ISSUED:

2026MAR02

PRODUCED BY:

SCDWG

SIA Credential Design
Working Group

CORPORATE CREDENTIAL DESIGN GUIDE

SIA
SECURITY INDUSTRY ASSOCIATION

Recommended Practices for the Design and Implementation of Credentials and Badges By Corporate Security Teams: Covering Physical Credentials, Identity Verification, Badge Production, Data Security, Counterfeiting Protection, Technology Options and More.

Produced by: **SIA Credential Design Working Group**

Table of Contents

Corporate Credential Design Guide

1 Executive Summary

Corporate identity credentials are foundational elements of modern enterprise security. They enable access to buildings, systems and services, while also representing organizational identity and supporting workforce mobility. Yet today's corporate credential ecosystem is fragmented, inconsistent and increasingly vulnerable to new forms of attack. These guidelines establish a unified, vendor-neutral framework for designing secure, interoperable and user-friendly corporate credentials.

These guidelines establish a unified, vendor-neutral framework for designing secure, interoperable and user-friendly corporate credentials.

1.1 The Challenge

Organizations currently operate with non-standardized badge formats, inconsistent identity proofing, weak counterfeit protections and fragmented mobile solutions. Employees frequently expose badges online, making visual cloning trivial. Legacy proximity technologies remain widespread and are easily replicated with low-cost hardware. Mergers, shared campuses, contractors and mobile access exacerbate interoperability issues. Without unified guidance, organizations risk operational inefficiencies, social engineering attacks and misaligned security controls.

1.2 The Solution

This document defines a comprehensive set of best practices covering the entire credential life cycle:

1. Identity Proofing and Issuance Governance

Credentials must be tied to verified identities. Aligning with National Institute of Standards and Technology (NIST) SP 800-63 principles improves trustworthiness by establishing standardized proofing, enrollment, audit, renewal and revocation processes.

2. Credential Topology, Design and Accessibility

Consistent placement of photos, names, roles and expiration dates improves verification speed and reduces errors. Visual design must balance branding with readability, accessibility (aligned to WCAG/ADA principles) and operational clarity. Photos should follow International Organization for Standardization (ISO)-compliant capture guidance to support recognition under varied conditions.

3. Printing, Materials and Durability

Organizations should understand the capabilities of direct-to-card, retransfer, laser and inkjet printers and select robust materials (composite, polycarbonate, Teslin) based on credential life cycle and security needs. Accurate barcode and QR printing require high-resolution, durable print technologies.

4. Usability and Human Factors

Clear "Tap Here" indicators, consistent layouts and simplified role displays reduce user confusion and security friction. Designs must account for guard validation workflows, low-light conditions, long names, mobile interactions and multilingual user bases.

5. Security Features and Counterfeit Resistance

A layered security model—including holographic laminates, microtext, UV/IR features, ghost images, redundant data placement and digitally signed machine-readable zones—significantly raises the cost and difficulty of counterfeiting. Control of blank card stock, ribbons and consumables is equally critical.

6. Mobile Credential Convergence

Mobile IDs are the future, but today's landscape is fragmented across vendors and platforms. These guidelines recommend vendor-neutral provisioning workflows, hardware-backed cryptographic binding (Secure Enclave/TPM), phishing-resistant authentication and alignment with ISO/International Electrotechnical Commission (IEC) 18013-5 (mDL) concepts for long-term interoperability.

7. Standards and Interoperability

Adopting consistent field sets, standardized machine-readable zones (signed PDF417/QR), ISO-compliant portrait design and harmonized visual layouts ensures cards work across physical access control system (PACS) ecosystems, shared campuses and multi-vendor environments. This also prepares organizations for mobile and federated identity models.

1.3 Outcome

By implementing these guidelines, organizations gain:

- Stronger resistance to counterfeiting and impersonation
- Consistent, accessible and user-friendly credentials
- Improved interoperability across systems, vendors and facilities
- Scalable support for mobile access and future digital identity ecosystems
- Alignment with global identity standards and zero-trust principles

These guidelines serve as a unified foundation for secure, modern and interoperable corporate credential programs—supporting both today's operational needs and tomorrow's identity ecosystem.

2 Introduction

In today's rapidly evolving enterprise security environment, organizations rely on identification and access credentials as a primary control for protecting people, facilities and information. When these credentials are poorly designed or inconsistently managed, they create friction for users and gaps for attackers.

This document establishes a set of practical design guidelines and implementation considerations for corporate identity (ID) and access credentials. It is intended to support security, facilities, and technology teams in creating credentials that are:

- **Secure**—resistant to cloning, tampering and misuse
- **Usable**—easy to recognize, present and verify in real-world conditions
- **Interoperable**—designed to work across systems, sites and future technologies
- **Manageable**—supported by clear life cycle and governance processes

By defining common principles for the design and management of physical and mobile credentials—and the systems that issue, validate and retire them—this guideline aims to help organizations improve security, reduce operational risk and provide a consistent, predictable experience for cardholders and security personnel.

2.1 Scope

This document will focus on several key areas, including the design and implementation of secure corporate ID and access credentials, the establishment of practical and effective security features and the creation of best practices that balance strong security with ease of use. This document will focus on the topology of a credential, specifically its structural design and the relationships among its physical and logical components. While a credential is composed of both topology and electronic interfaces, only the topology is within the scope of this document. The electronic interfaces, including data exchange mechanisms and communication protocols, are specifically out of scope. This document outlines best practices for designing secure and interoperable credential topologies that strike a balance between security, usability and alignment with relevant industry standards.

These guidelines are intended for a wide range of stakeholders, including security professionals, technology providers, corporate security managers and administrators. By fostering collaboration across these sectors, we aim to ensure the broad adoption of standardized practices and adequately address evolving threats.

2.2 Why Is This Guideline Needed?

The lack of harmonized practices has led to a corporate ID landscape marked by inconsistent security measures, fragmented protocols and a patchwork of proprietary solutions. This not only complicates access management and diminishes the user experience, but also leaves organizations vulnerable to social engineering, AI-assisted counterfeiting and credential misuse, making it challenging to keep pace with emerging threats.

A unified guideline helps organizations adopt a common baseline for credential design, ensuring that credentials are secure, recognizable, interoperable and easier for users and security personnel to understand and verify.

2.2.1 Problem Statement

Without a shared guideline, organizations face:

Inconsistent Security Measures
Different sites and business units implement varying levels of security. Some credentials have strong anti-counterfeiting features; others do not. These inconsistencies create exploitable gaps for social engineers and attackers.

Poor Interoperability
Credentials and readers from different vendors often do not work seamlessly together. This complicates mergers, shared facilities, multi-tenant sites and cross-organization collaboration.

Fragmented User Experience
Employees, contractors and visitors may juggle multiple badges, confusing designs or unclear rules. This friction encourages insecure workarounds, such as tailgating or badge sharing.

Difficulty Keeping Pace With Threats
Without a living, consensus-based guideline, many organizations react to incidents rather than build forward-looking capabilities that address emerging risks such as AI-enabled forgery, credential stuffing and increasingly sophisticated social engineering.

2.2.2 Impact on Organizations

The lack of a unified approach to credential design and life-cycle management directly affects organizational security and resilience:

Increased Vulnerability
Credentials continue to be a primary target for both physical and cyberattacks. Weak, duplicated or poorly managed IDs are a frequent root cause of breaches and unauthorized access incidents.

Regulatory and Compliance Risks
Misaligned practices can lead to gaps relative to frameworks and regulations (e.g., NIST, Federal Information Processing Standards (FIPS), privacy laws). This can expose organizations to legal, financial and contractual consequences.

Operational Disruption and Reputational Damage
Incidents involving credential misuse can interrupt core operations, trigger investigations and erode trust with employees, customers, partners and regulators.

Barrier to Security Convergence and Zero Trust
As organizations move toward integrating physical and logical access (e.g., converged PACS/identity access management (IAM), Zero Trust architectures), inconsistent credential strategies and weak identity foundations become significant blockers and sources of hidden risk.

2.2.3 Objective of This Guideline

This guideline exists to:

- Provide clear, actionable design and process recommendations for corporate credentials
- Promote harmonized practices across sites, systems and vendors
- Support interoperability and future evolution, including mobile and derived credentials
- Help organizations strengthen identity assurance while maintaining usability and respecting privacy
- By adopting a shared framework, organizations can reduce fragmentation, enhance resilience and make it more difficult for attackers—and easier for legitimate users and security staff—to do the right thing.

3 Types of Corporate Credentials

Corporate credentials exist in multiple forms, each designed to support a range of physical and digital access needs. While technology, materials and security features may vary, all credentials should be designed and governed based on consistent principles established in this guideline.

This section provides an overview of the major credential categories used across enterprises today.

PHYSICAL ID CREDENTIALS

- **Employee ID Cards**
- **Contractor or Temporary Credenitials**
- **Visitor Credentials**

3.1 Physical ID Credentials

These are the most common forms of corporate identity and access credentials.

3.1.1 Employee ID Cards

Standardized ID cards are issued to full-time staff for visual identification and access control. Typically include:

- Employee photo, name and role
- Company branding
- Access encoding (radio frequency identification (RFID), near-field communication (NFC), contact or magnetic stripe)
- Security features (holograms, UV reactive designs, microtext)

3.1.2 Contractor or Temporary Credentials

Issued to non-employees requiring limited or short-duration access. Characteristics include:

- Distinct visual design
- Time-bound access rights
- Limited data and fewer privileges
- Clear identification to security personnel

3.1.3 Visitor Credentials

Short-lived badges for guests requiring supervised or low-risk access. Should be:

- Highly visible
- Clearly marked as "Visitor"
- Printed without personal details when possible
- Expirable (e.g., color-changing stickers, time-based indicators)

3.2 Electronic Access Credentials

Used for physical access control and increasingly integrated with cybersecurity systems.

3.2.1 Contactless Smartcards (13.56 MHz)

Include technologies that enable:

- Strong cryptographic authentication
- Multi-application storage (physical + logical access)
- Support for future mobile migration

3.2.2 Proximity Cards (125 kHz)

Legacy technology that remains widely deployed but is inherently insecure due to:

- No cryptographic protection
- Easy cloning and replay attacks
- Transmits static identifiers without authentication
- Widely available low-cost tools that allow cloning

These should be phased out as part of modernization initiatives.

3.2.3 Hybrid or Multi-Tech Cards

Cards incorporating multiple access technologies (e.g., 125 kHz + 13.56 MHz) to support transitional environments. May simplify migration but must be carefully designed to avoid read collisions and user confusion.

ELECTRONIC ACCESS CREDENTIALS

- **Contactless Smartcards**
- **Proximity Cards**
- **Hybrid or Multi-Tech Cards**

3.3 Mobile Credentials

Mobile identity credentials provide access through:

- Smartphone NFC
- Bluetooth Low Energy (BLE)
- Secure elements or wallet-based mobile IDs (Apple Wallet, Google Wallet, Samsung Wallet)

- Vendor developed wallet app for iOS and Android mobile devices

Characteristics:

- Can serve as primary or secondary credentials
- Require strong device binding and secure provisioning
- Reduce reliance on plastic card issuance
- May have privacy or user experience (UX) constraints imposed by platform vendors

Mobile credentials must be designed to preserve parity with physical badge identity, security features and governance.

3.4 Digital and Logical Access Credentials

These credentials support access to information systems and applications.

3.4.1 PKI Certificates/Smartcard Login

Used for:

- Zero Trust–aligned authentication
- Multi-factor login flows
- Access to corporate networks (VPN, VDI)

3.4.2 Derived Credentials

Digital representations of a physical credential stored in a secure element on mobile devices.

3.4.3 One-Time or Limited-Use Tokens

Useful for short-duration contractors, remote users or emergency overrides.

3.4.4 High-Assurance or Specialized Credentials

Certain environments require enhanced protections, including:

- Biometric-enabled smartcards
- Personal identity verification (PIV)/commercial identity verification (CIV)-aligned credentials
- Industry-regulated IDs (SOX, FDA, CFATS, FINRA, etc.)
- Critical infrastructure access credentials

These credentials incorporate advanced validation, cryptography and strict life-cycle controls.

4 Visual Design and Branding Considerations (Topology)

Credential design must strike a balance between branding, usability, accessibility and technical limitations.

Effective credential design must balance corporate branding requirements with the functional and security needs of an identification document. While organizations naturally want badges to reflect their brand identity, design decisions should never compromise readability, usability or the technical performance of embedded access technologies.

4.1 Balancing Branding and Practicality

Branding elements—such as logos, color schemes and design motifs—play a crucial role in reinforcing an organization's identity; however, oversized or visually dominant branding features can interfere with critical components of a credential, including:

- Photo visibility and facial recognition
- Legibility of names, roles and required text fields
- Placement of security features
- Antenna performance and chip read reliability

Marketing and branding teams should participate early in the design process, but their creative choices must remain aligned with the operational realities of card printing technology, badge usage behaviors and security requirements. Credential designers should ensure that:

- Branding does not obscure functional elements
- Layouts maintain consistent positioning of key data fields
- Designs support rapid visual verification by security personnel

A practical, security-first design philosophy ensures badges function effectively across diverse lighting conditions, environments and workflows.

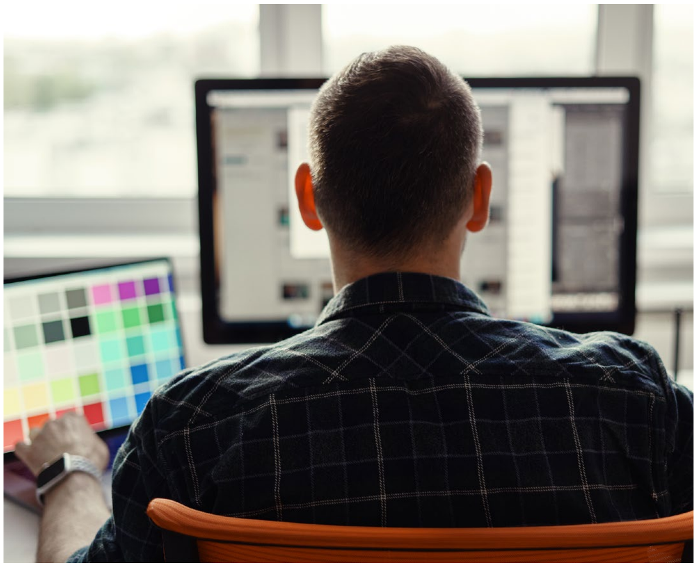
4.2 Color Strategy and Visual Communication

Color plays a powerful role in visual identification, but inconsistent or visually ambiguous color use can lead to confusion or reduced accessibility. Organizations should adopt a structured, standardized approach to color application that supports both branding and operational clarity.

Key recommendations include:

- Use clearly defined spot colors for role designation, department identification or access level categories.
- Ensure color accessibility, particularly for individuals with color vision deficiencies (e.g., avoid problematic pairings such as red/green or blue/purple without accompanying text or iconography).
- Support consistency by applying color coding uniformly across all badge types and business units.
- Pair colors with text or symbols, ensuring that visual cues remain recognizable even when color perception varies.

A thoughtful color strategy enhances usability, supports accessibility and improves the ability of security personnel to interpret badge information quickly.



4.3 Security Awareness in Badge Design

While visual design and branding are essential aspects of a corporate credential, the most critical design dimension is security. Badge design is not merely an aesthetic exercise—it is a core security function that directly influences an organization's exposure to social engineering, unauthorized access and credential misuse.

Modern attackers increasingly exploit human behavior, oversharing on social media, and advances in image replication to reproduce corporate badges with alarming accuracy. As a result, the design of corporate credentials must include intentional and measurable security protections that help prevent forgery, misuse and unauthorized entry.

4.3.1 Security as a Primary Design Requirement

Corporate badge design must incorporate visual and structural elements that support:

- **Rapid verification by security personnel:** Features must help security recognize legitimate credentials quickly—even in busy or low-light environments.
- **Resistance to counterfeit reproduction:** Designs should incorporate layered security features (e.g., microtext, UV elements, holograms), which are significantly harder for adversaries to replicate using readily available tools.
- **Mitigation of image-based spoofing:** Because employees often unintentionally expose their badges in photos posted online, designs should minimize elements that can be easily duplicated from a photograph.
- **Operational clarity:** Information must be placed consistently and clearly to reduce ambiguity during inspections.

4.3.2 The Human Element: Behavior Amplifies Risk

Even the most technically secure credentials are vulnerable when users behave insecurely. Common examples include:

- Displaying badges prominently on social media posts
- Posting selfies with ID cards visible
- Wearing badges publicly outside secure environments
- Photographing badges for internal communications or team events

Given the availability of artificial intelligence (AI)-driven image enhancement and printing tools, attackers can quickly reconstruct a badge from high-resolution photos posted online.

