IdenTrust Values & Benefits Statement

What broad value and benefits does your CA provide Apple? Please provide as much detail covering as many areas as possible. Please provide a link to an externally hosted document.

IDENTRUST CA VALUE

IdenTrust, a part of HID Global, is a long-established leader in digital identity and PKI (Public Key Infrastructure) certificate solutions, with over 25 years of experience. Headquartered in Salt Lake City, Utah, it operates globally with offices in the U.S. and Europe.

IdenTrust provides a comprehensive suite of digital certificates used for: TLS/SSL website security; S/MIME email encryption; Digital signatures and code signing; IoT device authentication; EPCS-compliant certificates for electronic prescriptions.

These solutions support secure data exchange, user authentication, and regulatory compliance across sectors like government, finance, healthcare, and enterprise IT.

Key Differentiators

- Proven Compliance: Meets strict standards (e.g., CAB Forum, DoD ECA, DEA EPCS) and is cross-certified with the U.S. Federal Bridge.
- Global Reach, Local Trust: Millions of certificates issued worldwide, with strong regional support.
- Security at Scale: Trusted by Fortune 500 companies and public sector organizations.
- Innovation with Integrity: Combines cryptographic expertise with emerging technologies as part of HID Global.

IdenTrust is positioned as a trusted provider of secure, compliant, and scalable digital identity solutions, enabling organizations to transact with confidence in a connected world.

APPLE QUESTIONS

A detailed response should be able to answer questions such as:

How do your processes ensure timely and transparent reporting of compliance incidents?

At IdenTrust, we are committed to maintaining full compliance with CA/Browser Forum (CA/B Forum) requirements, including timely and transparent incident reporting. Our organization has a well-established and documented process to monitor, detect, and respond to potential compliance issues.

Daily monitoring activities Includes but not limited to:

- SSLMate's CRL Watch and OCSP Watch
- Root Store CA disclosure channels
- Internal system monitoring tools
- Problem report mailbox traffic

When a potential incident is identified—whether internally or through external reports— the SWAT team gets notified which includes members from Tech Ops, Bus Ops, Development, QA, and Management team. The SWAT team will identify the Incident Lead and the Incident Lead is responsible for all aspects of emergency response; including incident objectives, managing all incident operations, application of resources as well as responsibilities for all person involved. The Incident Lead will work closely with our internal Browser Compliance Working Group (BCWG) for incident reporting. The BCWG comprise of Policy Management Authority (PMA), Risk Management Committee (RMC), Compliance, and Program Management teams.

Our Incident Response Protocol Includes:

1. Verification of the issue
2. Identification of affected certificates and revocation timeline
3. Root cause analysis and stop issuance when applicable
4. Preliminary incident disclosure within 72 hours
5. Notification to relevant root store programs

6. Publication of a full incident report within 14 days

We assign dedicated resources to manage each incident from discovery through resolution, ensuring accountability and transparency throughout the process.

How does your organization's internal processes reflect PKI industry standards for annual audits and policy maintenance?

IdenTrust is committed to upholding the highest standards in Public Key Infrastructure (PKI) operations. As part of this commitment, we undergo annual audits aligned with industry-recognized frameworks, including the WebTrust Program for Certification Authorities and SOC 2. These audits are conducted on a continuous basis, ensuring an unbroken sequence of audit periods, each not exceeding one year in duration.

In addition, Internal Audit and Compliance team maintain up-to-date knowledge of best practices and audit standards. Oversee compliance with laws, regulations, and internal policies; conduct risk assessments on a yearly basis to identify any potential risks and mitigate those risks. The team is also responsible for conducting independent internal audits of IdenTrust non-accounting functions once a year as determined by the CIO, to evaluate the effectiveness of risk management, control and governance processes.

IdenTrust Program Management team oversees a rigorous internal process for maintaining and updating our policy documentation. This process ensures that all policy documents are reviewed and updated at least annually, supporting our dedication to transparency, accountability, and compliance with evolving industry requirements.

How involved is your organization in the CA/B Forum, and how do you contribute to the CA community?

IdenTrust is an active participant in the CA/Browser Forum. We ensure consistent representation in bi-weekly teleconferences and in-person meetings, with dedicated team members from our engineering and network CA infrastructure groups attending regularly.

In support of the broader CA community, IdenTrust—through HID and the acquisition of ZeroSSL—actively contributes to the development and maintenance of major open-source ACME clients, including Caddy Server and ACME.sh. These efforts help promote accessibility, interoperability, and automation in certificate management.

As a certificate issuer, we also provide feedback through CA surveys and working group discussions. Our input helps shape and improve the Baseline Requirements, which are essential to enhancing the security and reliability of the web PKI ecosystem.

Does your organization's future goals, as a CA, align with the goals of the CA community?

