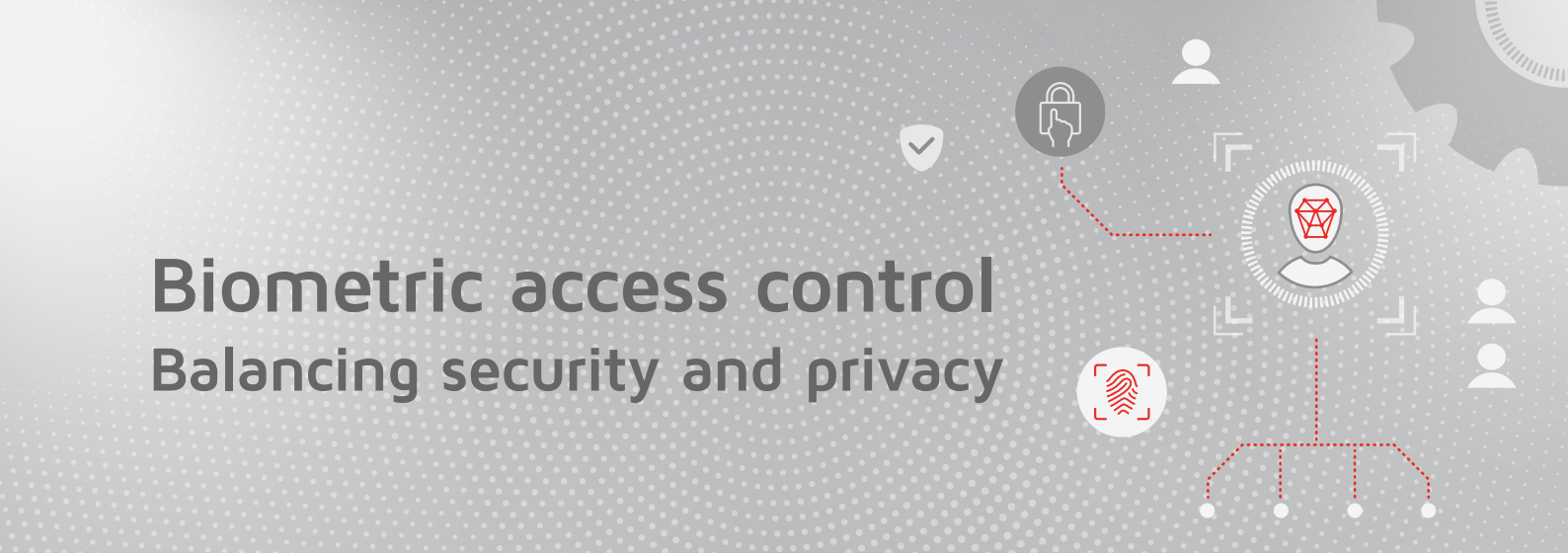
Biometric access control

Balancing security and privacy



Organizations are under growing pressure to strengthen access control while reducing operational friction. Cards, PINs, and even mobile credentials can be shared, stolen, or misused, and audit trails may reflect "credential use" rather than the person who actually entered. Biometric access control adds higher confidence by verifying who is requesting access at the door.

At the same time, biometrics raises legitimate privacy, governance, and regulatory questions. The most successful deployments treat privacy as a design requirement—selecting the right template storage model (central vs. Template-on-Card vs. device-based), applying risk-based authentication policies, and controlling enrollment, retention, and administrative access.

This web whitepaper explains where biometrics delivers the most value, outlines practical privacy controls, and provides a deployment blueprint you can apply across single-site or multi-site environments.

Why biometrics now

Credential-based access control systems tend to fail in predictable ways. Badges can be lost or borrowed, PINs can be observed, and shared credentials reduce accountability. In high-traffic or high-turnover environments (contractors, temporary workers, logistics hubs), these issues increase administrative overhead and reduce confidence in audit trails. Biometrics helps address these gaps by requiring the authorized user to be physically present at the point of access.

Security and operational benefits

Higher identity assurance

Biometrics verifies the person at the door, reducing reliance on shareable credentials.

Improved audit integrity

Verified identity makes event logs more meaningful for investigations and compliance reporting.

Reduced misuse & "buddy punching"

Deters credential sharing, especially in restricted zones or contractor workflows.

Streamlined experience

Fewer passwords/cards to manage and fewer support calls related to lost credentials.

A practical best practice is to deploy biometrics selectively—starting with higher-risk doors—so you gain security value without adding friction everywhere.

Risk-based authentication and multi-factor options

Not every door requires the same assurance level. Many organizations apply risk-based authentication: standard zones remain fast, while sensitive zones require stronger verification.

Typical policy patterns

Standard zones	Sensitive zones	High-risk zones
card or mobile credential (fast throughput)	biometric + PIN or biometric + mobile credential (two-factor)	stepped authentication or multi-modal verification (e.g., face + PIN) where the threat model warrants it

Privacy-by-design controls that build trust

Privacy concerns typically center on collection, storage, access, and retention. These concerns are addressable through clear architectural choices and enforceable operational controls.