Therefore, security-aware badge design must:

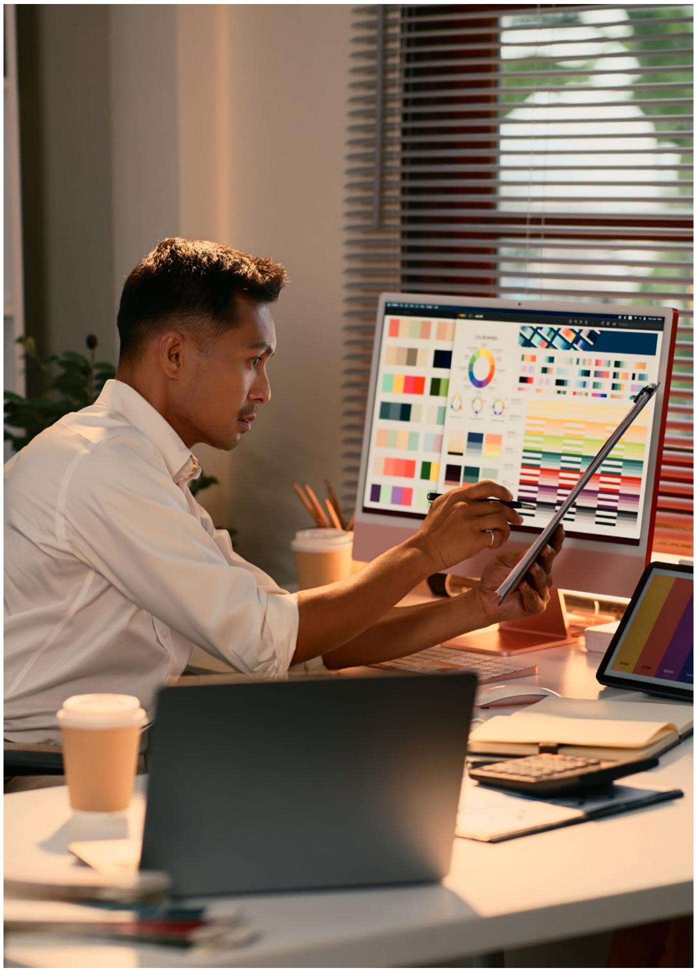
- Limit unnecessary personal data printed on badges
- Incorporate security features that degrade when photocopied or photographed
- Use designs that reduce replicability from a flat image
- Include employee education on safe badge handling

4.3.3 Security Features Belong in the Design Phase, Not as an Afterthought

Security safeguards should be considered at the beginning of the design process—not added late or inconsistently. Credential programs should:

- Integrate a multi-layered security approach involving visible, hidden and forensic elements
- Collaborate with physical security, IT security and risk management teams from the outset
- Ensure design does not weaken or cover critical physical or technical features
- Avoid overly complex visual layouts that make security inspection more difficult

An effective badge balances branding, usability and security—but security remains the non-negotiable foundation on which all other design choices should be built.



4.4 Importance of Marketing in Badge Design

Corporate credentials serve many operational and security functions, but they also act as a daily, visible extension of the organization's brand. For this reason, the marketing team plays an essential role in badge design—provided that branding decisions are balanced with security, usability, and printing constraints.

4.4.1 The Badge as a Brand Artifact

Employee ID cards are one of the most widely used and widely seen branded objects within an organization. They:

- Reinforce corporate identity internally
- Support culture and belonging among employees
- Serve as a visible representation of the organization at conferences, client sites and public spaces
- Provide a consistent and recognizable visual identity across locations

This makes branding considerations legitimate and necessary; however, marketing must design within the constraints of a security credential, rather than treating the badge as a promotional item.

4.4.2 Early Engagement Prevents Rework and Delays

Marketing should be involved at the beginning of the badge design process. Early engagement ensures:

- Alignment with brand guidelines
- Proper color usage and typography
- Reduced back-and-forth between teams
- Faster approval and rollout cycles

When marketing is brought in too late, organizations often encounter:

- Delays in badge production
- Designs that must be reworked because they obscure security features
- Badges that do not meet printing or durability requirements
- Internal dissatisfaction with the final design
- A collaborative approach ensures a badge that satisfies both brand identity and security stakeholders.

4.4.3 Branding Must Respect Technical Constraints

Badge printers, substrates, and embedded technologies impose fundamental limitations. Marketing teams must account for:

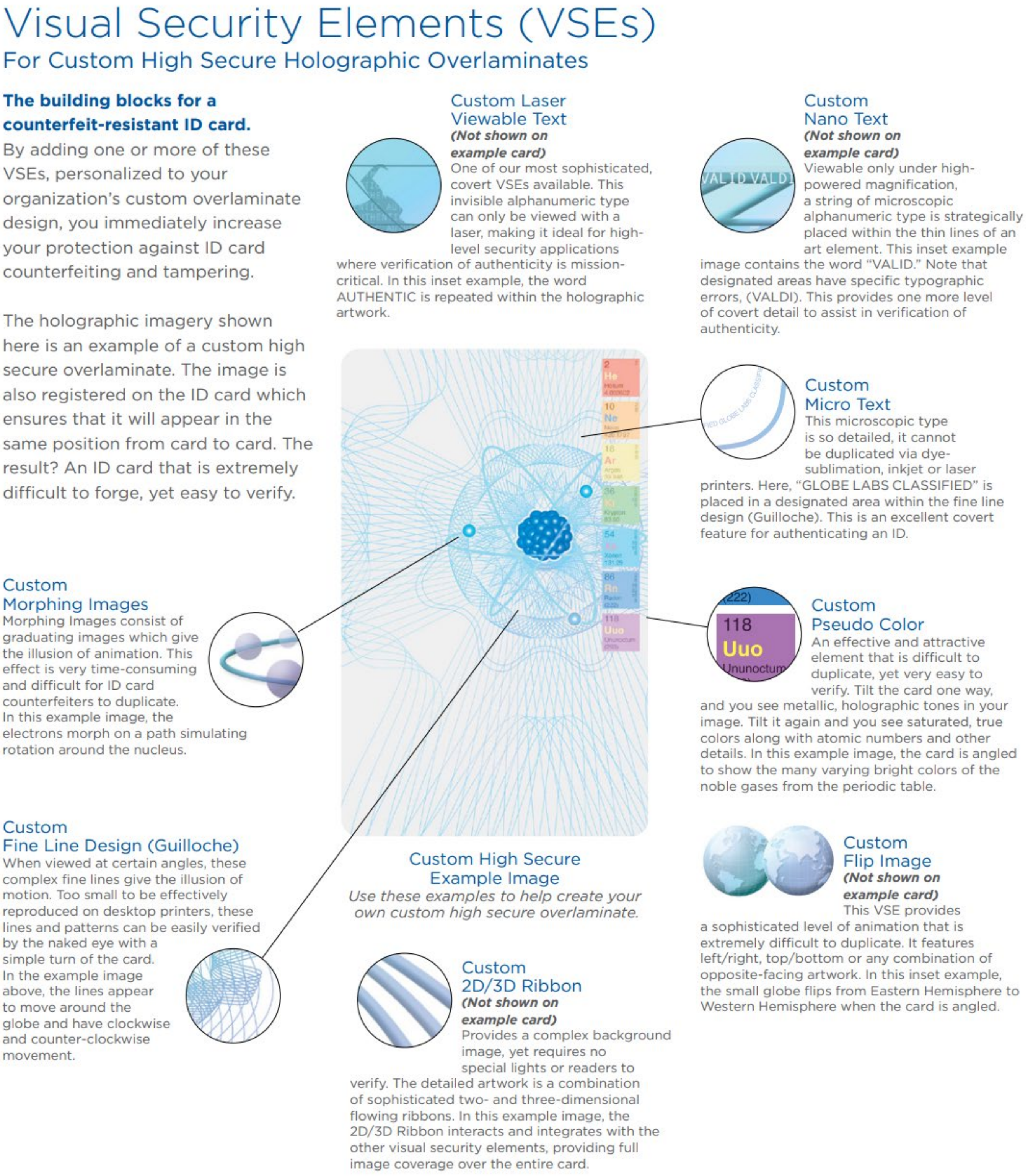
- Print resolution and color reproduction limits
  - o (especially on CMYK-based dye-sublimation and retransfer printers)
- Hardware considerations, such as:
  - o Antenna location
  - o Chip placement
  - o Lamination zones
  - o Punched-slot "no-print" areas
- Security feature placement, which may require certain areas to remain unobstructed

Creative elements must be adjusted to accommodate these technical realities rather than attempting to override them through design.

4.4.4 Situational Awareness and External Display Risks

While the badge serves as a branding tool, it also functions as an identity document that may be visible outside secure facilities. Marketing should collaborate with security teams to ensure designs:

- Avoid unnecessary personal information
- Minimize risk if a badge is photographed or lost
- Use designs that reveal minimal exploitable details when displayed publicly



Visual Security Elements (VSEs)

For Custom High Secure Holographic Overlaminates

The building blocks for a counterfeit-resistant ID card.

By adding one or more of these VSEs, personalized to your organization's custom overlaminate design, you immediately increase your protection against ID card counterfeiting and tampering.

The holographic imagery shown here is an example of a custom high secure overlaminate. The image is also registered on the ID card which ensures that it will appear in the same position from card to card. The result? An ID card that is extremely difficult to forge, yet easy to verify.

Custom Morphing Images

Morphing Images consist of graduating images which give the illusion of animation. This effect is very time-consuming and difficult for ID card counterfeiters to duplicate. In this example image, the electrons morph on a path simulating rotation around the nucleus.

Custom Fine Line Design (Guilloche)

When viewed at certain angles, these complex fine lines give the illusion of motion. Too small to be effectively reproduced on desktop printers, these lines and patterns can be easily verified by the naked eye with a simple turn of the card. In the example image above, the lines appear to move around the globe and have clockwise and counter-clockwise movement.

Custom Laser Viewable Text

(Not shown on example card)

One of our most sophisticated, covert VSEs available. This invisible alphanumeric type can only be viewed with a laser, making it ideal for high-level security applications where verification of authenticity is mission-critical. In this inset example, the word AUTHENTIC is repeated within the holographic artwork.

Custom High Secure Example Image

Use these examples to help create your own custom high secure overlaminate.

Custom 2D/3D Ribbon

(Not shown on example card)

Provides a complex background image, yet requires no special lights or readers to verify. The detailed artwork is a combination of sophisticated two- and three-dimensional flowing ribbons. In this example image, the 2D/3D Ribbon interacts and integrates with the other visual security elements, providing full image coverage over the entire card.

Custom Nano Text

(Not shown on example card)

Viewable only under high-powered magnification, a string of microscopic alphanumeric type is strategically placed within the thin lines of an art element. This inset example image contains the word "VALID." Note that designated areas have specific typographic errors, (VALDI). This provides one more level of covert detail to assist in verification of authenticity.

Custom Micro Text

This microscopic type is so detailed, it cannot be duplicated via dye-sublimation, inkjet or laser printers. Here, "GLOBE LABS CLASSIFIED" is placed in a designated area within the fine line design (Guilloche). This is an excellent covert feature for authenticating an ID.

Custom Pseudo Color

An effective and attractive element that is difficult to duplicate, yet very easy to verify. Tilt the card one way, and you see metallic, holographic tones in your image. Tilt it again and you see saturated, true colors along with atomic numbers and other details. In this example image, the card is angled to show the many varying bright colors of the noble gases from the periodic table.

Custom Flip Image

(Not shown on example card)

This VSE provides a sophisticated level of animation that is extremely difficult to duplicate. It features left/right, top/bottom or any combination of opposite-facing artwork. In this inset example, the small globe flips from Eastern Hemisphere to Western Hemisphere when the card is angled.

5 Balancing Branding and Practicality:
Technical Constraints and Printing Technologies

Badge aesthetics must always be grounded in the technical realities of card printing hardware and materials. Many design concepts that appear appealing on screens or in marketing materials cannot be consistently produced—or legibly—on physical credentials. Understanding printer capabilities, substrate limitations and color reproduction constraints is crucial for creating badges that appear professional, function reliably and maintain security integrity.

Effective design requires close coordination among marketing, security, credential operations and printer hardware vendors to ensure that the final product is both visually aligned with the organization's brand and technically feasible at scale.

5.1 Direct-to-Card (DTC) Printers

Direct-to-card (DTC) printers apply dye-sublimation color directly onto the card surface. They are widely used for their affordability and small footprint but come with significant design limitations.

5.1.1 Capabilities

- Lower-cost printers and consumables
- Faster print cycles, ideal for high-volume environments
- Compact size suitable for on-site badging stations

5.1.2 Limitations Design Teams Must Consider

- **Non–edge-to-edge printing:**
  DTC printing leaves a 1–2 mm unprinted border. Designs requiring full-bleed artwork will not render correctly.
- **Surface sensitivity:**
  DTC prints best on smooth, uniform PVC surfaces. Cards containing chips, antennas, or uneven layers may produce inconsistent color or banding artifacts.
- **Lower image precision:**
  DTC prints are visually acceptable but less sharp and vibrant than retransfer printing, especially for detailed logos, gradients or finely textured designs.

5.1.3 Design Guidance for DTC-Compatible Badges

- Avoid full-bleed backgrounds or borderless designs
- Use simplified, high-contrast graphics
- Ensure critical text is not positioned near print edges
- Consider pre-printing complex branding elements via offset printing if consistency is required

5.2 Reverse Transfer (Retransfer) Printers

Reverse transfer printers produce higher-quality, more durable cards by printing on a transparent film and then heat-fusing it to the card surface.

5.2.1 Capabilities

- **True edge-to-edge printing:**
  Artwork can extend fully to the card's border without white edging.
- **Superior image quality:**
  Richer colors, sharper lines and more consistent gradients.
- **Works on uneven or technology-heavy cards:**
  Ideal for proximity cards, smartcards and contactless credentials where embedded components create an uneven printing surface.

5.2.2 Limitations

- Higher printer and consumable costs
- Slower print cycles
- Larger physical footprint

5.2.3 Design Guidance for Retransfer-Compatible Badges

Better suited for:

- Strong brand color reproduction
- Detailed imagery, gradients or fine-line artwork
- Complex visual designs that demand consistency

Designers should still account for:

- Lamination zones
- Slot punch interference
- Heat-induced material variation when combining overlays with film layers

Retransfer printing is recommended for organizations prioritizing durability, brand fidelity and high-assurance card technologies.

5.2.4 Equipment Assessment: Printing and Encoding Technologies

Different credential designs require different print and encoding technologies. Printer capability should match card material and security requirements.

5.2.4.1 Printing Technologies

Direct-to-Card (DTC)

- Resolution: 300 DPI
- Pros: Fast, low-cost, suitable for PVC or smooth surfaces
- Cons: Bordering, weaker color accuracy, poor performance on uneven card bodies (smartcards)

Retransfer Printing

- Resolution: 300 DPI or 600 DPI
- Pros: Edge-to-edge printing, excellent color, ideal for uneven surfaces or embedded chips
- Cons: Higher cost per card, slower throughput

Laser Engraving

- Resolution: 600 DPI
- Pros: Highly tamper-resistant, excellent for long-life cards (PC/Teslin)
- Cons: Requires polycarbonate or compatible material; expensive

Inkjet

- Resolution: 1400 DPI
- Pros: Very high image quality; environmentally friendly technologies are emerging
- Cons: Requires special card stock; limited adoption in high-security credentialing

5.2.4.2 Encoding Requirements

Encoding processes must ensure proper data integrity.

Contact Chip Encoding

- Must maintain contact for at least 60 seconds
- Consistent pressure and stable connectivity are required

Contactless Encoding (RFID/NFC)

- Maintain a stable field connection for at least 60 seconds
- Avoid interference from metal surfaces or nearby antennas
- Verify programming post-encoding to prevent partial writes

5.3 Additional Considerations for Printer-Aware Design

5.3.1 Hardware Constraints That Affect Design

- Antenna inlays
- Contact chip modules
- Die-cut punch zones
- Lamination patch alignment
- Magnetic stripe placement

5.3.2 Barcode and QR Code Printing Issues

Credential validation often depends on machine-readable zones, so barcode clarity is essential.

Known Issues

- Low DPI may distort small bars or dots
- Misalignment from DTC edge borders
- Ink bleed on PVC cards
- Reflective surfaces complicate scanning

Recommendations

- Use retransfer or inkjet printing for higher barcode accuracy
- Apply matte laminate over machine-readable zones
- Validate with multiple scanners before issuing
- Use certified symbology's such as PDF417 for critical data

Proper printing ensures reliable on-site and mobile scanning performance.

5.3.3 Designer Checklist

Before finalizing design, teams should:

- Confirm printer model capabilities
- Validate color reproduction in live print tests
- Ensure security features remain unobstructed
- Confirm artwork does not overlap antennas or chip modules
- Test designs across multiple card batches to validate consistency

Card Printing Options

Reverse Transfer/Retransfer Printing

Reverse transfer printers produce higher-quality, more durable cards by printing on a transparent film and then heat-fusing it to the card surface.

Direct-to-Card Printing

Direct-to-card (DTC) printers apply dye-sublimation color directly onto the card surface, but leaves an 1-2 mm unprinted border.

5.4 Lamination

Lamination is a critical component in the durability, security and long-term performance of corporate credentials. While often viewed as an optional enhancement, lamination can significantly improve resistance to wear, environmental exposure and tampering attempts. The choice of lamination—overlay, patch, holographic or custom security layers—should be driven by both the operational requirements of the organization and the security posture needed for the credential type.