Yes, IdenTrust's roadmap is closely aligned with the strategic direction of the CA community - focusing on enhanced security, governance, and automation.

IdenTrust/HID supports the two of the largest opensource ACME clients, which is Caddy and ACME.sh. By focusing on these areas, we demonstrate commitment to the shared goals of the CA community to focus on certificate lifecycle automation, contributing to a more secure and trustworthy digital environment.

How does your organization align with Apple's policy on privacy?

IdenTrust collects only the personal data necessary for certificate issuance and only from applicants or trusted Registration Authorities - no extra data is sourced from any other third parties which mirrors Apple's principle: collect only what's needed and only with user understanding and consent. IdenTrust privacy policy clearly outline the framework. https://www.identrust.com/privacy.html

Does your organization provide a current security policy to protect Apple users?

Yes, IdenTrust maintains a comprehensive and robust System Security Plan which is the master policy and procedure document for system security and data protection aligned with the NIST Cybersecurity Framework. This policy is made available to authorized external auditors for validation purposes. Separately, our data privacy practices—referenced in the previous question—are specifically designed to safeguard the personal and certificate-related information of all Digital Certificate Subscribers.

Does your organization keep user information private from third party vendors?

Yes, as indicated in section 2B "HOW WE USE YOUR PERSONAL INFORMATION" of the IdenTrust Privacy Policy, "*We do not sell or otherwise provide your data to any third party for their marketing purposes*."

CA LIFECYCLE MANAGEMENT

Apple is looking to have CAs more regularly replace root certificates and key material, which helps ensure that keys are generated, protected, and used according to the most effective security practices currently known. As this may involve CAs replacing roots and keys created under older security standards and practices with new key material, Apple would like to understand CAs' current and planned approaches to CA lifecycle management. Please describe your CA Lifecycle Management plan. Please provide a link to an externally hosted document.

A detailed plan should be able to answer questions such as:

How many Roots are in active operation?

We currently operate two publicly trusted, multi-purpose roots that support the issuance of both RSA and ECC certificates. These roots are authorized to issue certificates for a wide range of use cases, including TLS/SSL, S/MIME, Code Signing, Client/Device Authentication, and Timestamping services:

1. IdenTrust Commercial Root CA 1
2. IdenTrust Public Sector Root CA 1

How many Roots are planned for?

We are in the process of having these nine (9) single purpose roots trusted by the browsers:

1. IdenTrust Commercial Root TLS RSA CA 2
2. IdenTrust Commercial Root TLS ECC CA 2
3. IdenTrust Commercial Root SMIME RSA CA 2
4. IdenTrust Commercial Root SMIME ECC CA 2
5. IdenTrust Commercial Root Code Signing RSA CA 2
6. IdenTrust Commercial Root Timestamp RSA CA 2
7. IdenTrust Commercial Root Timestamp ECC CA 2
8. IdenTrust Commercial Root Client-Auth RSA CA 2
9. IdenTrust Commercial Root Client-Auth ECC CA 2

How far in advance of a Root expiring is its replacement signed

To ensure continuity of trust, new public trust root certificates are generated well in advance. For example, the current IdenTrust Commercial Root CA 1 is expiring in 2034 but we already have new single purpose roots generated in 2025 to replace the existing root CA as policy changes. Typically, we plan to have replacement Roots at least five years before the expiration of the currently trusted root. These newly created roots are submitted to the CCADB, initiating the process for inclusion in major browser and operating system trust stores.

How are cross-signatures handled between generations?

Once a new root is created, if there is a need to maintain ubiquity with an older root, the new root certificate is cross-signed by the private key of the older root certificate.

What trust purposes is each Root created to serve?

CURRENT ROOTS	PURPOSE RSA & ECC
1. IdenTrust Commercial Root CA 1 **2.** IdenTrust Public Sector Root CA 1	TLSS Server Authentication, S/MIME, Code Signing, Timestamping, Client/Device Authentication

NEW ROOTS	PURPOSE
1. IdenTrust Commercial Root TLS RSA CA 2	TLS Server Authentication (RSA)
2. IdenTrust Commercial Root TLS ECC CA 2	TLS Server Authentication (ECC)
3. IdenTrust Commercial Root SMIME RSA CA 2	S/MIME (RSA)
4. IdenTrust Commercial Root SMIME ECC CA 2	S/MIME (ECC)
5. IdenTrust Commercial Root Code Signing RSA CA 2	Code Signing (RSA)
6. IdenTrust Commercial Root Timestamp RSA CA 2	Timestamping (RSA)
7. IdenTrust Commercial Root Timestamp ECC CA 2	Timestamping (ECC)
8. IdenTrust Commercial Root Client-Auth RSA CA 2	Client/Device Authentication (RSA)
9. IdenTrust Commercial Root Client-Auth ECC CA 2	Client/Device Authentication (ECC)

How comprehensive is the PKI with regards to algorithmic and key size usage?

