Security, Compliance & Digital Identity FAQ

Everything you need to know about the security, privacy, and compliance of our products.

1. General

Q1. Are your solutions secure?

Yes. Our services rely on proven security standards, a resilient infrastructure, and a robust governance framework. Each product undergoes regular risk assessments, independent audits, and penetration tests.

Q2. Are you compliant with all applicable laws, including privacy laws?

Yes. We comply with the laws applicable in all jurisdictions where we operate, including:

- Law 25 (Quebec)
- PIPEDA (Canada, federal)
- GDPR (Europe)
- CAN-SPAM / Canadian Anti-Spam Law We have appointed a Data Protection Officer (DPO).

Q3. Do you have a public privacy policy?

Yes. Our policy is accessible on our website and explains how we collect, use, share, and protect personal data.

Q4. Do you obtain explicit user consent before collecting data?

Always. We use clear consent mechanisms with logged proof, tailored to each use case.

Q5. Who can access my data?

Only authorized personnel, following the least privilege principle, can access your data if necessary. All access is logged, monitored, and regularly reviewed.

Q6. Are your practices governed by documented policies and procedures?

Yes. We maintain:

- A set of security and privacy policies approved by management

- Incident response plans
- Employee training materials
- Procedures with third parties, including contractual clauses
- Internal and external compliance reviews

Q7. Are you registered with any regulatory or self-regulatory authorities?

Yes. Depending on our products, we collaborate with:

- The OQLF (French language compliance in Quebec)
- Certification bodies (e.g., ETSI/eIDAS, ISO)
- Regulatory authorities as required

2. Technical Security

Q8. Do you protect data in transit and at rest?

Yes. We use encryption (AES-256, TLS), pseudonymization, and anonymization, especially in testing or preproduction environments.

Q9. Do you have hardening standards for your servers, networks, and endpoints?

Yes. We apply strict standards, including:

- Patch management
- Mandatory MFA
- No generic or shared accounts
- Securing routers, firewalls, access points, endpoints, physical and virtual servers

Q10. Do you use intrusion detection systems (IDS)?

Yes. We deploy network monitoring tools (IDS/IPS) to detect anomalous or malicious behavior.

Q11. Do you conduct penetration tests and manage vulnerabilities?

Yes. We conduct annual penetration tests by specialized firms and maintain a formal vulnerability management program (automated scans, tracking, corrective actions).

Q12. Are user devices protected (encryption, antivirus, etc.)?

Yes. All laptops and desktops feature:

- Full-disk encryption
- Centralized EDR protection

- Remote wipe capabilities in case of loss or theft

Q13. Are activity logs detailed and usable?

Yes. Our logs contain full metadata (access, modification, signature, consent) and support investigations, audits, and controls.

3. Data Protection

Q14. Where is my data hosted?

Your data is hosted in Canada. No transfers outside this area occur without your explicit consent.

Q15. Is the data encrypted?

Yes. All data is encrypted at rest and in transit using strong algorithms (AES-256, TLS 1.2+). We also implement integrity checks, digital signatures, and anti-tampering protection.

Q16. Do you retain my data after the end of our business relationship?

We only retain your data as needed for legal, regulatory, or contractual purposes. You can request its permanent deletion, except where otherwise required.

4. Signatures & Digital Identity

Q17. What does CertifiO guarantee about the identity of a signer?

CertifiO binds a digital certificate to an individual's verified identity. This identity is:

- Validated using official ID
- Reviewed by an authorized agent or via automated video
- Linked to a cryptographic key controlled by the user

Q18. Are CertifiO certificates legally recognized?

Yes. Our certificates comply with legal frameworks in Quebec and Canada, and some are qualified under eIDAS in Europe. Signatures are:

- Legally binding
- Linked to verifiable identity proof
- Timestamped to the second
- Sealed by an accredited certificate authority

Q19. What is the difference between CertifiO and other e-signatures?