5.4.1 Purpose of Lamination

Lamination serves three primary functions:

1. Durability Enhancement

Corporate IDs are handled daily, often exposed to friction, moisture, UV light and bending. Lamination:

- Protects printed artwork from abrasion
- Reduces color fading
- Extends the lifespan of the card surface

2. Security Reinforcement

Lamination layers can embed or overlay security features such as:

- Holographic images or patterns
- Microtext or micro line structures
- Embedded optical or tactile elements
- Tamper-evident layers (tear, void, or distortion effects)

These features increase the difficulty of reproducing or altering a badge using consumer-grade tools.

3. Protection for Embedded Technologies

Smartcards, proximity inlays and contact chip modules benefit from lamination that:

- Reduces surface wear
- Reinforces structural integrity
- Protects against cracking or warping during daily use

This is especially important for retransfer-printed cards, which may contain complex layered substrates.

5.4.2 Types of Laminations

Overlay Lamination: A thin protective film applied during printing.

- Lower cost, lower durability
- Provides basic scratch resistance
- Suitable for low-risk or short-term use cards

Patch Lamination: A thicker, more durable laminate patch applied with heat and pressure.

- More resistant to wear
- Supports embedded holograms
- Provides higher tamper resistance
- Ideal for long-life-cycle cards or environments with elevated security needs

Custom Holographic Lamination: Custom holograms significantly strengthen security by introducing:

- Issuer-specific patterns
- Optical variable devices (OVDs)
- Elements that distort upon copying or scanning

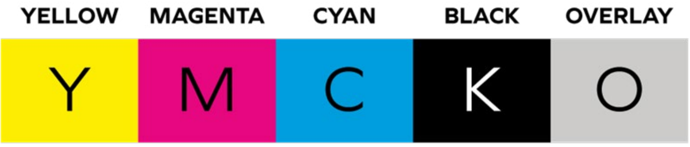
These are difficult for counterfeiters to reproduce without access to specialized manufacturing.

5.4.3 When to Use Lamination

Organizations should consider lamination when:

- Cards must last three or more years
- Credential forgery is a realistic threat
- Cards are frequently exposed to environmental wear
- Branding elements must remain vibrant and protected over time
- Contact or contactless cards require surface protection

Lamination should be included as part of a holistic card security strategy, not as an optional add-on.



5.5 Color Matching and Printing Limitations

Color is a key branding element in corporate badge design, but card printers—unlike professional press equipment—operate under technical constraints that can make perfect color matching difficult. Corporate branding teams often expect precise Pantone or spot color reproduction, but most ID card printers use CMYK dye-sublimation or retransfer processes, which inherently limit color accuracy.

To maintain visual consistency while ensuring realistic expectations, organizations should understand these limitations and account for them early in the design phase.

5.5.1 Why Color Matching Is Challenging

Most corporate badge printers (DTC and retransfer) rely on:

- Four-color CMYK ribbons
- Fixed chemical dyes
- Thermal transfer processes
- Variable substrate characteristics

This means:

- Spot colors cannot be perfectly reproduced (especially saturated or brand-specific colors)
- Color output varies between printer models, card types, heat cycles and ribbon batches
- Background designs with gradients or subtle hues may print unevenly

Even minor variations in card surface texture, laminate type or environmental conditions can alter printed color output.

5.5.2 Best Practices for Achieving Consistent Color

1. Test Print Early in the Design Process

Print prototypes on the exact:

- Printer model
- Ribbon type
- Card substrate
- Lamination process

This helps reveal real-world deviations from digital mockups.

2. Use YMCK-Optimized Color Palettes

Convert brand colors into YMCK values optimized for:

- DTC printers (lighter, less saturated tones)
- Retransfer printers (more consistent and vibrant results)

3. Avoid Large Flooded Background Colors

Large solid-color backgrounds often show:

- Banding
- Variations in density
- Visible print artifacts

Smaller, controlled use of brand color yields better print quality.

4. Pre-Print Complex Elements When Needed

For high-fidelity branding requirements:

- Logos
- Patterns
- Background gradients

Organizations may pre-print these via offset printing at the card manufacturer, then personalize the card onsite.

5. Implement Standardized Color Controls

Define:

- Approved badge color palettes
- Printer calibration schedules
- Ribbon replacement intervals
- Monitoring procedures for color drift

This ensures ongoing consistency, especially in organizations with multiple printing locations.

5.5.3 Setting Expectations with Marketing and Branding Teams

It is essential to communicate early and clearly that:

- Screen colors (RGB) do not match printed colors (CMYK)
- Brand colors may require adjusted values for consistent reproduction
- Final color accuracy depends on card material and laminate finish
- Retransfer printers yield the closest match but still cannot replicate true Pantone output

Managing expectations upfront prevents rework and accelerates approval cycles.

5.6 Accessibility and Color Use

Accessible badge design ensures that all individuals—including those with visual impairments, color blindness or low-vision conditions—can quickly interpret the information on a corporate credential. Because badges function as both identification documents and security tools, accessibility is not only an inclusion requirement but also a safety and operational imperative.

Organizations should intentionally design credentials so that critical identity and access information can be recognized under varying lighting conditions and by users with diverse visual capabilities.

The design of the card should allow for consideration of an individual's "protective characteristics."

For instance, there should be consideration to enable blind/less dexterous individuals to distinguish their building access cards from other (bank) cards with touch identification (e.g., Braille) in terms of making adjustments for use.

5.6.1 Do Not Rely on Color Alone to Convey Meaning

Color can be a helpful visual indicator, but it should never be the only method used to communicate role, clearance or access level.

Recommendations:

- Pair color codes with text labels (e.g., "CONTRACTOR", "VISITOR", "STAFF").
- Use icons or symbols consistently to reinforce meaning.
- Ensure any stripe or color band used for role designation is accompanied by readable text.
- This ensures clarity even for cardholders or security personnel with color vision deficiencies.

5.6.2 Avoid Problematic Color Pairings

Certain color combinations are difficult for individuals with common forms of color blindness—particularly red-green, blue-purple and green-brown pairings.

When selecting color schemes for badges:

- Avoid relying on contrast between these combinations
- Test designs using color-blind simulation tools
- Ensure all essential elements remain distinguishable without color

5.6.3 Maintain Consistent Placement of Key Data Fields

Consistency across badge templates supports faster human recognition and easier security screening.

Best Practices

- Place fields such as clearance level, department or role in the exact same location across all badge types
- Standardize field order, spacing and prominence
- Use consistent iconography for repeated data points

Predictability improves accessibility for all users—not only those with visual impairment.

5.6.4 Ensure Readable Fonts and Adequate Text Size

Readable text is critical for rapid badge inspection under real-world conditions such as:

- Low lighting
- Distance viewing
- Moving crowds
- Security checkpoints

Guidelines

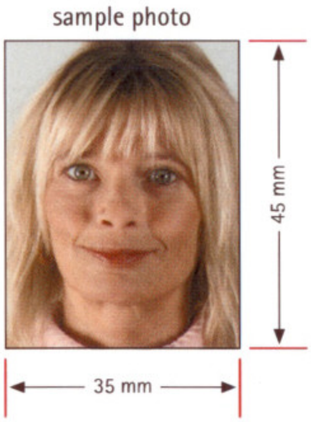
- Use sans-serif fonts for optimal legibility
- Ensure names are printed in a size that is readable from several feet away
- Avoid overly condensed or decorative typefaces
- Maintain WCAG-informed contrast ratios for text against background colors

5.6.5 Use High-Quality Photos to Improve Recognition

Badge photos should support facial recognition under real-world conditions. Poor-quality images reduce badge usefulness—especially for those with low vision.

Recommended Photo Standards:

- High contrast
- Uniform, neutral background
- Proper lighting without harsh shadows
- Clear, unobstructed view of the face
- Adherence to ISO/IEC 19794-5 or ICAO 9303 photo guidelines (optional but strongly recommended)



SOURCE: *ICAO Photo Guidelines*

6 Usability and Human Factors

6.1 Multi-Technology Card Issues

Modern organizations often rely on credentials that support multiple access technologies—such as legacy 125 kHz proximity systems and modern 13.56 MHz contactless smartcard protocols. While multi-tech cards can ease migration between systems, they introduce usability challenges that directly affect user experience, security operations and reader performance.

6.1.1 Common Issues With Multi-Tech Cards

Ambiguous Antenna Placement

Multi-tech credentials frequently contain multiple embedded antenna loops. When antenna placement is not clearly indicated:

- Users "hunt" for the correct tap location
- Reads become inconsistent or delayed
- Security queues slow down
- New users require additional training

Inconsistent or Unpredictable Read Behavior

When multiple technologies share space on a single credential:

- Readers may detect the wrong interface
- Older systems may "win" the read, preventing intended secure protocols
- Read ranges differ between technologies
- Slot punching may damage or detune antennas

User Confusion During System Transitions

If different doors expect different technologies:

- Users present the wrong side of the card
- Access failures occur frequently
- Guards must troubleshoot unnecessarily
- Operational efficiency declines

These frictions often reduce confidence in the access system and increase the rate of workarounds (tailgating, holding doors open, etc.).

6.1.2 Recommended Design Strategies

1. Minimize Multi-Tech Designs Whenever Possible

Multi-tech cards should be transitional, not permanent.

- Prefer a single secure technology for long-term architectures
- Retire legacy 125 kHz systems as soon as feasible (per NIST and industry risk guidance)
- Communicate clearly which interface each door expects during migrations

2. Mitigate Read Conflicts in Hybrid Environments

Where multi-tech cards are unavoidable:

- Configure readers to prioritize secure protocols
- Physically orient antennas to reduce read overlap
- Use technology-specific tap symbols when necessary
- Document expected behavior at each door
- These controls reduce read failures and enhance user experience.

3. Consider adding a Universal "Tap Here" symbol

Directly above the contactless inlay's true center point, print a clearly recognizable tap area. This could reduce hesitation and ensures users present the card correctly the first time.

4. Align Markings With the Antenna—Not the Artwork

The tap symbol should align with the actual antenna loop. Design teams should:

- Request precise inlay placement diagrams from card manufacturers
- Avoid guessing or centering symbols purely on visual design
- Validate placement through test prints and reader trials

6.2 Image and Text Visibility

Clear and consistent visibility of both images and text is essential for security personnel, employees, and automated systems to quickly identify cardholders.

Badge designs must ensure that names, faces and critical information remain readable under real-world conditions including distance, low lighting, movement and variable background environments.

Effective image and text visibility improves security, speeds access control and reduces reliance on manual checks or secondary verification methods.

6.2.1 Photo Visibility Requirements

Badge photos must remain recognizable at commonly encountered distances.

Recommended Standards

- **Recognizable at ~4 feet:**
  Security personnel should be able to confirm that the person wearing the badge matches the photo without requiring close inspection.
- **Use standardized portrait geometry:**
  Adopt ISO/IEC 19794-5 or ICAO 9303 photo guidelines to ensure:
  - Full-frontal orientation
  - Eyes positioned within the correct vertical band
  - Neutral lighting with no harsh shadows
  - High-contrast, distraction-free background

Standardization increases recognition consistency across departments and sites.

6.2.2 Text Legibility Requirements

Names, titles, and organization identifiers must be readable quickly and reliably.

Recommended Standards

- **Names legible from ~8 feet:**
  Based on ADA viewing-distance tables, names should typically use a character height of 0.25–0.35 inches (≈18–25 pt).
- **Maintain strong contrast:**
  Follow WCAG AA contrast guidelines (minimum ratio 4.5:1) for:
  - Names
  - Role/clearance levels
  - Organization name/logo (where applicable)
- **Avoid hard-to-read typefaces:**
  - No italic script
  - No overly condensed fonts
  - No decorative or stylized faces

Readable typography improves both speed and accuracy of visual confirmation.

6.2.3 Production Specifications for Image and Text Quality

Follow Physical Card Standards

- ISO/IEC 7810 ID-1 format for card dimensions
- CMYK print processes require high-contrast design choices
- Ensure all text meets WCAG AA contrast standards

Follow Photo Standards

- ISO/IEC 19794-5 or ICAO 9303 geometry for portraits
- Clear, even lighting
- No patterned backgrounds
- High-quality source images (minimum 5 MP recommended)

6.3 Photo Shape: Square vs. Round

The shape of the photo frame on a corporate credential is more than a stylistic choice—it directly affects facial recognition accuracy, both for human verification and for any automated or semi-automated identity confirmation processes.

Although circular portrait frames are increasingly common in modern graphic design, they offer limited security, remove important facial context and deviate from established identity document standards. Corporate credentials should prioritize recognition, clarity and standard alignment over aesthetic trends.

6.3.1 Why Photo Shape Matters

Credential verification—whether performed by security officers, supervisors or automated systems—depends on the availability of consistent facial features and contextual information such as:

- Head shape
- Hairline
- Shoulders
- Chin angle
- Relative scale of face to frame

Rounded photo frames obscure or eliminate much of this surrounding context, making accurate verification more difficult.

6.3.2 Recommended Standard: Rectangular Image Frames

International identification standards—including PIV, ICAO and ISO/IEC 19794-5—use rectangular or square photo frames for several reasons:

- They preserve head-and-shoulders framing
- They allow accurate scaling and head-size measurement
- They reduce cropping errors
- They provide more reference points for identity confirmation
- They improve usability in low-light or rapid-inspection environments

Following these standards increases consistency across sites and supports long-term interoperability with security technologies.

6.3.3 Issues With Circular or Non-Standard Cropping

Circular portraits, while visually appealing, introduce several problems:

Security Issues

- Reduce the amount of visible contextual facial information
- Increase risk of misidentification during quick visual checks
- Compromise future use of automated facial comparison or recognition tools

Photo Shape: Square vs. Round

Preserves head-and-shoulders framing

Allows accurate scaling and head-size measurement

Reduces cropping errors

Provides more reference points for identity confirmation

Improves usability in low-light or rapid-inspection environments

Square

Round

Reduces the amount of visible contextual facial information

Increases risk of misidentification during quick visual checks

Often cut off shoulders, forehead or chin

Users with longer hairstyles or hats may appear cropped incorrectly

Inconsistent framing across photos reduces overall credential uniformity

Operational Issues

- Circular crops often cut off shoulders, forehead or chin
- Users with longer hairstyles or hats may appear cropped incorrectly
- Inconsistent framing across photos reduces overall credential uniformity

Design Issues

- Circular frames require precise placement to avoid interfering with text or security features
- They may clash with printer resolution or lamination edge boundaries

For these reasons, circular frames should generally be avoided for any high-security or widely used corporate credential format.

6.3.4 When Circular Frames May Be Acceptable

Only extremely low-risk badge types (e.g., event passes, volunteer tags, visitor stickers) may use circular portraits—provided they do not serve as authentication instruments for secure areas.

For all other corporate ID types, rectangular framing remains the best practice.

6.4 Long Names and Character Length

Corporate credentials must accommodate a wide range of name lengths, linguistic structures and character sets. Names may include:

- Multiple family names
- Middle names or initials
- Hyphenated structures
- Diacritics (é, ñ, ü, ç)
- Non-Latin scripts
- Suffixes (Jr., Sr., III)

A failure to properly plan for these variations can lead to truncation, illegibility or inconsistent badge layouts that interfere with both security screening and user experience. Badge designs must balance readability, space constraints and identity integrity, ensuring that names remain clear and consistent across all credential types.

6.4.1 Design Challenges With Long Names

Long or complex names can cause the following issues:

- Text wrapping into unintended areas of the badge layout
- Reduced font size to fit character length, making names unreadable at a distance
- Overlapping with photos, icons or security elements
- Inconsistent formatting across badges
- Risk of cutting off culturally significant portions of the name
- Rendering issues for non-Latin alphabets or diacritics on older printers

A proactive typography and layout strategy is essential.

6.4.2 Best Practices for Accommodating Long Names

1. Allocate Sufficient Vertical and Horizontal Space

Badge templates should be designed to support up to two lines for the name field without compromising clarity.

2. Avoid All-Caps Formatting

All-caps reduces word shape recognition and makes long names more difficult to read.

Use mixed case for optimal legibility.

3. Use Accessible, Readable Typography

Follow ADA and WCAG-informed guidance:

- Character spacing: 10–35%
- Stroke thickness: 10–30% of character height
- Line spacing: 135–170%

These principles improve readability at distance.

4. Maintain High Contrast

Names should meet or exceed WCAG AA contrast ratio (4.5:1) against the background.

5. Avoid Truncation Whenever Possible

If space forces truncation:

- Never truncate the surname
- Truncate the middle name or nonessential identifiers first
- Ensure the full legal name is stored in:
  - Barcode
  - QR code
  - Digital credential record

This preserves identity integrity for audits, background checks, and HR processes.

6. Support Unicode and Multi-Script Rendering

Systems should support:

- Diacritics
- Accented characters
- Non-Latin scripts
- Hyphenated names

Testing must be done before rollout to ensure correct encoding and printer compatibility.

