately instill confidence when officers are verifying their identities to civilians. Making sure that people in the jurisdiction know exactly what to expect when an officer's ID is displayed provides a basis for this confidence.

A poster highlighting security features is a good start to familiarize the community with the ID security measures. The content from the poster can be used on the agency's website and reposted on Facebook and Twitter. Agencies can also send a press release and graphics to the local newspaper and other local media about the secure ID card program.

Prevent tampering by overlapping variable data.

"Variable data" are data found on the ID card that change from card to card. One variable field can be overlapped with another, such as a photo. This increases security for several reasons. If one of the overlapping fields is altered, the other must be too. This prevents someone pasting a different photo over the ghosted image, for instance.

The chief's signature and departmental seal are not variable, but the badge number and the officer's photo *are* variable. Having a large badge number on the card makes it easier for those checking the card to match up the number on the card with the badge on the officer. The officer's signature and the ghosted image are two more variables to overlap for greater security.

Include a 24/7 phone number.

The ID card should include a phone number that can be called 24/7 to verify the officer's identity. This should be the same number listed on the "know your officer's ID card" posters.

An address not only reminds people that the police are just around the corner, but also aids in the return of lost IDs. It's recommended to put the address and phone on the front of the card—anyone requesting to see an officer's ID should be able to immediately see the department's phone number.

Put supplemental information on the back of the card.

The back of an officer's ID card is a great place for additional information that doesn't need to be seen immediately or doesn't fit on the front of the card. Additional information gives further proof of an officer's identity, especially in unusual situations. Identifying information can include sex, age, hair color, height, and weight. Optionally, the card can list the officer's blood type, which could be lifesaving information in an emergency.

Agencies may wish to add a quick response (QR) code to the back of their cards. A QR code on the card can be scanned by a phone and linked to a database of the officers' personal emergency medical information. Besides the blood type, the EMT could view items like allergies, name of the officer's physician, and information about the police agency.

Include the agency's seal.

It may seem obvious to include the agency's seal, but there are a lot of police departments that have only text identifying the department. It should be absolutely clear that the ID is associated with a specific police agency. If there isn't a seal, it may be too easy for someone to use a generic police ID card to impersonate an officer. For further security, also add a watermark of the seal.

While the front of the card should be in color, it's fine to use black and white for the back of the card. Color isn't really necessary here and adds cost.

While smart cards are virtually unfalsifiable, it's still important to remember that officers' ID cards must instill confidence in the community. Besides boosting security and functionality, these eight best practices make it very easy for civilians to know if they are looking at a genuine ID.

Police leaders running agencies of all types and sizes are increasingly choosing to add smart technology to their officers' ID cards. The gain in security and functionality is well worth the modest additional cost. ❖

David Allen is head of user experience at InstantCard. Mr. Allen has an MS in mathematics and is an expert on the technical aspects of ID cards, including smart card technology. He can be reached at dallen@instantcard.net.

An expert on photo ID cards and smart cards, **David Finkelstein** is president of InstantCard (www.instantcard.net), a leading online provider of photo ID cards and credentialing services based in Rockville, Maryland. He can be contacted at 301-216-3846 or dfinkelstein@instantcard.net.