IdenTrust
Certificate Authority (CA) Value

IdenTrust
part of HID

Contents

1 IDENTRUST SERVICES LLC – CA VALUE

IdenTrust, part of HID Global, is a leading provider of trusted identity solutions, delivering digital certificates that secure online transactions, encrypt communications, and authenticate identities. Recognized by financial institutions, healthcare providers, government agencies, and enterprises worldwide, IdenTrust ensures compliance, security, and operational efficiency across industries.

As the only bank-developed identity authentication system in the world, IdenTrust delivers a legally and technologically interoperable environment for authenticating and using identities in more than 175 countries. With over 11 million certificates in active production, IdenTrust supports over 126 billion validations per year.

Core Principles

- Trust & Compliance – IdenTrust certificates comply with global security standards, such as WebTrust for CA, SOC 2, DirectTrust, Federal PKI, GDPR, eIDAS, and DEA EPCS mandates, ensuring businesses meet regulatory requirements.
- Scalability & Integration – Offering SSL/TLS, client authentication, document signing, Code Signing, S/MIME for Email Signing and Encryption and IoT certificates, that are publicly trusted or trusted by U.S. Government. IdenTrust provides seamless integration with enterprise and cloud-based systems.
- Reliability & Automation – With 99.9%+ system uptime, IdenTrust ensures uninterrupted validation and issuance while enabling automated certificate lifecycle management.

Industry Solutions

IdenTrust serves a diverse range of industries with identity-based digital certificates tailored for security and compliance:

- Government – Federal, state, and local agencies use IdenTrust for secure application access, digital signing, and encrypted email.
- Healthcare – Digital certificates ensure compliance with DEA mandates for EPCS prescribing, protect patient data, and secure medical devices.
- Banking & Finance – Trusted by financial institutions, IdenTrust provides secure authentication and digital signing for regulatory compliance and fraud prevention.
- Enterprise & Corporate – Organizations implement identity-based security solutions to protect sensitive data, manage access, and enable secure digital workflows.
- Personal & Professional – Individuals use IdenTrust certificates for secure email, electronic document signing, and eNotary services.
- IoT & Device Security – Ensures secure data exchange between connected devices and protects device authentication in critical environments.

Headquartered in Salt Lake City, UT, IdenTrust operates from its primary datacenter with additional support from its London, UK office, serving banking and financial customers in EMEA. By combining trusted identity authentication, global compliance, and industry-leading reliability, IdenTrust empowers businesses, governments, and individuals to transact securely with confidence in an increasingly digital world.
IdenTrust has achieved significant milestones, including:

- Accreditation to issue U.S. Department of Defense External Certification Authorities certificates known as DoD-ECA certificates;
- Issuer of device certificates for major ATM vendors via private PKI
- Becoming a Federal Bridge Certification Authority (FBCA) to secure communications and transactions with U.S. federal, state and local government agencies

- Partnership with Let's Encrypt in 2015 by cross-signing Let's Encrypt intermediate certificate using IdenTrust widely trusted "DST Root X3" root certificate which was immediately recognized and trusted by most device's browsers; and,
- Playing a role in enabling trusted relationships for B2B commerce.

The value of IdenTrust as a Certificate Authority can be assessed through several key aspects:

Trust and Reputation: IdenTrust has established a strong reputation in the industry as a reliable CA. Organizations often prefer to work with trusted CAs to ensure their digital certificates are recognized and accepted globally.

Compliance and Standards: As a service organization in PKI, IdenTrust strictly adheres to various industry compliance standards and regulations, such as those set by the IETF, ITU, X.509, RFC, WebTrust for CAs, FISMA, NIST, FIPS and the CA/B Forum Baseline Requirements and Network Security.

Diverse Offerings: IdenTrust offers a variety of certificate options for both private and public roots, including SSL/TLS, S/MIME, Code Signing, Client Authentication and Timestamping services. This diversity enables businesses to find solutions tailored to their specific needs such as:

- Control access to systems, websites or applications by implementing two-factor authentication
- Protect email communications to ensure the integrity of messages and to encrypt contents to ensure privacy
- Encrypt data and documents while at rest and in transit
- Establish non-repudiation, enhanced auditability, improved processing and paper reduction when replacing traditional "wet ink" signing with digital signing
- Comply with DEA regulations when prescribing controlled substances using Electronic Prescriptions for Controlled Substances (EPCS)
- Ensure the integrity and confidentiality of data streams between devices and authenticate devices in the field
- Secure domain names and organization identities, allowing online transactions to be conducted with complete trust and confidence

Security Features: IdenTrust employs strong security measures to protect its certificate issuance and management processes. This includes robust authentication procedures and cryptographic techniques that enhance the security of the certificates issued.

Automation: Automated TLS/SSL issuance and renewal process with ACME or RESTful API, reducing manual efforts and errors, and streamlining enterprise certificate management across all servers and subdomains. It integrates seamlessly with existing IT infrastructures.

Global Reach: IdenTrust's certificates are widely recognized and trusted across various browsers, U.S. Federal and State Agencies and financial institutions with customer base across 175 countries.