6.4.3 Scaling for Distance-Based Readability

Names intended to be legible at approximately 8 feet should generally follow:

- Uppercase "I" height: 0.25–0.35 inches (≈18–25 pt)
- Larger font sizes for high-traffic environments (lobbies, guard stations)
- Increased font size if the badge will be viewed through glass or in low-light conditions

Readable names significantly improve throughput and reduce misidentification.

7 Multi-Credential Capability (One Badge, Many Uses)

Corporate environments increasingly expect a single credential to support multiple use cases across both physical and digital ecosystems. A modern identity credential may need to grant access to facilities, authenticate on workstations, enable secure printing, validate time and attendance and support parking or transportation systems. However, integrating multiple applications into a single card requires careful planning to avoid security compromises, operational conflicts or user confusion.

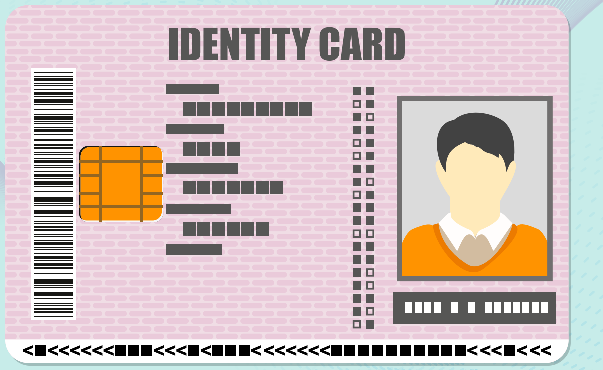
This section outlines the principles and best practices for designing credentials capable of supporting multi-application environments safely and effectively.

7.1 The Goal: A Unified, Multi-Purpose Credential

A properly designed multi-credential solution allows:

- Door access (PACS)
- Logical access (workstations, VPN, VDI)
- Secure printing / pull printing
- Parking or transportation access
- Time and attendance systems
- Specialized systems (labs, data centers, manufacturing floors)

A unified badge reduces the number of tokens employees must carry and simplifies lifecycle management—but only if built on secure, compartmentalized architectures.



7.2 Use Secure, Multi-Application Technologies

Modern smartcard platforms support:

- Multiple isolated application domains
- Independent, diversified key sets
- Secure messaging and cryptography
- Controlled inter-application access

These capabilities make them suitable for multi-purpose credentialing without exposing one system to vulnerabilities in another.

Legacy technologies—particularly 125 kHz Prox—offer none of these protections and should not be used as part of a long-term strategy.

7.3 Avoid Long-Term Dependence on Legacy 125 kHz Prox

Proximity cards:

- Are easily cloned with inexpensive tools
- Offer no cryptographic protection
- Cannot securely store additional applications
- Create long-term operational risk
- Should be sunset as soon as feasible

Multi-technology readers should have insecure technologies disabled as soon as migration is complete

During migration periods, dual-tech cards (Prox + smartcard) may be used, but only as a transitional measure.

7.4 Design for Application Isolation and Life-Cycle Control

Every application on a multi-use credential must be:

- Cryptographically isolated
- Governed by its own unique key
- Managed with key-rolling schedules
- Bound to a secure enrollment record
- Administered with strict key custody processes

Using a hardware security module (HSM) or secure access module (SAM) for key protection is strongly recommended.

These controls prevent compromise of one application from affecting others.

7.5 Support Consistent User Experience Through Visual Design

To reduce confusion and support quick user training, the back of the credential may include subtle icons indicating supported use cases:

- Door icon → PACS
- Printer icon → secure printing
- PC icon → logical access
- Clock icon → time and attendance

The front of the badge should remain uncluttered to ensure visual identity and security elements remain primary (photo, name, role, organization).

7.6 Align Multi-Credential Design With Future Mobile Migration

A unified credential ecosystem is easier to migrate to mobile formats:

- Physical and mobile credentials should share data structures
- Application definitions should support digital equivalence
- A mobile-first strategy should not require redesigning credential security models

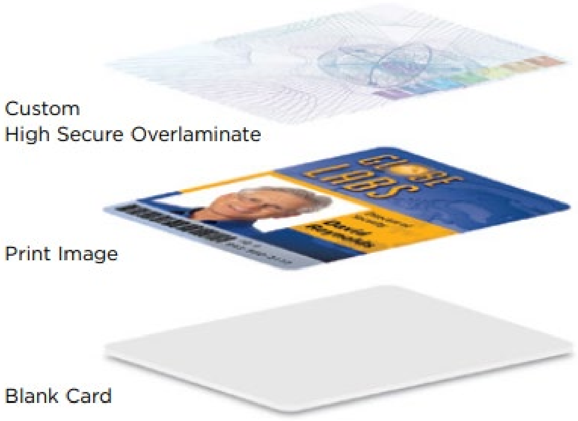
Ensuring long-term interoperability today saves costly redesigns later.

8 Security Features, Counterfeit Risk and Adversarial Testing

8.1 Secure Document Materials

Secure document materials are a critical layer in protecting corporate credentials against counterfeiting, manipulation, and unauthorized reproduction. These materials introduce physical and visual features that cannot be easily replicated using consumer-grade equipment, raising the barrier for attackers attempting to create convincing fake IDs.

When designed and implemented correctly, secure document materials contribute to a layered defense strategy—supporting quick visual verification, tamper detection and machine-readable authentication.



8.1.1 Purpose of Secure Document Materials

Secure document materials serve several key functions:

- Deterring reproduction by requiring specialized equipment to replicate
- Revealing tampering if a badge is altered or manipulated
- Allowing instant visual verification for security personnel
- Enhancing durability through protective overlays
- Supporting forensic-level authentication when incidents occur

These materials must be selected and applied strategically, ensuring they complement other anti-counterfeit measures.

8.1.2 Holographic Elements and Custom Patches

Custom holograms are one of the strongest overt security features available to corporate credential programs.

Why Custom Holograms Are Effective

- Require specialized manufacturing equipment
- Cannot be reproduced accurately through photocopying or digital printing
- Display distinct optical behaviors that are easy for guards to verify
- Provide immediate visual cues that counterfeiters often fail to imitate

Best Practice: Over-Photo Placement

Placing holographic patches or optical security films partially over the photo:

- Prevents photo swapping
- Creates a tamper-evident interaction between the hologram and the portrait
- Forces attackers to reproduce complex interactions, not just the image

This significantly increases the difficulty of producing a passable counterfeit.

8.1.3 Additional Secure Document Features

Depending on the organization’s risk profile, additional materials may be incorporated:

Examples

- UV-visible inks
- Microprinting
- Guilloche or random pattern printing
- Security threads
- OVD (Optically Variable Device) features
- Laser-engraved elements on specialized card materials

- Anti-scan or anti-copy backgrounds
- Embedded metallization patterns

These features require specialized knowledge and equipment to reproduce, limiting counterfeiting to highly skilled adversaries.

8.2 Data Duplication

Data duplication is a proven strategy in secure document design. By printing critical information in multiple locations and formats, organizations increase the difficulty of altering or counterfeiting credentials. Redundant placement of key data—such as expiration dates, employee identifiers or role indicators—creates a multi-layer verification model that supports both human inspection and automated authentication.

Attackers seeking to modify a badge must replicate or manipulate every instance of the data consistently, significantly raising the effort and expertise required.

8.2.1 Purpose of Data Duplication

Duplicating essential data elements enhances security in several ways:

- **Complicates counterfeiting attempts:** Multiple data points in different typefaces, locations and sizes create more opportunities for discrepancies.
- **Supports faster visual verification:** Security personnel can confirm authenticity by quickly comparing duplicated fields.
- **Improves tamper detection:** Misalignment or inconsistency between duplicated fields is a reliable indicator of alteration.
- **Allows flexible validation under varied conditions:** Larger or secondary text allows readability from a distance or in poor lighting.

8.2.2 Recommended Data Duplication Practices

A. Duplicate Expiration Data

Print expiration information in at least two formats:

1. Full date, in smaller or standard-size text
2. Month/year (MM/YY) or year only, in larger, more prominent text

This ensures:

- Quick recognition of expired badges
- Readability at distance
- Greater difficulty for counterfeiters attempting to alter only one part of the date

B. Duplicate Critical Identity Elements

Examples include:

- Employee ID or UID
- Clearance level
- Visitor designation
- Role or department (when operationally necessary)

These fields should be placed in positions that cannot be easily overlaid or replaced without damaging the card.

C. Use Multiple Formats Where Appropriate

For enhanced integrity:

- Pair printed text with a machine-readable version (barcode, QR, or NFC data)
- Print data in different font sizes or styles
- Place duplicated data across separated areas of the card

Variation in placement and format significantly increases tamper resistance.

8.2.3 Integrating Data Duplication With Other Security Layers

Data duplication works best when combined with:

- Holographic overlays crossing one or more data fields
- UV-printed duplicates of key data
- Digitally signed barcodes or QR codes
- Microtext or guilloche patterns bordering critical information
- Tamper-evident lamination patches

Layered security ensures that altering any duplicated element results in damage, distortion or visible discrepancies.

> **Badges should incorporate features that are visible under normal lighting, cannot be replicated accurately using consumer technology, and provide quick visual confirmation without slowing throughput.**

8.2.4 Strategic Feature Layering Based on Threat Trends

Threat intelligence should guide the layered application of:

- Overt features
- Covert features
- Forensic elements
- Digital signatures
- UV security
- Microtext
- Holograms
- Tamper-evident overlays

By combining lower-resistance features (e.g., standard microtext) with harder-to-replicate features (e.g., custom holograms crossing the portrait), organizations create a security posture that forces counterfeiters to overcome multiple hurdles simultaneously.

8.3 Counterfeit Risk

Counterfeit credentials pose a significant threat to corporate security. Attackers increasingly exploit inexpensive printing technologies, AI-enhanced image reconstruction and online tutorials to create badges that resemble authentic corporate IDs. These counterfeits may not function electronically, but their visual similarity is often sufficient to defeat low-friction screening processes, tailgate into secure areas or impersonate legitimate personnel.

Organizations must assume that any visual element of a badge can and will be replicated unless protected through a layered, tamper-resistant and verification-enabled design.

This section outlines both the risks and the defenses needed to protect corporate credentials from adversarial reproduction.

8.3.1 Understanding Adversarial Threats

Counterfeiting threats exist along a continuum, from low-skill actors with office supplies to sophisticated adversaries with professional printing equipment. Adversarial testing should reflect this range.

Three Levels of Adversarial Testing

1. Self-Test (Low Skill):

Attempts to replicate badges using:

- o Common office printers
- o Consumer laminators
- o Readily available cardstock

2. Vendor Testing (Intermediate Skill):

Testing performed using professional-grade equipment in accordance with contractual requirements.

Assesses the ability of mid-level counterfeiters to replicate visual, tactile and machine-readable elements.

3. Specialized Adversarial Testing (High Skill):

Conducted by forensic document laboratories to simulate:

- Organized attackers
- Industrial counterfeiters
- Targeted espionage threats

Organizations should conduct or commission testing at levels appropriate to the risk profile of their facilities and industry.

8.3.2 Security Personnel Capability and Real-World Constraints

Security personnel often have:

- Limited time to inspect badges
- Variable lighting conditions
- High traffic environments
- Inconsistent familiarity with badge variations

As a result, badges must include security features that are immediately recognizable at a glance, require minimal training to verify and support rapid "yes/no" authentication decisions.

Badges should incorporate features that:

- Are visible under normal lighting
- Cannot be replicated accurately using consumer technology
- Provide quick visual confirmation without slowing throughput

Badge design should never assume that guards have forensic tools or extended inspection time.

8.3.3 Recommended Tamper-Resistant and Anti-Counterfeit Features

Counterfeit risk is reduced through layered security that combines overt, covert and forensic elements.

Overt Security Features (Visible, Quick Check)

- Custom holographic patches (ideally placed partially over the photo)
- UV-printable elements
- Microtext or guilloche patterns
- Color-shifting inks
- High-contrast, standardized layouts

Covert Security Features (Visible With Tools)

- UV microtext is not visible under normal light
- Security threads or embedded fibers
- Latent images are visible at certain angles

Forensic Features (Specialized, Hard to Replicate)

- Serialized holographic foils
- Secure lamination patches
- Machine-verifiable features (digital signatures, encrypted barcodes)

Layering reduces reliance on any single feature and significantly increases the difficulty of counterfeiting.

8.3.4 Digital Signatures and Machine-Readable Security

Because visible features can be replicated, organizations must incorporate machine-verifiable integrity features into their credentials.

Strongly Recommended

- Digitally signed QR codes
- Digitally signed hashed data blocks
- Secure barcodes (PDF417 or equivalent) with integrity protection
- Encrypted chip-based credentials

These features enable:

- Validation that badge data has not been altered
- Detection of photo swapping
- Automated verification by handheld readers or mobile devices
- Stronger identity binding

Digitally signed visual codes are especially important because they prevent a counterfeit badge:

- From passing data validation
- From reproducing or altering key fields without detection

8.3.5 Avoid Reliance on Tactile-Only Security Features

Tactile features (e.g., raised text, surface embossing) are easily duplicated with consumer-grade embossers or 3D-printed tools.

They should not be used as primary security features.

Tactile features may be included only when:

- Combined with other visual or machine-verifiable layers
- Designed to distort under duplication
- Supported by controlled manufacturing processes

Using tactile-only features introduces a significant risk that casual counterfeiters will produce superficially convincing badges.

8.3.6 Strengthen Symmetric Key Handling and Live Validation Capabilities

Advanced credential programs should:

- Implement strong symmetric key management (HSM-backed where possible)
- Regularly rotate issuance keys
- Adopt real-time credential validation capabilities, such as:
  - On-demand online validity checks
  - Mobile device verification apps
  - Reader-based signature validation

Live validation significantly reduces the value of counterfeit badges by ensuring that presentation alone is not sufficient for access.

8.4 Other Supporting Credential Materials

These are the materials that are used to carry, display and protect corporate credentials—such as lanyards, badge holders and clips—play an important role in the integrity and visibility of the credentialing ecosystem. Although these items may seem purely functional, they influence:

- How easily security personnel can identify badge types
- How difficult it is for attackers to spoof or reuse accessories
- The likelihood of badge loss, damage or unauthorized transfer
- The consistency of branding and user recognition across sites

Standardizing these materials improves security, usability and organizational professionalism.

8.4.1 Branded Lanyards and Visual Identification

Branded lanyards provide a subtle but effective security layer by:

- Making unauthorized accessories easier to spot
- Reinforcing corporate or site identity
- Helping security personnel identify employees at a distance
- Reducing the likelihood that attackers can blend in using generic lanyards

Best Practices

- Issue standardized, branded lanyards for employees and contractors
- Use distinct colors or patterns for groups such as visitors, vendors, interns or temporary roles
- Avoid distributing unlabeled or generic lanyards
- Ensure lanyards match accessibility and safety requirements (breakaway clasps, non-twist designs)

8.4.2 High-Security Lanyards and Badge Holders

Organizations with elevated security needs may require more advanced accessories.

High-Security Options

- Coded or serialized badge holders
    - Difficult for attackers to acquire or replicate
    - Allow periodic reissuance to reduce spoofing
- Frequent color-change cycles for lanyards
    - Introduce unpredictability
    - Limit long-term reuse by unauthorized parties
- Secure locking badge holders
    - Prevent removal or swapping of credentials
    - Reduce badge sharing or "borrowed badge" risks

High-security lanyards and holders should integrate into broader anti-counterfeit and enforcement strategies.

8.4.3 Operational and Safety Considerations

Safety and usability must not be overlooked.

Recommended features include:

- Breakaway clasps for environments with machinery
- Non-twist or swivel attachments to maintain forward badge orientation
- Durable materials suitable for daily wear
- Clear visibility of the photo, name and role at all times

Materials should be tested across multiple workplace conditions—office, industrial, laboratory and outdoor settings.

8.4.4 Periodic Refresh Cycles

To reduce spoofing and ensure consistent appearance:

- Rotate lanyard colors or designs on an annual or semi-annual basis
- Rotate coded badge holders on predictable schedules
- Retire obsolete designs promptly
- Ensure expired accessories are collected and destroyed (similar to credential destruction protocols)

Regular refresh cycles reduce the value of stolen or lost accessories and help security personnel adapt quickly to updated visual cues.

8.4.5 Human Factors Considerations

Data duplication should assist—not overwhelm—security personnel.

Designers should ensure:

- Duplicated fields are logical and uncluttered
- Role-critical data is easy to find
- Format differences enhance verification rather than create confusion
- Duplicated data does not interfere with photo clarity or machine-readable zones

The goal is improved clarity without reducing usability.

8.5 Counterfeit Trends and Threat Intelligence from Open Web Sources

Modern counterfeiters no longer rely solely on specialized equipment or underground markets. A growing ecosystem of counterfeit materials, templates and tutorials is openly available on mainstream online marketplaces, social media platforms, hobbyist forums and global e-commerce sites. This creates a rapidly evolving threat landscape that organizations must monitor and respond to proactively.

Understanding what counterfeiters can easily access allows organizations to design credentials that resist the most common—and most likely—methods of attack.