IdenTrust PKI infrastructure uses these guidelines for certificate issuance:

For RSA Key Pairs: ensure that the modulus size, when encoded, is at least 2048 bits, and; • Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA Key Pairs, ensure that the Key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve. No other algorithms or Key sizes are permitted.

For Keys corresponding to Root and Subordinate CAs: If the Key is RSA, then the modulus must be at least 2048 bits in length. If the Key is ECDSA, then the curve must be one of NIST P-256, P-384, or P-521.

For Keys corresponding to Subscribers: If the Key is RSA, then the modulus size, when encoded, is at least 2048 bits in and is evenly divisible by 8. If the Key is ECDSA, then the curve must be one of NIST P-256, P-384, or P-521.

How quickly are customers transitioned from one Root to another?

Customer migration from one root certificate to another can typically be completed within 1-3 years based upon the trust ubiquity into different operating systems and browsers.

When are new Roots submitted to the Apple Root Program for inclusion?

We plan to submit the new roots 3 to 5 years in advance unless there are changes to the policy and practices that enforce the change sooner.

LINTING

If linting is performed by your CA, please provide a detailed description of your linting configuration and playbooks. If linting is not performed by your CA, please confirm that and outline any plans you have for introducing linting into your processes. Please provide a link to an externally hosted document. A detailed description should be able to answer questions such as:

Do you perform pre-issuance linting?

Yes.

If a pre-issuance linter detects an issue, what steps are performed?

If any issues are detected during pre-issuance linting, production issuance is automatically blocked. Our team is immediately notified to review the details.

Do you regularly run linters post-issuance?

Yes, Post-issuance linting is performed on every issued certificate as well.

What linters do you run?

Zlint for TLS certificates and PKIlint for S/MIME certificates.

How often do you update linters and/or linter configurations?

Key members of our development team are subscribed to linter update mailing lists to stay informed of changes. Upon receiving an update, the changes are incorporated into our standard change control process and prioritized accordingly. Our goal is to plan for the updates within 90 days of their release to ensure continued compliance and certificate quality.

Do you disable any lints from any linters? If so, what lints? How do you decide what lints to disable?

We do not disable any Lints.

What is your process for reviewing or contributing new lints?.

IdenTrust uses publicly available linting tools to validate certificate compliance. Any issues flagged during linting are cross-checked against our certificate profiles, which are regularly reviewed for alignment with RFC 5280 and CA/Browser Forum Baseline Requirements.

If a linting alert is determined to be inaccurate or not applicable, we document the discrepancy and submit it through the linter's GitHub repository.

To date, we have not identified or reported any discrepancies requiring contribution back to the linting projects.

What is your process for executing lints on all of your valid certificates?

Lints are executed pre and post certificate signing and as a part of audits

CUSTOMER AND CHANGE MANAGEMENT

Apple continually evolves its policies and requirements in response to security threats and needs of its products. As part of that, Apple looks to understand the impact such changes may have on its users and on those using certificates designed to work with its products. Please describe the process for communicating changes to users. Please provide a link to an externally hosted document.

A detailed description should be able to answer questions such as:

Do you provide public resources about upcoming changes?

Yes, via this website.

How do you communicate to existing subscribers about upcoming changes?

In accordance with our Service Level Agreement (SLA), we maintain a proactive communication strategy for software and infrastructure changes:

1. Initial Notification: A detailed announcement is sent to customers via mass mailing lists at least 30 days prior to any scheduled change control activity.
2. Reminder Notification: A follow-up reminder is issued 72 hours before the update is implemented, ensuring customers have adequate time to prepare.
3. Post-Update Confirmation: After the change is applied, a confirmation message is promptly sent to inform customers of the outcome—whether the update was successfully implemented or if any issues were encountered.

How do you ensure that you have current and correct contact information for Subscribers?

For our enterprise customers, we assign dedicated POC representatives to ensure their contact information is always up to date. For web subscribers, the contact details are verified before issuing the certificate during the initial certificate application and at renewal or earlier, as required by the CA/B Forum baseline requirements.

How is feedback gathered regarding potential changes under discussion in the industry?

Account representatives regularly communicate with customers to inform them about upcoming changes and collect their input during these conversations. In addition, we conduct structured surveys to capture broader feedback and ensure customer perspectives are considered in decision-making.

ACME DOMAIN VALIDATION

Do you support domain validation compliant with the ACME protocol?

Not currently, but we plan to implement domain validation compliant with the ACME protocol in near future.

ACME CERTIFICATE ISSUANCE

Do you support certification issuance through the ACME protocol?

Yes, IdenTrust supports certificate issuance through ACME protocol.