Data minimization and secure processing

- Prefer template-based processing over storing raw biometric images where possible.
- Encrypt biometric templates in transit and at rest; restrict administrative access by role.
- Limit who can enroll, update, or delete biometric profiles; log and audit all biometric administration actions.

Transparency, consent, and governance

- Provide clear user notice: what is collected, why, where it is stored, and how long it is retained.
- Implement documented joiner/mover/leaver workflows and enforce retention rules.
- Maintain an incident response plan that includes biometric data handling.

Compliance readiness (e.g., GDPR)

Regulatory requirements vary by jurisdiction, but common themes include lawful basis for processing, purpose limitation, minimization, retention controls, access governance, and user rights handling. Privacy-forward architectures—especially decentralized storage models—can reduce risk by shrinking the amount of sensitive data stored centrally.

Important to know: Biometric technologies involve the processing of sensitive personal data. Organizations considering the deployment of biometric access control solutions should ensure that their implementation complies with applicable local laws, privacy regulations, and data protection requirements. Regulatory obligations related to biometric data may vary between jurisdictions, and appropriate legal, privacy, and security assessments should be conducted prior to implementation.

Architecture options: where templates are stored

One of the most important decisions is the template storage model. Different approaches have different privacy, scalability, and operational implications.

Model	What it means	Security/Privacy posture	Operational considerations
Central template storage	Templates are stored in a secured database/ server and matched during verification.	Higher central responsibility; strong controls needed; larger impact if the database is compromised.	Simpler enrollment and lifecycle at scale; easier multi-site use; requires strong governance and monitoring.
Template on Card (ToC)	Template is stored on the user's smart card; comparison is performed using the card-held template.	Privacy-forward; avoids a central biometric database; reduces attack surface and improves data isolation.	Requires smart card lifecycle management; enrollment must securely write templates to cards.
On-device / reader-based templates	Templates are stored on the biometric reader/device (where supported) and matched locally.	Reduces central storage; privacy depends on device security and admin controls.	Can increase complexity in multi-site fleet management; depends on device capabilities and update strategy.

Template-on-Card is often preferred by organizations that want the security benefits of biometrics while minimizing centralized sensitive data.

Scaling biometrics across sites and integrating with access control infrastructure

A biometric program should be scalable: as an organization grows, policies and administration should remain consistent across sites. Modern networked access control architectures typically use IP controllers and centralized management to enforce uniform rules and produce unified reports.

For example, enterprises often deploy IP controllers (such as Rosslare's AC-825IP class controllers) to connect biometric readers and door hardware into a unified system. This supports standardized permissions, consistent audit logs, and the ability to apply higher-security modes to specific zones without redesigning the entire deployment.

Deployment blueprint (recommended steps)

Define the risk model	Classify doors into standard, sensitive, and high-risk zones; decide where biometrics adds measurable value.
Choose the storage architecture	Select central vs Template-on-Card vs on-device templates based on privacy posture, scale, and operations.
Define authentication policy	Decide which zones require two-factor (biometric + PIN/mobile) and which remain credential-only.
Establish enrollment governance	Define who can enroll users, what documentation is required, and how removals are handled.
Implement retention and access controls	Set retention rules, restrict admin roles, and audit biometric admin actions.
Pilot and expand	Pilot in a high-value area, measure outcomes, then scale to additional zones/sites.

Common applications and expected outcomes

Biometric access control is widely adopted in environments where identity certainty matters: financial services, healthcare, government, critical infrastructure, and logistics centers with contractor access. Typical outcomes—when deployed with good policy and governance—include reduced credential sharing, improved audit confidence, and fewer incidents related to lost or misused credentials.

When describing outcomes publicly, use measured language unless you have published KPI evidence (for example: “significant reduction in unauthorized entries” or “reduced lost-card overhead”).

Conclusion

Biometric access control can deliver stronger security and better accountability—especially in high-risk areas—when deployed with privacy-by-design principles. By selecting the right template storage architecture (including Template-on-Card), applying risk-based authentication, and enforcing clear governance over enrollment, retention, and administration, organizations can improve security outcomes while maintaining user trust.

Quick checklist for a privacy-forward rollout

- ☐ Start with high-risk doors and contractor workflows; expand after pilot success.
- ☐ Choose a storage model aligned to privacy posture (consider Template-on-Card to reduce centralized data).
- ☐ Use two-factor authentication in sensitive zones (biometric + PIN/mobile).
- ☐ Define enrollment governance and user transparency/consent.
- ☐ Set retention rules and enforce deactivation/removal for leavers.
- ☐ Encrypt templates; restrict admin access; audit all biometric admin actions.
- ☐ Ensure multi-site policy consistency and centralized reporting.