8.5.1 Availability of Counterfeit Materials Online

Today, adversaries can readily purchase:

- Blank cards resembling corporate badge stock
- Laminates, overlays, and generic holographic patches
- Card printers capable of near-professional print quality
- Slot punches and badge accessories similar to corporate-issued materials
- Digital templates for ID layouts
- UV inks and inexpensive UV flashlights
- RFID/NFC cloning tools

These materials are marketed to a broad audience and require minimal skill to use effectively.

8.5.2 Why Monitoring Online Counterfeit Markets Matters

Monitoring openly available counterfeit materials provides insight into:

- Which security features are easily replicated

- Which features counterfeiters rarely attempt (and therefore remain strong)
- Emerging tools and methods used to mimic corporate credentials
- Trends in visual replication (AI-based enhancement, image interpolation, etc.)
- Availability of card substrates similar to legitimate credential stock

Threat intelligence gathered from open sources helps organizations update designs before counterfeiters catch up.

8.5.3 Using Threat Intelligence to Improve Credential Security

Organizations should incorporate open web research into their credential life cycles by:

A. Conducting Regular Marketplace Reviews

- E-commerce stores
- Global marketplaces
- Specialized printing forums
- Dark web aggregators (optional, via trusted security partnesr)

B. Updating Security Features Based on Findings

If certain features are widely available, such as generic holograms or common laminate patterns, organizations should:

- Replace them with custom designs
- Introduce forensic-level features
- Add machine-verifiable elements

C. Pairing Threat Intelligence With Adversarial Testing

Findings from open web monitoring should feed into self-testing or commissioned adversarial evaluations.

For example:

- If counterfeit ribbons become widely available, test replication using those ribbons
- If digital templates are discovered online, evaluate their accuracy and weaknesses

9 Data Security and Ecosystem Considerations

9.1 Digitally Signed Hashes and Advanced Data BindingTechniques

As counterfeiters gain access to increasingly sophisticated reproduction tools, relying on visual security features alone is no longer sufficient. Modern credential programs must incorporate cryptographically verifiable mechanisms that allow systems—and, when appropriate, security personnel—to confirm the authenticity and integrity of credential data.

Digitally signed hashes, secure barcodes, QR protocols and advanced data-binding techniques provide strong protection against data tampering, photo swapping and unauthorized duplication. These features significantly raise the difficulty of producing a forged credential that can withstand automated validation.

9.1.1 Why Digital Signatures Are Essential

Digitally signing a badge's encoded data establishes:

- **Authenticity:** The data was issued by the legitimate authority
- **Integrity:** The data has not been changed since issuance
- **Binding:** The data belongs to the specific individual to whom the card was issued

Without these protections, counterfeiters can:

- Swap photos
- Alter expiration dates
- Modify role or access level
- Reproduce a badge visually while inserting fraudulent data

Signed data prevents such manipulations from going undetected.

9.1.2 Digitally Signed Hashes in Printed and Digital Formats

The most common method for embedding signed data includes:

A. Digitally Signed QR Codes

QR codes can contain:

- Cryptographically signed data blocks
- Face templates or biometric hashes
- Time-bound or revocable access assertions
- Embedded issuer identifiers

Because signatures must validate against the issuer's public key, attackers cannot produce a QR code containing altered fields without breaking the signature—an infeasible task with modern cryptography.

B. Digitally Signed PDF417 Barcodes

PDF417 is widely used in government-issued IDs due to its:

- High data capacity
- Robust error correction
- Support for digital signatures
- Compatibility with handheld scanners and mobile devices

Embedding signed content enables rapid validation during badge checks.

C. NFC or Contactless Chip Data Binding

Smartcards allow:

- Encrypted data sectors
- Signed identity credentials
- Tamper-evident application structures

This is the strongest binding method and should be used when available.

9.1.3 Binding Visual and Encoded Data Together

Attackers often attempt photo substitution—swapping the portrait on a badge while leaving other data intact.

To prevent this:

- Encode the photo hash or face template into the digital signature
- Link the printed portrait to the encoded facial data

- Use holographic overlays that intersect both the photo and the QR/barcode

This ensures:

- If the printed photo is changed, the machine-readable signature fails
- Physical and digital data must match, providing a dual-layered check

This dramatically reduces the viability of photo-based forgery attacks.

9.1.4 Benefits of Cryptographically Bound Credentials

Implementing digital signatures and hashing provides:

Stronger Security

- Prevents modification of printed fields (name, expiration, role)
- Detects tampering instantly
- Enables trusted, decentralized verification

Better Life-Cycle Control

- Supports real-time revocation
- Integrates easily with mobile readers or handheld validation tools

Improved Forensic Capability

- Provides auditable integrity checks
- Assists in incident investigations
- Enables validation even when visual features are damaged

Scalability

- Works across multiple facilities, integrators and contractors
- Supports future mobile credential migration

9.1.5 Implementation Considerations

Key Management

Organizations must maintain:

- Strong symmetric or asymmetric key handling
- HSM-backed key protection (recommended)
- Controlled signing environments

Validation Infrastructure

Validation may require:

- Handheld scanners
- Mobile validator apps
- Reader-side signature verification
- Backend services for online checks

Privacy Considerations

When embedding biometric or identity data:

- Use minimal necessary data
- Ensure compliance with privacy regulations
- Apply hashing or template protection methods

9.2 Electronic Security and Communication Vulnerabilities

While physical credential security addresses visual counterfeiting and material integrity, electronic vulnerabilities represent an equally critical attack surface. Organizations should address reader-to-controller communication security, credential cloning risks and cryptographic key management to prevent attackers from bypassing physical security measures entirely.

9.2.1 Reader-to-Controller Communication Security

Standard Wiegand protocol transmits credential data unencrypted between readers and access control panels. This architectural limitation allows interception of facility codes and card numbers during legitimate presentations using commercially available tools costing under $50. Once captured, credential data can be replayed indefinitely.

- Organizations should implement encrypted reader-to-controller communication for all new installations and high-security areas.

> **While physical credential security addresses visual counterfeiting and material integrity, electronic vulnerabilities represent an equally critical attack surface.**

- SIA Open Supervised Device Protocol (OSDP) Secure Channel (SIA OSDP v2) with AES-128 encryption should be deployed as the minimum standard for reader-panel communication, replacing legacy Wiegand where operationally feasible. OSDP Secure Channel requires explicit configuration and is not enabled by default on most readers. Organizations should verify secure channel activation through packet capture or configuration audit rather than assuming encryption is active.
- Existing Wiegand installations should be documented in risk assessments with defined migration timelines based on area sensitivity.
- Reader supervision features (tamper detection, communication monitoring) should be enabled where supported by hardware.

9.2.2 Downgrade Attack Mitigation

Multi-technology credentials and readers create systemic vulnerabilities when legacy protocols remain enabled alongside modern secure technologies. Attackers can clone a credential's legacy data (e.g., 125 kHz Prox, unsecured MIFARE Classic UID) at one location and present it at another where backward-compatible readers accept both technologies. The cryptographic security of modern credentials becomes irrelevant when the same logical identity can be presented via an unencrypted channel.

- During technology migrations, organizations should document which credential interface each reader expects and operate single technology per reader where possible.
- Legacy 125 kHz proximity technology should not be deployed in new installations and should be retired from existing installations per NIST SP 800-116 Rev. 1 risk guidance.
- Multi-technology readers should have legacy technologies disabled upon completion of migration periods. Defined sunset timelines should be established at project inception.
- Organizations should implement technology-specific "tap here" indicators if dual-technology cards must operate during transition with different read ranges per technology.

9.2.3 Credential Cloning and Replay Prevention

Credential cloning represents a primary attack vector where adversaries duplicate electronic credential data to unauthorized cards or devices. Prevention requires both secure credential technologies and proper implementation.

- Organizations should deploy credentials utilizing mutual authentication with diversified, site-specific cryptographic keys rather than manufacturer default ("standard") keys.
- Credentials relying solely on static identifiers (UID-only reads, facility code/card number without cryptographic verification) should not be used for access control in medium or high-security applications.
- For high-security areas, organizations should implement anti-passback, time-based access restrictions or secondary authentication factors (PIN, biometric) to limit replay attack effectiveness.
- Reader configurations should be validated to ensure cryptographic verification is active rather than merely supported. Technology support does not guarantee secure implementation.

9.2.4 Cryptographic Key Management

In addition to implementing electronic security best practices, organizations must understand how their cryptographic design choices directly affect the scale and scope of a security incident if keys are compromised. The security impact varies significantly depending on whether the system relies on symmetric or asymmetric cryptography.

Compromised or improperly managed keys can undermine the entire credential ecosystem regardless of cryptographic strength. Proper key custody, life-cycle controls and architectural decisions are therefore essential.

9.2.5 Symmetric Key Management Considerations

Symmetric architectures rely on shared secrets, which means that compromise of one high-value key (such as a master key) can place an entire site, or even an entire enterprise, at risk.

Organizations should:

- Utilize site-specific symmetric keys, never manufacturer defaults, for all secure credential deployments.
- Store master keys only in HSMs or SAMs with strict access controls and audit logging.
- Implement key diversification so that compromise of one credential key does not expose keys for other credentials in the population.
- Maintain documented key-rolling procedures, including:
- Routine key rotation intervals based on risk assessment
- Emergency key replacement workflows in the event of suspected compromise
- Ensure encoding workstations enforce least-privilege access, and never store or transmit key material on general-purpose systems or unencrypted channels.

Risk profile:

A compromised symmetric master key may expose all dependent credentials, enabling replay, cloning or unauthorized access across the entire deployment.

9.2.6 Asymmetric Key Management Considerations

Asymmetric architectures use public/private keypairs, which provide a fundamentally different—and typically safer—risk model.

Key advantage:

If a single private key stored within a credential is compromised, only that credential is affected. The blast radius is limited to one card or device, not an entire site. Organizations adopting asymmetric credential models should ensure:

- Private keys are generated in secure hardware and never exported from the secure element that created them.
- Certificate issuance, revocation and renewal processes are defined, auditable and automated where possible.
- Root and intermediate signing keys are stored within HSMs with strict administrative controls, monitoring and logging.
- Lifecycle operations are aligned with organizational PKI policies and industry best practices.

Risk profile:

Asymmetric systems dramatically reduce systemic exposure by isolating each credential's compromise to that credential alone. Master keys or CA keys, when properly protected, do not expose the entire credential population.

10 Cardstock and Consumable Inventory Management

The security of corporate credentials begins long before a card is issued. Effective control over cardstock, printer consumables and production materials is essential to preventing unauthorized credential creation, supply theft or misuse. Poor inventory management introduces opportunities for insider threats, credential duplication and bypass of formal issuance workflows.

This subsection outlines best practices for managing all physical materials associated with credential production.

To strengthen consistency, organizations should:

- Use standardized card stock types, matched to life cycle and risk
- Store blank cards in restricted access, logged environments
- Follow secure destruction procedures for spoiled or expired cards
- Ensure issuance equipment is physically secured and under surveillance

Credential issuance systems must be treated as high-value security assets.

10.1 Credential Material Selection and Life-Cycle Alignment

This section provides additional guidance on credential materials, durability, printing technologies, encoding requirements and photo recapture. These considerations ensure that credential programs maintain long-term reliability, visual clarity, machine readability and alignment with the expected lifecycle of the card.

Credential durability depends largely on the substrate used. Selecting materials aligned to the expected badge lifecycle reduces replacement costs, ensures consistent visual quality and strengthens security features.

Key Guidance

- Choose material based on security level, expected use and environmental exposure.
- Polycarbonate, Teslin or metal substrates should be used for high-security or long-life credentials.
- PVC should be used only when frequent renewal is required or in low-risk environments.

Encoding should be logged, auditable and tied to the credential’s unique ID.

Recommended Material Durability Ranges

Material Type	Expected Life Cycle	Notes
PVC	~2 years	Suitable for low-cost, short-term credentials; prone to warping and cracking under heat/UV
Composite (PVC/PET)	3–5 years	More durable; better for moderate use and retransfer printing
Polycarbonate (PC)	6–10 years	High durability; supports laser engraving and advanced security features
Teslin (Synthetic Paper)	11–15 years	Highly durable; excellent for complex security printing and lamination
Metal (Various Alloys)	3–15 years	Extremely durable; niche use cases; requires specialized printers

10.2 Credential Reuse Considerations

Organizations sometimes consider reusing physical credentials for cost savings; however, reuse introduces forgery and integrity risks, especially if credentials contain:

- Worn edges
- Residual printing
- Laminate degradation
- Outdated security features

If reuse is necessary, add a new security feature each year to recertified cards, such as:

- Laser-engraved date markers
- Holofoil elements for each renewal cycle
- Year-specific printed icons or spacing patterns

This helps ensure reused cards cannot be easily forged using an old credential body.

10.3 Cardstock Inventory Controls

Blank cards are equivalent to pre-currency in the credentialing ecosystem—any unauthorized use can directly result in a fraudulent ID. Cardstock must be treated as a controlled asset.

Recommended Controls

- Locked storage with access restricted to authorized personnel
- Keycard- or biometric-controlled access to stock rooms
- Inventory logs documenting:
  - Lot numbers
  - Quantities received
  - Issuance for printing
  - Spoilage or damaged cards
- Regular audits of inventory levels
- Segregation of special-purpose cards (e.g., admin, visitor, high-security)
- Tamper-evident storage containers for high-risk environments

10.4 Printer Ribbon and Consumable Management

Printer ribbons contain imprinted personal data after printing. Without proper destruction, used ribbons can be harvested by attackers to obtain names, photos, barcodes or other sensitive information.

Recommended Controls

- Store ribbons and consumables in secured, access-controlled cabinets
- Maintain consumable usage logs tied to print jobs
- Implement mandatory shredding of used ribbons using certified devices
- Ensure disposal procedures comply with privacy regulations and corporate retention policies

10.5 Tracking of Consumables

Consumables should not be freely accessible or interchangeable without oversight. Implement system-based or manual tracking to detect anomalies or suspicious activity.

Examples of Effective Tracking

- Daily or weekly reconciliation of ribbon counts
- Cross-verification of print volumes vs. consumed materials
- Barcode-based tracking of cardstock
- Alerts for unusual usage patterns

Tracking should be automated wherever possible to reduce administrative burden and increase accuracy.

10.6 Secure Storage Conditions

Storage areas for consumables should:

- Maintain controlled temperature and humidity
- Protect consumables from UV exposure
- Ensure materials are protected from tampering or contamination
- Be monitored by CCTV where appropriate

Physical security reinforces chain-of-custody integrity.

10.7 Consumable Waste Disposal

Waste materials such as misprints, damaged cards and used ribbon panels must be disposed of securely to prevent unauthorized recovery.

Disposal Requirements

- Shred all defective or spoiled cards using a cross-cut shredder rated for PVC
- Ensure used ribbons are either:
  - Shredded
  - Incinerated
  - Disposed of through a certified destruction vendor
- Document destruction through logs or vendor certificates when required

10.8 Secure Destruction of Credentials

Expired, damaged or revoked credentials present a security risk if not destroyed properly. Unauthorized individuals can use discarded badges to impersonate employees, bypass initial security screening or create convincing counterfeits. A structured and auditable destruction process is therefore essential for maintaining the integrity of the credentialing ecosystem.

10.8.5 Why Secure Destruction Matters

Credentials—even deactivated ones—contain valuable information, such as:

- Branding and visual layout
- Employee photos
- Names and roles
- Barcodes or QR codes

- Credential numbering
- Anti-counterfeit features (which can be studied and replicated)

If a discarded card falls into malicious hands, it can be:

- Altered
- Photocopied
- Enhanced with AI tools
- Used to test cloning techniques
- Employed in social engineering attacks

Proper destruction prevents exploitation and reduces organizational risk.

10.8.6 Destruction Methods

To ensure complete and irreversible destruction, organizations should use one or more of the following methods, depending on badge type and security requirements.

A. Mechanical Destruction

- High-quality cross-cut shredders capable of shredding PVC or composite cards
- Dedicated card destruction devices designed specifically for ID credentials
- Manual destruction with cutting tools for low-risk environments (not recommended for high-security cards)

B. Thermal or Chemical Destruction

- Incineration via certified providers
- Chemical breakdown of card substrates (specialized processes only)
- Contracted secure destruction services with documented chain of custody

C. Electronic Destruction for Smartcards

For smartcards or RFID-enabled credentials:

- Physically destroy antenna loops and chip modules
- Ensure that embedded chips cannot be harvested or reused

10.8.7 Required Controls and Documentation

Organizations should implement:

Controlled Collection

- Locked disposal bins at badge issuance stations
- Direct handover of surrendered badges during offboarding
- Badge retrieval procedures integrated with HR workflows

10.8.8 Integration With Credential Life-Cycle Management

Destruction should be integrated with the organization's identity and access life cycle:

- Deactivate the credential before destruction
- Validate user offboarding status
- Ensure no active credentials remain unreturned
- Document both deactivation and destruction together

This maintains alignment with audit, HR and compliance processes.