Support and Services: IdenTrust offers 99.9% system uptime providing uninterrupted certificate issuance and validations. IdenTrust offers 24x7 phone support for any priority 1 or 2 issues.

Innovation: IdenTrust is at the forefront of adopting advanced technologies like Post Quantum Cryptography (PQC), Automated Certificate Lifecycle Management, and passwordless authentication for network and IoT devices. These innovations significantly enhance security and reduce risks within the web ecosystem, ensuring robust protection and maintaining high trust in their digital certificates.

In summary, the value of IdenTrust as a Certificate Authority lies in its reputation, compliance with standards, diverse offerings, strong security measures, global recognition, customer support, and willingness to innovate.

These factors make it a valuable partner for organizations seeking to implement secure digital communications and transactions.

APPLE QUESTIONS

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

IdenTrust documents and maintains security incident response and compromise handling policies and procedures, as well as disaster recovery and business continuity plans. Such procedures and plans are available for onsite review by its auditors and major Authorized Relying Parties under appropriate non-disclosure agreements. Below is a synopsis of the incident response policies and procedures.

For each incident, an initial goal of the incident response plan is to determine the degree and scope of the incident. This includes a determination of the cause or source of the incident (e.g., internal System failure, external malicious attack, user error), and the potential severity of the harm caused by the incident. For all incidents, data is collected and analyzed to determine, among other things:

- Whether a crime has been committed, and if so, whether evidence can be collected that will be helpful to law enforcement;
- What data was disclosed or compromised, and whether there was a Private Key compromise; and
- What steps need to be taken immediately to mitigate further damage.

For anticipated threats, IdenTrust maintains step-by-step procedures and task assignments for members of the incident response team, depending on the type of incident that is believed to have occurred. IdenTrust annually tests, reviews, and updates these procedures. Procedures are tested at least annually as part of the disaster recovery exercise.

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

IdenTrust adheres to PKI industry standards for annual audits and policy maintenance through the following processes:

1. IdenTrust Operations related to its own CA, CSA and RA are audited annually against the criteria of the WebTrust Program for Certification Authorities. These audits provide an unbroken sequence of Audit Periods that shall not exceed one year in duration. Certificates that are capable of being used to issue new Certificates are either (a) Technically Constrained and audited in line with Section 8 of the CPS only in regard to self-audits, or (b) unconstrained and fully audited in line with all remaining requirements from the CA/B Forum BR. A Certificate is deemed capable of being used to issue new Certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.
2. If the IdenTrust CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4 of the CPS, then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in- time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4 of the CPS. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

By implementing these processes, we ensure our PKI infrastructure remains secure, compliant, and aligned with industry standards.

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

IdenTrust actively participates in the CA/B Forum, with dedicated resources attending the working groups bi-weekly teleconferences and sending at least one representative to in-person meetings.

We contribute feedback as Certificate issuer via CA Surveys to help establish and refine the baseline requirements which are geared to enhancing the security of the web PKI ecosystem.

Our commitment to the CA community extends beyond the CA/B Forum, as we continually work to provide robust security solutions and stay at the forefront of digital certificate technology.

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

As a CA, our future goals are aligned with the CA community's objectives of enhancing digital security, trust, and reliability. Key areas of alignment include:

1. Improving security practices: Continuously adopting encryption standards and security protocols to protect against evolving cyber threats.
2. Fostering transparency: Implementing clear policies and procedures for certificate issuance and management, promoting trust within the digital ecosystem.
3. Advancing interoperability: Working towards seamless integration with various platforms and systems to ensure widespread compatibility of certificates.
4. Supporting emerging technologies: Adapting to new developments like quantum computing to maintain the relevance and effectiveness of digital certificates.

By focusing on these areas, we demonstrate commitment to the shared goals of the CA community, contributing to a more secure and trustworthy digital environment.

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

IdenTrust complies with industry standards and Apple's program requirements to ensure user privacy and security. Key aspects of IdenTrust's privacy expectations for CAs include:

1. Compliance in accordance with applicable laws and regulations, including US federal and state laws and the European Union GDPR.
2. Transparency: Disclosure of all CA Certificates chaining up to their CA Certificate(s) included in the Apple Root Program.
3. Audits and monitoring: Adhere to Apple's reserved right to require additional audit engagements, appoint or reject auditors, and request detailed controls reports from CAs.
4. Data protection: Implementing measures to protect user information and limit data collection to what is necessary for certificate issuance and management.
5. Consent for personal data: Obtain user consent for the global transfer and publication of any personal data contained in a Certificate.
6. De-identification of personal data: Removal of all personal data elements, including full addresses and identifiers linked to personal data, for data to be considered de-identified.

IdenTrust's data privacy policy is publicly disclosed here: https://www.identrust.com/privacy.html

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

IdenTrust does have and maintain a robust Security Policy, compliant with the NIST framework, which is only shared on site with authorized external auditors for validation; however, our data privacy referenced in the above question is designed to protect all our 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*."