CertifiO is backed by a certified PKI, key ownership proof, and verified identity. Unlike drawn or clicked signatures, it allows cryptographic verification after signing.

5. Infrastructure & Cybersecurity

Q20. Do you have an information security policy?

Yes. Our policy is governed internally and is subject to quarterly audits and annual external penetration testing.

Q21. What happens in the event of a security incident?

We follow a strict response process:

- Rapid detection and containment
- Client notification depending on severity and law
- Centralized registry and post-mortem analysis
- Transparency and continuous improvement

Q22. What audits do you undergo annually?

We are audited for:

- ISO 9001: Quality management system
- ISO 27001: Information security
- SOC 2 Type II: Security controls
- External penetration tests and code reviews
- eIDAS audits for our trust services

Q23. Are your logs admissible as evidence in court?

Yes. Our logs are:

- Digitally sealed
- Immutable
- Timestamped by a certified time authority They can be used for legal proof or audit purposes.

6. Consent & Privacy

Q24. How do you collect user consent?

Our interfaces include explicit consent mechanisms tailored to each context. In ad hoc cases, we log the proof of consent.

Q25. Can I exercise my rights (access, withdrawal, correction, etc.)?

Yes. You or your users can contact us at any time. We respond within the legal deadlines (generally within 30 days).

7. Integration, APIs & SLA

Q26. Can your products integrate with our existing systems?

Yes. Our solutions provide secure APIs, full technical documentation, and connectors to third-party systems.

Q27. Do you offer service level agreements (SLAs)?

Yes. In addition to the SLAs on our website, specific agreements can include guarantees on availability, response times, and support.

Q28. Do you provide legal proof in case of a dispute?
Yes. We can provide technical evidence, timestamped documents, and certified transaction logs upon request from a court or arbitrator.

8. End-User Protection

Q29. How do you protect vulnerable users?

We prioritize:

- Clear interfaces
- Simple language
- Non-biometric alternatives where needed
- The ability to withdraw or refuse without pressure

9. Governance & Compliance

Q30. Do you have a Data Protection Officer (DPO)?

Yes. Our DPO oversees compliance with Law 25, Canadian, and international privacy laws. They act as the contact point for rights requests or regulatory inquiries.

Q31. Do you have charter committee or a governance program?

Yes. Our ISO/SOC2 program includes:

- Internal committees (security, compliance, product)
- Management reviews
- A strategic planning cycle based on risk analysis
- Quality indicators and monthly security KPIs

10. Auditability & Third-Party Verification

Q32. Are you certified or audited by independent third parties?

Yes. We undergo regular audits, including:

- ISO/IEC 27001: Information security
- SOC 2 Type II: Security, confidentiality, integrity
- ISO 9001: Quality management
- eIDAS: For certificates and identity verification We share summaries or proof with clients on request, under certain conditions.

Q33. Are your security policies accessible to clients?

Our internal policies are confidential, but we can provide an executive summary or a table of contents, and proof of compliance upon request.

Q34. Do you have cyber insurance?

Yes. We maintain insurance coverage for security incidents, data leaks, human error, data loss, and service interruption.

Q35. Are your systems auditable?

Yes. Critical events (authentication, signature, consent) are logged with timestamps in tamper-proof logs, which are usable for audits and legal purposes.

Q36. Can I audit your practices or request compliance evidence?

Absolutely. Upon request, we provide:

- Executive summaries of our audits or certifications (SOC 2, ISO, etc.)
- Records of processing
- Risk and impact assessments (PIAs)
- Policy documentation (under NDA if required)

11. Incidents, Disputes & History

Q37. Have you had recent security incidents?

No material or significant incidents have occurred in the past 24 months. Our detection and response processes have proven effective.

Q38. Have you been subject to government investigations, complaints, or external audits related to data protection?

No such cases have occurred in the past 24 months. We fully cooperate with authorities upon request.

Publication date: 2025-07-04

Disclaimer