Chain-of-Custody Documentation

- Logs showing who surrendered, transported and destroyed each badge
- Witness signatures for high-security environments
- Certificates of destruction for third-party services

Periodic Audit

- Regular review of destruction logs
- Spot-check inspections
- Process validation to ensure full compliance

10.9 Badge Expiration Protocols

Expiration dates are a foundational security control in corporate credential management. They ensure that outdated, unused or compromised badges do not remain valid indefinitely and help organizations align identity verification practices with employee life-cycle changes; however, organizations vary widely in their expiration policies, and many do not revisit badge photos or personal data for long periods, reducing the reliability of visual verification.

This section outlines the recommended principles and practices for establishing effective, defensible badge expiration protocols.

10.9.5 Why Badge Expiration Matters

Effective expiration policies help prevent:

- Unauthorized reuse of old or forgotten badges
- Long-term reliance on outdated photos that hinder recognition
- Credential validity beyond employment or contract terms
- Visual discrepancies that weaken trust during manual inspections
- Retention of access long after user roles have changed

Expiration requirements ensure the badge remains a current, accurate and trustworthy representation of the identity it conveys.

10.9.6 Recommended Expiration Intervals

Badge expiration should align with:

- Card material durability
- Employee role and risk profile
- Regulatory or compliance requirements
- Changes in employee appearance
- Security posture of the organization

General Recommendations

- High-security environments: Renew every 2–3 years
- Standard corporate environments: Renew every 3–5 years
- Low-risk or infrequent-access employees: Up to 5-year maximum

These intervals mirror best practices from passport, driver's license and enterprise credential guidelines.

10.9.7 Photo Update Requirements

Updating the photo is just as important as the expiration date itself.

Recommended Practices

- Require a new photo every 4–6 years, depending on environment
- Require a new photo if the employee undergoes substantial appearance changes
- Automatically refresh photos during reissuance cycles
- Require photo recapture when:
    - Hair, facial hair or aging significantly alters appearance
    - Weight change affects recognition
    - Previous photos were low-quality or legacy-format
    - Upgrading to a new credential design

Improved photo quality directly enhances visual and automated verification accuracy.

10.9.8 Visual Expiration Indicators

Badges should include clearly visible expiration markers to support fast manual inspections, especially during:

- Lobby checks
- Security guard verification
- Event or temporary site access
- Customer-facing roles

Examples include:

- MM/YY printed in large, bold text
- Color-coded expiration bands for quick visual sorting
- Month/year duplication in multiple locations (see Section 7.6 Data Duplication)
- Laminates or holographic elements that interact with expiration fields

Clear indicators reduce inspection time and prevent expired badge use due to oversight.

10.9.9 Policy and Governance Requirements

Organizations should formalize expiration rules through:

- Published badge life-cycle policies
- HR-aligned onboarding and offboarding workflows
- Automated identity management systems (IDMS/IAM)
- Consistent enforcement across all job categories

Policies should include:

- How replacements are triggered
- Renewal notification cycles
- Responsibility for verifying updated photos
- Required data validation during reissuance

Well-governed expiration practices strengthen both physical and digital security controls.

10.9.10 Integration With Interoperability Goals

Standardizing badge expiration intervals across organizations supports:

- Contract worker identity validation
- Multi-tenant campus collaboration
- Temporary access workflows
- Federated or reciprocal trust frameworks

Consistent expiration policies make shared ecosystems safer and more manageable.

11 Biometrics for Corporate Credentials

While corporate credentials typically do not require the same biometric rigor as government-issued identification (e.g., passports, driver's licenses, PIV cards), the quality and consistency of the photo remain essential for:

- Accurate visual verification by security personnel
- Automated facial comparison (now or in future expansion)
- Fraud prevention
- Consistent badge appearance across an organization
- Usability in CCTV-supported access control environments

If biometric technologies are used, organizations should consider establishing clear, requirements for the capture, processing, storage, transfer and validation of biometric data used within corporate security ID credentials. Requirements should address technical quality and accuracy, privacy protections and legal compliance to ensure reliable identity verification, resistance to misuse and respect for individual rights.

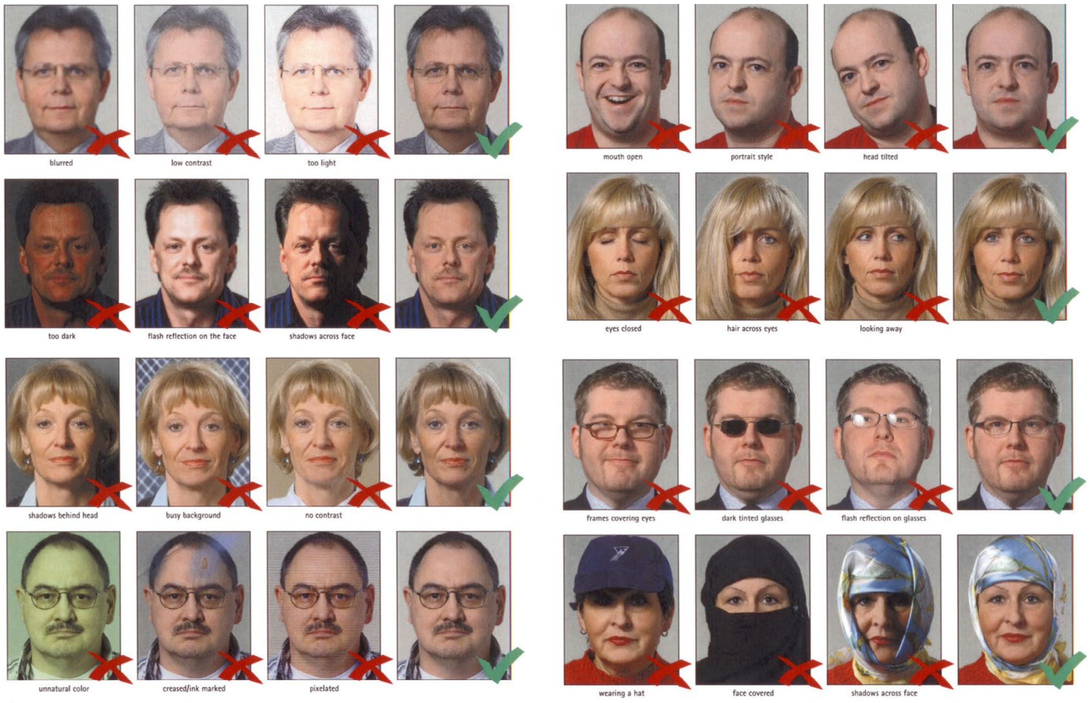
This section outlines recommended standards for photo capture, formatting, and resolution, drawing on established biometric guidelines such as ISO/IEC 19794-5 and ICAO 9303, adapted to corporate needs.

11.1.1 Why Biometric Photo Quality Matters

High-quality, standardized badge photos:

- Improve recognition under varying lighting conditions
- Reduce errors in identity verification
- Prevent attackers from exploiting low-quality or ambiguous images
- Support futureproofing for emerging technologies (AI-enhanced verification, automated visitor processing, etc.)
- Increase consistency and professionalism across sites

Poor-quality images degrade badge usability and can weaken security processes.



SOURCE*: The Federal Criminal Police Office of Germany, Bundeskriminalamt (BKA)*

11.1.2 Recommended Photo Capture Standards

These biometric-aligned guidelines improve clarity and reliability without imposing excessive operational burdens. Biometric portraits (e.g., facial images) **should be captured** in accordance with **ISO/IEC 19794-5** and **ICAO Doc 9303** scene, photographic and digital image constraints (e.g., frontal pose, tight tolerances for pitch/yaw/roll, uniform lighting, sharp focus, minimum inter-eye resolution) to support human and automated recognition and interoperability.

A. Resolution

- Minimum: 5 megapixels (MP)
- Higher resolutions preferred to support future automated recognition
- Avoid pixel compression or low-quality exports

B. Lighting

- Even, diffused lighting
- Avoid shadows on the face or background
- Avoid bright reflections or glare
- No colored lighting that alters skin tone

C. Pose and Expression

- Neutral expression (no exaggerated smiles)
- Eyes open and clearly visible
- Head centered and upright, not tilted
- Full-frontal orientation

D. Background Requirements

- Neutral background (white, gray or corporate-standard blue)
- Uniform color
- No patterns, textures or objects
- High contrast relative to the subject

E. Attire

- Avoid hats, sunglasses or distracting accessories
- Religious coverings permitted as long as the face is fully visible
- Avoid color blends between clothing and background

11.1.3 Photo Geometry and Cropping

Follow ISO/IEC 19794-5 or ICAO 9303-aligned geometry recommendations:

- Face height: 50–69% of the image
- Eye line: 55–65% of the height from the bottom of the image
- Head and shoulders must be fully visible
- Avoid tightly cropped or irregular portrait shapes

Rectangular portraits are recommended over circular crops because:

- Circular masks remove part of the shoulder/outline needed for accurate identification
- Cropping artifacts hinder visual verification
- They reduce compatibility with automated systems

11.1.4 Consistency Across All Capture Stations

To maintain uniformity:

- Use standardized camera kits and lighting setups
- Require calibration checks for brightness and color accuracy
- Maintain consistent operator training
- Enforce fixed camera distance and alignment guides
- Periodically audit image quality across locations

Standardization prevents large visual variations that complicate badge checking.

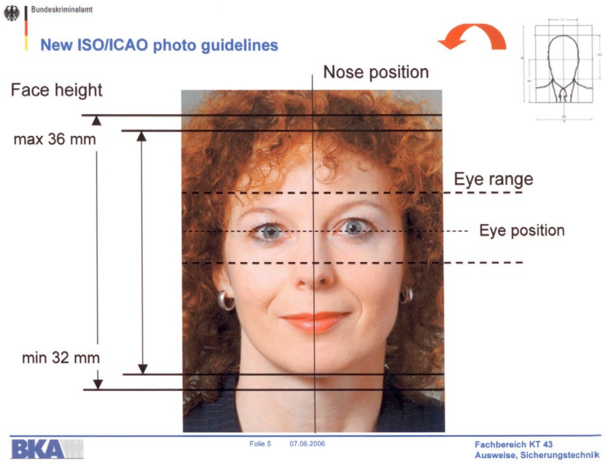
11.1.5 Biometric Quality for Digital and Mobile Credentials

As organizations move toward mobile-based identity verification, biometric quality becomes even more important.

- Digital credentials may embed face templates or photo hashes
- Mobile wallets display high-resolution images
- Security reviewers may zoom in on photos during mobile verification

In these contexts, the badge photo must be:

- Sharp
- High-resolution
- Free of artifacts
- Suitable for both small on-card display and larger digital display



SOURCE*: The Federal Criminal Police Office of Germany, Bundeskriminalamt (BKA)*

11.1.6 Photo Retake Requirements

Organizations should establish policies requiring photo retakes when:

- The badge holder's appearance changes significantly
- The photo is older than the recommended life cycle (e.g., 4–6 years)
- The image does not meet quality standards
- Low-quality legacy images are identified during migration to new credential formats

You already captured renewal intervals in Section 8 (life cycle), allowing coordination with card durability schedules.

11.1.7 Biometric System Accuracy and Performance

Biometric verification systems shall define and meet performance targets, including false match rate and false non-match rate appropriate to the organization's risk tolerance; performance shall be periodically assessed and re-baselined over time. NIST SP 800-63-4A guidance on identity assurance and life-cycle management should inform target setting and ongoing evaluation.

Where biometric matching is used as part of identity proofing or authentication, design should align to the applicable NIST SP 800-63A/B assurance frameworks and processes.

11.1.8 Lawful Basis, Consent and Individual Rights

Biometric data used for uniquely identifying an individual constitutes a special category of personal data. When used for corporate ID credentialing, organizations shall obtain explicit, informed consent from the individual prior to collection, specifying purpose, data elements and retention period.

Organizations shall obtain explicit, informed consent before collecting biometric data, specifying purpose, data elements and retention. Controllers must identify lawful basis and comply with applicable regulations (GDPR/UK GDPR, CPRA, BIPA). Policies shall support rights for access, correction, deletion and withdrawal of consent.

11.1.9 Privacy Risk Assessment and Governance

Prior to deployment, organization shall conduct a data protection impact assessment (DPIA) (or equivalent privacy assessment) addressing collection purpose, data flows, risks (e.g., function creep), mitigations and residual risk acceptance; DPIA outputs shall be reviewed and updated after changes in technology or scope.

Policies shall define authorized use, purpose limitation, access governance, auditability and processes for consent withdrawal and data subject requests (access, correction, deletion, limitation).

11.1.10 Data Security Controls

Biometric data (images, templates, feature vectors) must be protected by cryptographic controls (encryption in transit and at rest), integrity protection, role-based access control and secure key management consistent with the organization's security policy. As such it is essential that organization ensures that biometric data (templates and images) are encrypted at all times, at rest and in transit.

Storage systems and access control devices shall implement least-privilege access, tamper-evident logging, segregation of duties and breach response procedures tailored to the heightened sensitivity of biometrics (non-revocable identifiers).

Third-party processors (card production vendors, PACS integrators, cloud services) shall be bound by data processing agreements that enforce security, purpose limitation, sub-processor controls, incident notification, and deletion at contract end.

11.1.11 Retention, Minimization, and Destruction

Organizations should collect only the minimum biometric data necessary for credential issuance and verification. Retention should be limited to the disclosed purpose and duration, with documented destruction upon termination of need or employment, consistent with local law (e.g., BIPA retention schedules). 24

Retention schedules and deletion procedures shall be publicly available where required (e.g., Illinois) and communicated to individuals at the time of consent.

12 Mobile Credential Gap (Physical → Mobile)

Mobile credentials—delivered through NFC, BLE, or secure digital wallet ecosystems—are increasingly becoming a strategic priority for organizations seeking to modernize identity and access management. However, corporate mobile credentialing remains fragmented and lacks the standardization seen in regulated environments such as government-issued mobile IDs (mDLs).

Despite advancements in mobile wallet technologies, the corporate sector still lacks a universally supported pathway to convert a physical badge into a mobile equivalent. As a result, organizations face challenges in provisioning, revocation, interoperability, and user experience.

This section outlines the current gaps, the emerging standards, and the steps organizations can take now to prepare for a mobile-first future.

12.1 Current State of Mobile Credentialing

Today’s corporate mobile access landscape is dominated by proprietary, vendor-specific ecosystems, each with its own constraints:

- Mobile access may require compatible readers
- App-Based credentials transmitted over BLE work across devices that are compatible with Bluetooth Low Energy. They may be susceptible to unintended range or read variability based on reader configuration and mounting material
- Wallet programs like Apple, Google,and Samsung Wallet must be deployed in accordance within the terms of service of the platforms that the Wallet credential will be issued. Those terms may include requirements that enable the Wallet to pass function across both access and non-access use cases, as well as to have the passes provisioned via self-service portals. These terms should be reviewed prior to engagement to avoid delays. Higher Education mobile ID models do not map cleanly to corporate use cases due to requirements that include integration with campus financial systems

Because of this fragmented environment:

- There is no universal “card-to-mobile” handoff process
- Migrations rely on vendor integrations rather than open standards
- Interoperability across access control systems is limited
- User experience varies widely by device platform
- Organizations should be hyper-aware of the third party access systems they may need to flow through to access their controlled space. Parking Garages, Base-building/landlord access spaces, Elevator systems.

12.2 What Organizations Should Do Now

While the ecosystem evolves, organizations can still establish foundational practices:

12.2.1 Adopt Vendor/Manufacturer Agnostic Standards Where Possible

Track and reference:

- ISO/IEC 18013-5:2021 and ISO/IEC 18013-7:2025
  - GitHub - ISOWG10/ISO-18013
- NIST guidance on mobile and Digital identity
  - SP 800-63-4, Digital Identity Guidelines | CSRC
  - NIST 800-63A Profile for mDL Issuance — NCCoE Mobile Driver's License Project
- Vendor-neutral, Open or standard based digital credential initiatives

These frameworks help future-proof mobile strategies.

12.2.2 Design a Vendor-Neutral Provisioning Workflow

A robust mobile credentialing workflow should support:

- Real-time issuance and revocation
- Secure enrollment using validated identity evidence
- Device binding tied to user identity
- Consider implementing an Enterprise mobile wallet that is not dependent on any specific device operation system
- Multi-device support when appropriate
- Cryptographically signed credential payloads
- Prioritize interoperability standard first
- Align provisioning workflow to NIST SP800-63 Digital Identity Guidelines
- Ensure security controls are aligned with NIST SP800-53 Rev5 Security and Privacy Controls for Information Systems and Organizations

This model reduces reliance on any single vendor ecosystem.

12.2.3 Align Physical and Mobile UX

User expectations should remain consistent across physical and mobile credentials.

This includes:

- Using the same "tap here" symbols on readers
- Standardizing cues for where to present a phone
- Ensuring readers clearly indicate NFC/BLE compatibility

12.2.8 Track Industry Evolution

As mobile wallet providers refine enterprise APIs, organizations should:

- Participate in early-adoption programs where feasible
- Ensure reader infrastructure supports mobile NFC
- Avoid long-term contracts that lock systems into legacy architectures

12.2.9 The Long-Term Outlook

Corporate mobile credentials will eventually achieve broader standardization, but timelines depend on:

- Mobile OS vendor adoption
- PACS industry alignment
- Open standards maturity
- Enterprise demand for interoperability

Organizations that begin planning now will gain flexibility, reduce long-term costs and improve user experience as mobile-first identity ecosystems mature.