2 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:

2.1 How many Roots are in active operation?

We currently have these active multi-purpose publicly trusted root CA which can issue both RSA and ECC certificates for 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

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

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

New public trust roots are created at least 5 years before the expiration date of the currently trusted root. These newly created roots are submitted to the Common CA Database (CCADB) for browser inclusion within a year of their creation.

2.4 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 signed by the older root certificate.

2.5 What trust purposes is each Root created to serve?

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

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

Our PKI infrastructure uses these guidelines for certificate issuance:

Algorithm Selection: PKI employs a variety of cryptographic algorithms to secure communications. Commonly used algorithms include RSA, ECC (Elliptic Curve Cryptography), and DSA (Digital Signature Algorithm). The choice of algorithm impacts both security and performance. For instance, ECC can provide equivalent security to RSA but with shorter key lengths, making it more efficient.

We are currently familiarizing ourselves with the Post-Quantum Cryptography (PQC) algorithms under review and approval by NIST. We are closely monitoring their timelines to ensure a smooth transition to PQC and maintain compliance.

Key Lengths: The strength of cryptographic keys is directly related to their length. Longer keys provide stronger security but may require more computational resources. For example, RSA keys are typically 2048 or 4096 bits long, while ECC keys can be as short as 256 bits and still offer strong security.

Standards and Recommendations: Organizations like NIST and ENISA provide guidelines on appropriate key lengths and algorithms. These recommendations evolve as computational capabilities and cryptographic research advance. For instance, NIST recommends a minimum security level equivalent to 128 bits for new systems

2.7 How quickly are customers transitioned from one Root to another?

Transitioning customers from one root to another can be accomplished within 3-month period, once the new public trust root is enabled by the browser root stores.

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

Our standard procedure is to submit new root certificates at the earliest opportunity. This submission process is initiated as soon as we can generate a production-ready test end-entity certificate. This certificate is a crucial component of the inclusion request for TLS certificates. We aim to complete this process at least three years before any currently trusted root certificate is scheduled to expire

3 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:

3.1 Do you perform pre-issuance linting?

Yes.

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

We conduct thorough pre-issuance linting for every certificate before it is released.
If any issues are detected during the linting process, the system automatically blocks the certificate from being issued.
Upon detection of an issue, our team receives immediate notification.

3.3 Do you regularly run linters post-issuance?

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

3.4 What linters do you run?

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

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

Key members of our development team are subscribed to mailing lists for linter update notifications. These updates are subsequently integrated into our standard change control process and prioritized accordingly for implementation.

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

We only disable lints that do not align with our certificate issuance practices and offerings. Specifically, we evaluate lints based on their relevance to our certificate profiles and disable those that do not match or apply to our certificate issuance processes
For example, we disable these CA/B S/MIME OIDs as we do not enable those in our certificate profiles:
Organization-Validated Legacy: 2.23.140.1.5.2.1
Sponsor-Validated Legacy: 2.23.140.1.5.3.1
Individual-Validated Legacy: 2.23.140.1.5.4.1

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

We use public linters to validate our certificates, and any error notifications they generate are cross-checked against our certificate profile, which is also evaluated for compliance with RFC 5280 and the CA/Browser Forum Baseline Requirements. If we find a linter flag to be inaccurate, we document the discrepancy through the linter's GitHub repository.

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

All of our public trust certificates governed by the CA/B Forum are reviewed using both pre-issuance and post-issuance linters.

4 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:

4.1 Do you provide public resources about upcoming changes?

Yes, via this website.

4.2 How do you communicate to existing subscribers about upcoming changes?

As per our Service Level Agreement (SLA), we maintain a proactive communication strategy regarding software and infrastructure changes:

1. Initial Notification: Customers receive a detailed announcement via mass mailing lists 30 days before any scheduled change control.
2. Reminder: A follow-up reminder is dispatched 72 hours prior to the implementation of the update, ensuring customers are well-prepared.
3. Post-Update Communication: After the change has been applied, we promptly send a confirmation message. This communication informs customers whether the update was successfully implemented or if any issues were encountered.

4.3 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.

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

IdenTrust gathers feedback on potential industry changes through several channels:
Industry Forums and Working Groups: IdenTrust actively participates in industry forums and working groups, such as the CA/Browser Forum, PKI Consortium, DirectTrust and other relevant organizations. These platforms provide opportunities to discuss upcoming changes and gather feedback from various stakeholders.

Partnerships and Collaborations: IdenTrust collaborates with technology partners and other Certificate Authorities (CAs) to stay informed about industry trends and gather diverse perspectives on proposed changes.

Internal Review and Analysis: IdenTrust conducts internal reviews and analyses of industry developments. This process involves evaluating the potential impact of changes and gathering input from internal experts.

5 ACME DOMAIN VALIDATION

5.1 Do you support domain validation compliant with the ACME protocol?

Not at present, but plan to incorporate by year-end 2025

6 ACME CERTIFICATE ISSUANCE

6.1 Do you support certification issuance through the ACME protocol?

Yes, for our Enterprise customers.