13 Identity Verification

Identity verification is one of the most critical components of credential issuance. Without a reliable, auditable, and standardized verification process, even the most advanced badge designs become vulnerable to impersonation, insider threats and fraudulent enrollment.

Corporate environments often lack consistency in how identities are validated, what documentation is accepted and how issuance events are recorded. This section establishes recommended practices for identity proofing, issuance governance, audit trail requirements, and alignment with external frameworks—all tailored to the corporate ecosystem.

13.1 Identity Verification

13.1.1 The Need for Standardized Identity Verification

Many organizations currently rely on informal or inconsistent identity proofing practices, creating risks such as:

- Issuance of badges without proper identity validation
- Lack of documentation showing who authorized or produced a badge
- Creation of duplicate or fraudulent records
- Inability to reconstruct issuance events during audits
- Unverified contractors receiving long-term access
- Badge issuing personnel having excessive or uncontrolled permissions

A consistent verification framework strengthens trust in the credential and supports both internal and external interoperability.

13.1.2 Recommended Identity Verification Workflow

A well-governed identity verification process should include the following steps:

Step 1: Identity Evidence Collection

Acceptable evidence may include:

- Government-issued photo IDs (driver’s license, passport)
- Employment eligibility documents
- Verified HR onboarding records
- Prior validated identities (for renewals only)

Step 2: Identity Evidence Validation

Validation may involve:

- Inspection for authenticity
- Validation against issuing authority databases (when applicable)
- Automated document authentication tools
- Manual verification procedures

Step 3: Identity Binding

The individual must be physically or digitally present during enrollment to ensure the identity is bound to the correct person.

Methods include:

- In-person verification
- Live video verification (for remote employees)
- HR or manager attestation

Recommended Identity Verification Workflow

1–Identity Evidence Collection

Acceptable Evidence:

- Government-issued photo ID
- Employment eligibility documents
- Verified HR onboarding records
- Prior validated identities (renewals only)

2–Identity Evidence Validation

Validation Methods:

- Authenticity inspection
- Database verification (issuing authority)
- Automated document authentication tools
- Manual verification procedures

3–Identity Binding

Requirement:

Individual must be physically or digitally present.

Methods:

- In-person verification
- Live video verification
- HR or manager attestation

4–Credential Enrollment & Photo Capture

Capture:

- High-quality biometric photo
- Required identity attributes
- Optional/verifiable attributes

5–Supervisor / HR Approval

Critical Control:

Issuance may NOT occur solely at badge holder request.

Approval Required From:

- Human Resources
- Security Management
- Direct Supervisor

6–Credential Issuance & Activation

Activation Must:

- Occur after approval logging
- Be tied to IAM/IDMS record
- Require dual validation (high-security environments)

Step 4: Credential Enrollment and Photo Capture

Capture:

- High-quality biometric photo (see Section 7.11)
- Required identity attributes (name, role, employee ID, department)
- Optional/verifiable attributes (as needed)

Step 5: Supervisor or HR Approval

Issuance must never occur solely at the request of the badge holder.

Approval must come from:

- Human resources
- Security management
- Direct supervisors

Step 6: Credential Issuance and Activation

Activation should:

- Occur only after approval is logged
- Be tied to the IAM/IDMS record
- Require a second person to validate correct issuance in high-security environments

13.1.3 Audit Trail Requirements

A complete audit trail must document:

- Who requested the credential
- Who approved it
- Who verified the identity
- What identity evidence was provided
- Who printed the badge
- When and where printing occurred
- Serial number/credential ID of the issued badge
- Activation date and issuer name
- Destruction method for spoiled or replaced badges

Audit trails protect organizations from fraud, insider manipulation and compliance failures.

13.1.4 Alignment With Higher-Security Frameworks (Optional, Not Mandatory)

Corporate badges typically do not require compliance with government standards such as:

- FIPS 201-3 (PIV cards)
- NIST SP 800-63 (Digital Identity Guidelines)
- ICAO 9303 (Machine-readable travel documents)

However, many principles from these frameworks are valuable:

Useful Concepts to Reference

- Identity assurance levels (IALs)
- Document validation requirements
- Enrollment recordkeeping rules
- Photo quality and biometric standards
- Proofing agent training requirements

Corporate programs should align by reference, meaning:

- These frameworks inform policy design
- They are not required to be implemented fully
- Organizations may adopt only the components that fit their risk profile

This gives corporate issuers structure without forcing compliance with government operations.

13.1.5 Policy Integration and Internal Manuals

Identity verification processes should be formalized in:

- Corporate security policy
- HR onboarding procedures
- Credentialing standard operating procedures
- IDMS/IAM administration guides
- Badge issuance training manuals

Policies should clarify:

- Required identity documents
- Approval workflows
- Exceptions and escalation paths
- Roles and responsibilities
- Documentation retention rules

Policy structure ensures repeatability and reduces reliance on individual judgment.

13.1.6 Benefits of Standardized Identity Verification

Implementing consistent identity verification protocols results in:

- Stronger protection against impersonation
- Reduced insider threat
- Audit defensibility
- Reliable cross-site and contractor validation
- Improved alignment with industry expectations
- Foundation for future interoperability and universal ID frameworks
- Trustworthy data in badge, PACS and logical access systems

A secure credentialing system is impossible without strong identity verification.

13.2 Role of Corporate ID as Identity Evidence

NIST Special Publication 800-63-4 (Digital Identity Guidelines) provides a well-established framework for assessing the strength of identity proofing, enrollment, credential issuance and validation processes. Although corporate credentials are typically not required to meet federal identity standards, aligning with NIST principles significantly enhances security maturity, auditability and long-term interoperability—especially as organizations move toward Zero Trust and converged physical/logical access models.

Corporate ID cards are categorized in NIST SP 800-63A as "fair" identity evidence, meaning they provide some assurance of identity but are not inherently high-assurance credentials unless additional validation processes are applied.

Aligning corporate credential design and issuance processes with the NIST SP 800-63 guidelines enables organizations to elevate the overall strength, trustworthiness, and operational value of their ID credentials. By adopting these well-established identity assurance principles, organizations can ensure that credentials are grounded in verified identity evidence, supported by consistent and auditable processes and built to withstand modern security threats. Beyond improving security, alignment with NIST SP 800-63 also enhances interoperability and expands the potential use of the credential—enabling it to serve not only as an access badge but also as a reliable form of identity verification across additional corporate systems and services.

This section outlines how organizations can strengthen corporate credential issuance and validation by applying NIST-aligned practices.

Organizations should treat NIST-aligned practices as an investment in future-proofing credential ecosystems.

13.2.1 Identity Proofing Requirements

NIST SP 800-63 Volume A defines IALs, which establish the rigor required for identity validation prior to issuing a credential. To ensure a strong connection between a person and their corporate credential, the identity of each applicant must be verified using validated evidence, such as:

- Government-issued photo identification
- Employment authorization records
- Trusted HR or contractor onboarding data
- Biometrics (optional, based on policy)

Identity proofing should include:

- Evidence collection
- Evidence validation (authenticity and accuracy)
- Resolution and matching (ensuring the evidence belongs to the person)

These steps align with NIST Identity Assurance Levels (IAL1–IAL3).

13.2.2 Credential Issuance Requirements

Organizations should ensure that credential issuance processes:

- Bind the issued credential to an identity record validated during proofing
- Maintain complete enrollment records, including:
  - o Applicant information
  - o Verifying agent identity
  - o Date/time of issuance
  - o Evidence used and validation methods
- Apply strong controls to prevent unauthorized credential production

Enrollment records should be securely stored, auditable and protected against tampering and unauthorized access.

Machine-Readable Security Features for Physical Cards

- Barcodes (e.g., PDF417), QR codes or encoded symbols
- RFID or NFC chips with cryptographic authentication
- Holograms, microtext, UV features
- Digital hash or biometric template encoded into printed features for tamper detection

13.2.3 Security Features for Validation

Higher-assurance credentialing programs incorporate machine-readable security features that can be validated:

Physical Cards

- Barcodes (e.g., PDF417), QR codes or encoded symbols
- RFID or NFC chips with cryptographic authentication
- Holograms, microtext, UV features
- Digital hash or biometric template encoded into printed features for tamper detection

Digital Credentials

- Cryptographically signed digital identifiers
- Device binding and secure key storage
- Integrity-protected identity assertions

These features help establish whether a credential is authentic, unaltered and valid.

13.2.4 Validation and Verification Processes

Organizations should implement:

Automated Validation Systems

- Readers or handheld devices that verify barcodes or digital signatures
- Systems that detect tampering, photo swapping or cloning attempts
- Mechanisms to check card status (active, suspended, revoked)

Remote and In-Person Enrollment Options

NIST-aligned remote processes may include:

- Video interview verification
- Remote document capture and authentication
- Secure identity attribute validation

These capabilities enhance flexibility without weakening assurance.

13.2.5 Process and Policy Alignment

Credentialing must be governed by policies that:

- Define identity proofing requirements based on the targeted identity assurance level defined in NIST SP800-63-4
- Ensure individuals performing verification are trained and vetted
- Require revalidation when evidence expires (e.g., driver's license renewal)
- Prohibit expired evidence for medium or high assurance levels (IAL2+, per NIST)

Policies should also ensure that all decision-making and system activity is:

- Logged
- Auditable
- Retained for regulatory and risk management purposes

13.3 When NIST Alignment Is Most Useful in the Corporate Sector

NIST alignment is especially valuable when:

- Corporations work with government clients
- Organizations adopt Zero Trust architecture
- Federated identity or shared-access ecosystems are in place
- Contractors move between facilities
- A future universal corporate ID model is desired

Applying NIST principles enhances:

- User experience
- Interoperability across platforms
- Support for federated identity uses
- Compatibility with mobile or derived credentials
- Migration toward Zero Trust architectures

Organizations should treat NIST-aligned practices as an investment in future-proofing credential ecosystems. NIST references provide a common vocabulary for assessing identity trustworthiness across organizational boundaries.

13.4 Practical Guidance for Corporate Use

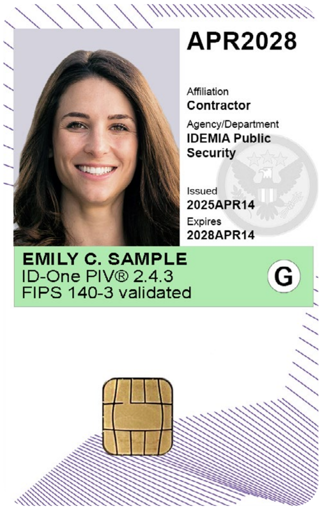
Organizations do not need to fully implement NIST 800-63A.

Instead, they should:

- Adopt the principles aligning to their risk environment
- Use NIST terminology to evaluate process maturity
- Improve identity assurance incrementally
- Treat corporate IDs as supporting evidence within a broader trust model

This approach ensures the program gains rigor without unnecessary complexity.

14 Civilian Identity Verification (CIV) Credential Option



The Civilian Identity Verification (CIV or PIV-C) credential is an advanced, standards-based identity credential derived from the U.S. federal PIV (Personal Identity Verification) ecosystem. CIV provides organizations with a stronger identity assurance model than a typical corporate ID by adopting many of the same principles used in federal identity programs—without requiring full FIPS 201 compliance.

CIV is designed for civilian organizations that require:

- Higher assurance identity proofing
- Cryptographically verifiable credentials
- Tamper-resistant card body features
- Stronger lifecycle management and auditing
- Interoperability across partner facilities, contractors and multi-tenant environments
- A pathway toward Zero Trust and federated identity
- Optional alignment with federal identity security expectations

CIV does not replace a corporate credential; it is an optional high-assurance pathway suitable for organizations with elevated risks, regulatory obligations or multi-organization access needs.

> **The Civilian Identity Verification (CIV or PIV-C) credential is an advanced, standards-based identity credential derived from the U.S. federal PIV (Personal Identity Verification) ecosystem.**

14.1 What Is a CIV Credential?

A CIV credential:

- Uses the PIV card data model but omits mandatory federal requirements
- Supports cryptographic authentication (PKI)
- Can be used for physical access, logical access and digital signing
- Can be paired with mobile or derived credentials
- Offers higher resistance against cloning and counterfeiting

CIV allows enterprises to benefit from hardened identity verification without the complexity of becoming a federal issuer.

14.2 When Should an Organization Consider CIV?

CIV is recommended when:

- Contractors require secure, cross-site access
- Employees need identity credentials recognized outside the organization
- Organizations must meet high regulatory or security expectations

> **“Enterprises with high-value assets, sensitive IP, critical infrastructure or distributed workforces gain the most benefit from use of a CIV credential.”**

- Zero Trust architecture requires strong identity binding
- Federal partners or customers expect higher-assurance identity standards
- A future shift toward mobile/digital identity is planned

Enterprises with high-value assets, sensitive IP, critical infrastructure or distributed workforces gain the most benefit.

14.3 CIV Identity Proofing Requirements

CIV issuers adopt a rigorous identity proofing process similar to NIST SP 800-63A IAL2:

- Verified government-issued identity evidence
- Authenticity checks (manual or automated)
- In-person or supervised remote identity verification
- Capturing biometric-quality photos
- Maintaining auditable enrollment records

This creates a strong link between the individual and the credential.

14.4 Credential Production Requirements

CIV credentials typically include:

- Polycarbonate or composite card body
- Laser engraving
- Secure chip technology
- PKI certificates for authentication
- Digitally signed card data
- Anti-counterfeit overlays or holograms

This ensures high tamper resistance and verifiable integrity.

14.5 CIV Life-Cycle Management

CIV supports robust lifecycle controls:

- Real-time revocation
- Online certificate validation (OCSP, CRL)
- Device-based authentication for mobile versions
- Auditable provisioning and deactivation
- Multi-year renewal and reproofing requirements

These capabilities align well with modern enterprise IAM programs.

14.6 CIV + Mobile Credentials

CIV can be extended into mobile identity through:

- Derived PIV credentials (similar to federal DPC)
- FIDO2/WebAuthn-based or certificate-based phishing-resistant authentication
- Phone-as-a-token access
- Secure element or trusted execution environment storage

This enables hybrid badge/mobile identity strategies.

14.7 CIV + Privacy

CIV supports privacy by:

- Using digital signatures instead of shared secrets
- Reducing the need to expose personally identifiable data during verification
- Allowing selective disclosure for mobile implementations
- Maintaining auditable but minimal enrollment records

CIV therefore strengthens both identity assurance and privacy protection.

14.8 Benefits of CIV

- Stronger identity assurance
- Reduced risk of counterfeit or cloned credentials
- Interoperability with partner ecosystems
- Improved compliance posture
- Compatible with Zero Trust initiatives
- Foundation for future mobile identity compatibility

CIV provides a measurable security and trust improvement over standard corporate credentials.

15 Privacy and Data Protection

15.1 Overview

This section establishes privacy principles specifically for corporate credentialing ecosystems.

- ISO/IEC 27701 (Privacy Information Management)
- ISO/IEC 29100 (Privacy Framework)
- NIST Privacy Framework
- GDPR (where applicable)
- OECD Privacy Principles

The result is a practical, standards-aligned privacy framework tailored for corporate credential design, issuance and life-cycle management.

15.2 Privacy by Design (ISO / GDPR / NIST-Aligned)

Integrate privacy controls into every stage of the credential life cycle:

- Identity proofing
- Photo capture
- Badge issuance
- Access logs
- Mobile credentials
- Data retention and destruction

Principles include:

- Proactive, not reactive (anticipate risks early)
- Privacy by default (minimal capture, least visibility)
- End-to-end security (from collection to destruction)
- Full life-cycle protection
- User-centric design

This aligns directly with GDPR Article 25 and ISO 27701 Clause 8.

15.3 Privacy Impact Assessments (PIAs)

Conduct PIAs when deploying:

- New badge technology
- Mobile credentials
- Cloud-based IAM systems
- Biometric technologies
- Cross-organization identity sharing
- New identity verification requirements

PIAs should follow NIST IR 8062 and ISO 29134 methodologies.

15.4 Data Minimization

Collect only data required for:

- Identity proofing
- Badge printing
- Access control decisions
- Compliance requirements
- Fraud prevention

Avoid collecting sensitive attributes unless required by law or safety/security protocols.

15.5 Purpose Limitation and Lawfulness

Data collected must be tied to a clear, legitimate purpose, communicated in advance.

Credentials should not be repurposed for:

- Employee monitoring
- Behavioral scoring
- Unrelated analytics
- Unapproved secondary uses

This aligns with GDPR Article 5(1)(b) and ISO 29100 privacy principles.

15.6 Storage Limitation and Retention Controls

Set retention periods for:

- Badge metadata
- Identity proofing documents
- Photo images
- Access logs
- Encryption keys
- Revocation events

Retention must follow:

- Legal requirements
- Operational need
- Security policies
- Internal audit schedules

When retention ends, securely delete or destroy data per NIST SP 800-88.

15.7 Data Accuracy and User Correction Rights

Provide simple mechanisms for:

- Correcting errors in identity data
- Updating badge photos
- Updating names or roles
- Validating authority or employment status

Accurate data reduces security errors and credential misuse.

15.8 Security of Processing and Storage

Apply organizational and technical controls:

- Encryption at rest and in transit
- Access control and least privilege
- Privileged access monitoring
- Secure badge printer environments
- Hardened identity management systems
- Vendor risk management

Credential data must be protected as a high-value security asset.

15.9 Access Restriction and Least Privilege

Access to personal data must be:

- Role-based
- Logged
- Monitored
- Segregated by duty

Badge printers, image capture stations and IAM systems must enforce strict RBAC controls.

15.10 Proportionality and Fairness

Identity data processing must be appropriate to:

- The access level requested
- The role and risk of the badge holder
- The sensitivity of the area or system accessed

Example: A visitor badge requires less identity data than a privileged employee credential.

15.11 User Control, Privacy Preferences and Reciprocity

Where appropriate, users should have:

- Ability to request data updates
- Visibility into how data is used
- Granular consent for optional features (e.g., mobile wallet enrollment)
- Default settings that minimize exposure of personal data

“Privacy by default” reflects both GDPR and ISO 27701 expectations.

> **Access to personal data must be role-based, logged, monitored, and segregated by duty**

15.12 Transparency and Notice

Provide clear explanations of:

- What data is collected
- Why it is required
- Who can access it
- How long it is retained
- How it may be audited or shared
- How users can correct their data

Plain-language transparency strengthens trust and reduces compliance risk.

15.13 Ongoing Review, Monitoring and Audit

Implement:

- Annual privacy reviews
- Access control audits
- Retention audits
- Badge issuance and destruction audits
- Supplier/vendor privacy reviews

Document all findings and corrective actions for governance reporting.

15.14 How Privacy Relates to Corporate Credentialing

Privacy practices should be tailored to specific credentialing components:

Identity Proofing

- Limit capture of unnecessary identity evidence
- Ensure temporary storage is encrypted
- Delete identity documents post-verification unless policy requires retention

Badge Photos

- Treat photos as biometric-adjacent data
- Apply strict access control
- Retain only for badge life cycle and regulated period

Access Logs

- Use role-based visibility
- Avoid storing more detail than necessary
- Apply retention limits and secure disposal
- Apply device-level protections
- Avoid unnecessary data transmission
- Use privacy-preserving digital signatures

Cross-organization Interoperability

- Ensure privacy contracts (DPAs) exist
- Limit shared data to essential identity attributes
- Use signed data instead of exposing raw personal data

16 Standards and Interoperability

Industry-wide consistency in corporate credential design remains limited. Unlike government-issued IDs—such as passports, driver's licenses and PIV cards—corporate credentials do not follow common standards for layout, data encoding, photo placement or machine-readable zones. This lack of uniformity creates operational inefficiencies, increases training burden for security personnel and hinders interoperability across corporate campuses, partner facilities and contract environments. The following sections outline the common challenges and recommended practices for improving standardization and interoperability.

16.1 Lack of Consistency

Corporate ID programs vary widely in their design choices, data structures and physical card formats. These inconsistencies make it difficult for security professionals, system integrators, and automated verification tools to validate identity information reliably. Unlike regulated identity documents—which follow provisions such as ICAO 9303, ISO/IEC 7810, AAMVA standards, or FIPS 201 corporate credentials lack equivalent harmonization.

This inconsistency introduces several problems:

- **Photo Placement Variability:**
  Different organizations place photos in varying sizes, shapes and positions, complicating security staff training and hindering reliable visual verification.
- **Inconsistent Use of Machine-Readable Zones (MRZs):**
  Barcodes (1D or 2D), QR codes, and magnetic stripes frequently store different data fields and formats from one issuer to another.
- **No Shared Data Element Set:**
  Unlike AAMVA-defined driver's license fields or MOSIP civil ID schemas, corporate badges use proprietary and unpredictable layouts.
- **Interoperability Challenges:**
  Contractors, multi-tenant facilities, partner organizations and shared campuses cannot consistently validate credentials due to mismatched formats.

A baseline standard does not require eliminating organizational customization; rather, it provides minimum alignment so that credential data can be recognized and validated across systems, readers and security personnel.

16.1.1 Recommended Practices for Achieving Greater Consistency

A. Adopt Standardized Photo Guidelines

Borrowing from ICAO/ISO standards:

- Rectangular portrait area
- Consistent head size ratio
- Consistent eye-line height
- Standard placement relative to card edges

This improves both visual recognition and future machine-automated checks.

B. Standardize Core Data Fields

Every corporate ID should contain a minimum, uniform set of data elements, such as:

1. Full legal name
2. Photo
3. Credential ID/serial number
4. Expiration date
5. Issuer name/organization

Optional fields may be included, but this core set should be consistent across facilities.

C. Harmonize Machine-Readable Data Structures

Organizations should align their digital encoding with established models:

- AAMVA model for 2D barcodes
- MOSIP civil ID model
- FIPS 201 data elements (when applicable)

This provides predictability and improves cross-system compatibility.

D. Provide Consistent Labeling, Iconography and Data Location

Roles, visitor types, access levels, and compliance indicators should appear in fixed, predictable positions across all badge variations.

16.1.2 Benefits of Increasing Consistency

By improving standardization, organizations gain:

- **Reduced Training Burden:**
  Security teams no longer need to memorize multiple badge layouts.
- **Better Interoperability:**
  Contractors, multi-site employees and partners experience fewer access issues.
- **Stronger Security Posture:**
  Predictable patterns support automated validation and reduce confusion.
- **Enhanced User Experience:**
  Badges become easier to understand, use and verify.

16.2 Universal ID Potential

The concept of a universal corporate ID—a standardized credential format recognized across multiple organizations, campuses, business partners or even industries—offers significant security and operational benefits. While full universal adoption is not yet practical, the growing convergence of physical and digital identity systems suggests that harmonization across corporate boundaries is increasingly achievable.

A universal model does not necessarily imply a single physical card used by all companies. Rather, it refers to shared rules, common data elements, recognizable security patterns and interoperable verification methods that allow credentials to be reliably validated wherever necessary.

16.2.1 Why Consider a Universal Corporate ID Model?

A. Interoperability Across Shared Environments

Many industries rely on interconnected workspaces:

- Corporate campuses shared by multiple tenants
- Partner facilities requiring cross-organization access
- Contract staff who move between different sites
- Private–public partnerships
- Global enterprises with distributed workforces

A universal ID framework allows these environments to authenticate visitors and workers more consistently and accurately.

B. Improved Security Through Standardization

Well-implemented, standardized elements (e.g., core data fields, QR signing methods, placement of machine-readable zones, photo structures) can make:

- Counterfeiting more difficult
- Training easier for security personnel
- Automated verification more reliable

Consistency can strengthen defenses across organizational boundaries.

[Note that poor implementation can result in difficult=to=detect compromised documents.]

C. Operational Efficiency

A Universal ID model can:

- Reduce onboarding friction
- Lower the cost of issuing “site-specific” badges
- Simplify mobile credential adoption
- Support shared service models for visitor management or contract labor

Organizations spending large resources reissuing temporary or contractor badges benefit the most.

16.2.2 What a Universal ID Would Require

A universal framework would require agreement on several foundational elements:

A. Physical Format Guidelines

- Standard photo placement
- Consistent portrait geometry
- Recognizable holographic positions (not identical designs, but consistent structure)
- Predictable iconography and labeling

B. Core Data Schema

Borrowing from models such as AAMVA, MOSIP and FIPS 201, a universal corporate badge could define:

- Required data fields (name, issuer, credential ID, expiration)
- Optional but recommended fields (role, site access level, department)
- Structured machine-readable zones with consistent ordering

C. Cryptographic Standards

For machine-verifiable identity assurance:

- Digitally signed barcodes
- QR codes with issuer certificates
- PKI or symmetric key validation models
- Shared or federated trust frameworks

D. Governance Model

A universal ID system must define:

- Who manages root keys
- Who sets compliance guidelines
- How organizations certify their credentials
- How updates and revisions are coordinated

This could mirror existing frameworks like:

- FIPS 201 Evaluation Program
- AAMVA Card Design and Security Committee
- PKOC (Public Key Open Credential) initiatives

16.2.3 Challenges to Implementing a Universal Corporate ID

Despite the benefits, widespread adoption faces practical challenges:

- Varying risk profiles across industries
- Diverse budgets and technology baselines
- Vendor dependencies and proprietary systems
- Legal and privacy considerations (especially cross-border)
- The need for multi-stakeholder governance
- Resistance to standardization from entrenched internal processes

However, these challenges are not insurmountable. Many industries (financial services, healthcare, manufacturing, energy) stand to benefit from even partial standardization.

16.2.4 A More Realistic Near-Term Approach

Instead of a single universal corporate ID, organizations can adopt:

Universal “Minimum Standards”

- Shared design patterns
- Commonly recognized photo and data layouts
- Standardized expiration and renewal cycles
- Common verification zones on the card
- Standard machine-readable formats

Federated Verification Models

- Organizations validate each other’s digital signatures
- Shared PKI trust anchors
- Reciprocal validation agreements for contractors

Mobile Identity Integration

As mobile credentials become standardized (e.g., ISO 18013-5 for mDLs), universal corporate identity may naturally evolve around mobile-first frameworks.

16.2.5 Bottom Line

A universal corporate identity standard is both technically feasible and operationally beneficial. While full cross-industry adoption may take time, organizations can begin implementing common data schemas, aligned security features and interoperable verification mechanisms today. This foundational alignment will accelerate future adoption of broader, standardized credentialing frameworks.

Conclusion

Corporate credentialing is no longer a purely operational function—it is a strategic component of enterprise security, privacy protection, identity assurance and user experience. This document provides a comprehensive framework for designing, issuing, validating and managing corporate credentials that meet modern security needs while supporting interoperability, usability and future growth.

By adopting consistent design standards, integrating strong security features, strengthening identity proofing processes and aligning with industry frameworks such as NIST 800-63A, organizations can dramatically reduce the risk of credential misuse, counterfeiting, social engineering and operational inefficiencies.

The future of corporate identity lies in:

- Standards-based design
- Cryptographically verifiable credentials
- Interoperable machine-readable data
- Mobile identity integration
- Privacy-first and security-by-design practices
- Shared governance and continuous improvement

As organizations move toward converged physical and digital ecosystems—including Zero Trust, mobile wallets and federated identity—the guidelines in this document provide a clear foundation for secure, scalable and adaptable credential programs.

Corporate credentials should be more than just access cards—they should be trusted, secure identity instruments supporting the entire life cycle of the modern workforce. This credential design best-practice guide is intended to serve as a foundational baseline for organizations seeking to strengthen the design, governance and life-cycle management of corporate ID credentials. Because credential ecosystems continue to evolve—with new technologies, emerging threats and shifting operational requirements—no single document can fully capture every consideration or scenario. As such, this guide should be viewed as a neutral, living resource technology.

We recognize that corporate ID credentials involve many interconnected components spanning security, usability, identity assurance, materials, issuance workflows and technology integration. As these elements advance, so too must the guidance that supports them. Ongoing input from practitioners, vendors, security experts and other stakeholders is essential to ensure this document remains relevant, practical and adaptable.

We welcome continued collaboration and feedback to refine and expand these guidelines in future iterations. By working together, the industry can strengthen trust, improve interoperability and raise the overall standard for secure and user-centered corporate ID credentials.

> **Corporate credentials should be more than just access cards—they should be trusted, secure identity instruments supporting the entire life cycle of the modern workforce.**

Glossary

A glossary ensures shared understanding across security teams, integrators, executives and vendors. The following definitions support the terminology used throughout the Corporate Credential Design Guidelines.

Key Terms

- **Adversarial Testing:** A structured evaluation that attempts to replicate or compromise a credential using the tools and methods available to potential counterfeiters.
- **Antenna Inlay:** The embedded coil inside a contactless card enabling RFID/NFC communication.
- **Barcode (PDF417):** A stacked 2D barcode format commonly used for high-density data storage, including signed identity data.
- **Biometric Photo Standard:** A set of guidelines (typically ISO/IEC 19794-5 or ICAO 9303) defining image geometry, lighting and resolution for identity photographs.
- **Credential ID:** A unique serial number or identifier assigned to a physical or digital credential.
- **Digital Signature:** A cryptographic method used to verify that data has not been altered and originates from a legitimate issuer.
- **Downgrade Attack:** An attack exploiting backward-compatible systems by presenting credential data via a less-secure technology channel (e.g., cloning 125 kHz Prox data from a dual-technology card) to bypass modern cryptographic protections.
- **Holographic Patch/OVD:** A tamper-resistant optical security device used to prevent photo substitution and counterfeiting.
- **HSM (Hardware Security Module):** Tamper-resistant hardware device that safeguards cryptographic keys and performs encryption operations in a protected environment.
- **Identity Assurance Level (IAL):** A NIST-defined measure of identity verification rigor (IAL1, IAL2, IAL3).
- **Key Diversification:** Cryptographic technique where unique keys are derived for each credential from a master key, ensuring that compromise of one credential's keys does not expose others.
- **Machine-Readable Zone (MRZ):** An area of a credential containing encoded data intended for automated scanning.
- **Mobile Credential:** A digital identity stored on a smartphone or device, authenticated via NFC/BLE and protected through cryptographic methods.
- **Mutual Authentication:** Cryptographic process where both the credential and reader verify each other's identity before exchanging protected data, preventing unauthorized readers from extracting credential information.
- **Overlay/Patch Laminate:** Protective layers added to card surfaces; patches offer stronger tamper resistance.
- **SAM (Secure Access Module):** Embedded secure element in readers or encoders that stores cryptographic keys and performs authentication operations isolated from general-purpose firmware.
- **Secure Destruction:** The irreversible destruction of expired or spoiled credentials using shredders, incineration or certified vendors.
- **Tactile Feature:** Raised or textured elements on a credential; not reliable as a primary security feature.
- **OSDP (Open Supervised Device Protocol):** SIA standard for reader-to-controller communication supporting bidirectional data exchange and AES-128 encryption (Secure Channel) as an alternative to legacy Wiegand.
- **Wiegand Protocol:** Legacy unidirectional, unencrypted communication standard between readers and access control panels. Transmits facility code and card number in cleartext.

References

Below is a recommended, publication-ready reference section that aligns with the documents you uploaded, and the sources cited throughout the white paper.

19.1 Standards and Specifications

- NIST SP 800-63A—Digital Identity Guidelines: Enrollment and Identity Proofing
- NIST SP 800-116—Guidelines for PIV Credentials in Physical Access Control Systems
- FIPS 201-3—Personal Identity Verification (PIV) of Federal Employees and Contractors
- ISO/IEC 7810—Identification Cards—Physical Characteristics
- ISO/IEC 19794-5—Biometric Facial Image Data
- ICAO Doc 9303—Machine-Readable Travel Documents
- AAMVA DL/ID Card Design Standards
- ISO/IEC 18013-5—Mobile Driver's License (mDL) Specifications

19.2 Industry Resources

- FIDO2 / W3C WebAuthn Specifications
- PKOC (Public Key Open Credential) Framework
- DHS/TSA mDL Pilot Documentation
- Federal Identity, Credential and Access Management (FICAM) Trust Framework

19.3 Supporting White Papers and Reports

- Identity Proofing Equity Study—Privacy Impact Assessment
- Civilian Identity Verification Credential (PIV-C/CIV) White Paper
- Biometrics Discussion Document
- Corporate Identity Code of Practice (internal companion document)

Contributors

Produced by:
SIA Credential Design Working Group

This document reflects the expertise, collaboration and cross-industry experience of the Credential Design Working Group. The following individuals contributed to research, writing, technical validation and subject matter review.

Primary Contributors

- Teresa Wu—Vice President, Smart Credentials and Smart Integrate, IDEMIA Public Security
- Tiffany Renz—Director of Sales, North America, HID
- Beth Wenisch—Sales and Business Development Manager, HID
- Lindsay Martin-Nez—Vice President of Industry Engagement, Secure Issuance, HID
- Jim Cooper, SICC—Founder, Physec Systems
- Mert Karakaya, Ph.D.—Senior Research Engineer, IPVM
- James Burke, CISSP—Principal, SynchroCyber
- Elaine Wooton—Principal Consultant, IDxQD
- Travis Willis, CFF—Business Development, Legic
- Andrew Campagnola—Director of Product Management, Kastle Systems
- Cameron Walker-Miller—Director of Standards and Technology, Security Industry Association

Acknowledgments

The Working Group wishes to acknowledge the organizations, agencies and industry partners whose standards, white papers and research informed these guidelines, including:

- The American Association of Motor Vehicle Administrators (AAMVA) - AAMVA DL/ID Card Design Standard
- Information Technology Laboratory National Institute of Standards and Technology (NIST) - Federal Information Processing Standards Publication, Digital Identity Guidelines Identity Proofing and Enrollment
- International Civil Aviation Organization (ICAO) – Document 9303, Machine Readable Travel Documents
- International Organization for Standardization (ISO)
- The Federal Criminal Police Office of Germany, Bundeskriminalamt (BKA)

securityindustry.org