

HID IdenTrust Timestamping-as-a-Service

As organizations across the globe adjust to a long-term hybrid work culture, there is a need to empower employees to perform all functions digitally. The days are gone where you needed to print and sign the document with wet ink. Digitization processes have been expedited with the remote work environment and people are adopting digital signatures as a part of their digital transformation journey. Many states in the U.S. now allow eNotary signatures while many others are in the process of approving them. As we sign documents or software code digitally, what are the risks associated with it?



RISKS ASSOCIATED WITH DIGITAL SIGNATURES

When you sign a legal document, it's typically done in the presence of a notary to make sure that date and time have been validated. How do you enforce this process with a digital signature? When someone signs a PDF file digitally, the system will add a timestamp using the computer's local time settings which can easily be changed or forged. Someone can forge the system clock and make an expired certificate valid. How do you prevent such situations?

THE SOLUTION

Timestamping Authority can prevent such forgery and create longevity for digital signatures of document or software application code. HID Timestamping-as-a-Service binds the digital certificate used for signing the document or software application code with the data being signed, creating a unique hash, and identifies when the digital signature has been applied. The result is a trusted, accurate digital date and timestamp seal embedded within the digital file that contains X.509 digital signatures. Any change in the timestamped file will break the timestamp seal, alerting the user that the file is no longer in its original state.

HID Timestamping-as-a-Service helps organizations reduce risk by providing long-term validation and non-repudiation of time and date. It provides a digital seal of data integrity and trusted date and time of when the transaction has occurred.

Apply RFC 3161 compliant trusted timestamp to digital signatures and software application code.

KEY BENEFITS

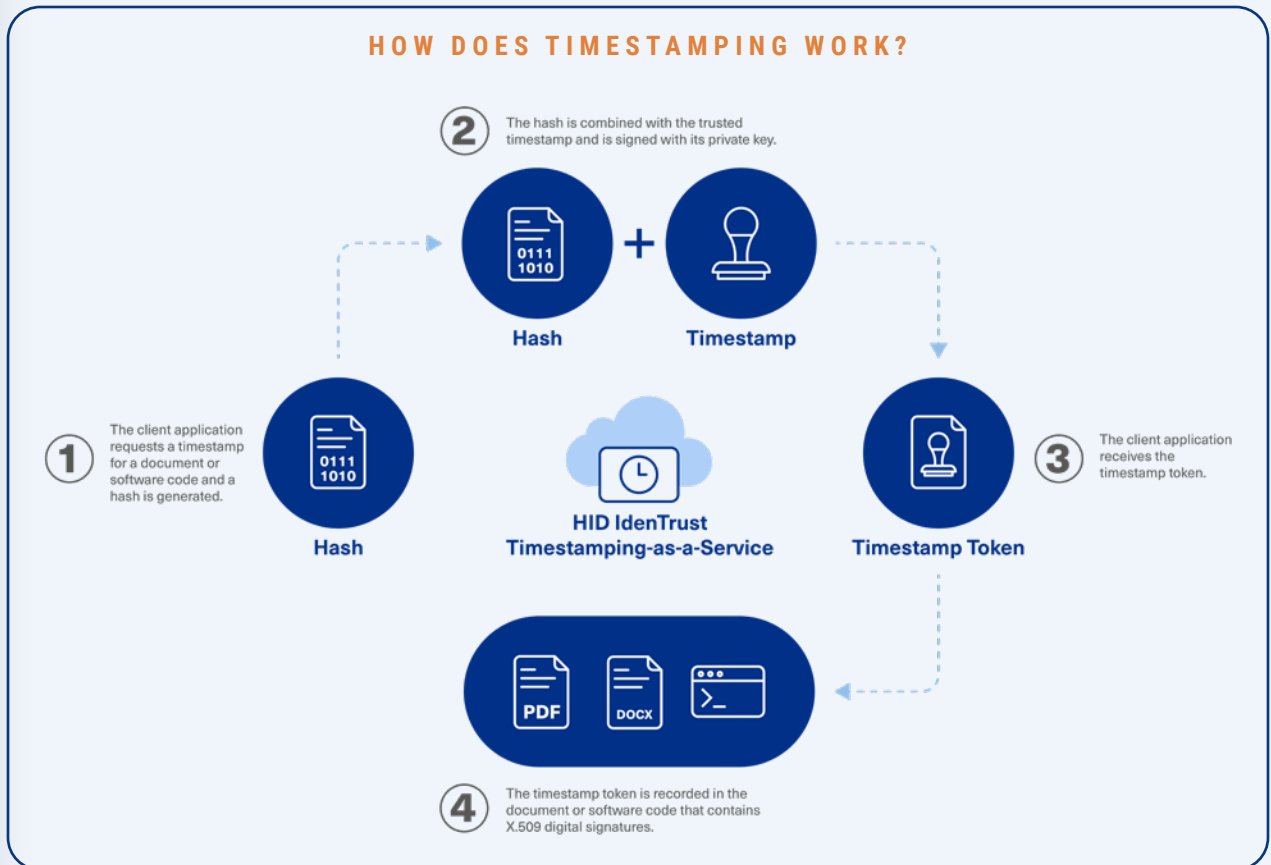
- **RFC 3161 Compliant Timestamp** – Create trusted timestamps with Timestamping Authority (TSA) using any software tool that complies with the RFC 3161 Timestamping Protocol (TSP), such as Microsoft® SignTool and Authenticode and other similar applications
- **Long-Term Signatures** – Reduce risk by adding a timestamp to authenticate digitally signed data for regulatory compliance, financial transactions, and legal evidence
- **Cloud-Based Timestamping-as-a-Service** – Highly available, secure, and audited timestamping service without managing or maintaining any infrastructure

HID TIMESTAMPING-AS-A-SERVICE FEATURES:

- RFC 3161 compliant timestamp
- Works with any application that complies with RFC 3161 such as Microsoft SignTool and Authenticode
- Creates legally binding, and non-repudiation signatures
- Cloud-based deployment eliminates need to manage or maintain any infrastructure
- High availability and redundancy with guaranteed contracted SLAs
- Trusted timestamp is generated using secure FIPS compliant hardware security module
- Low subscription-based pricing based on throughput

TIMESTAMPING CAN BE USED FOR THE FOLLOWING USE CASES:

- Digital document signing
- Software application code signing
- Mobile application code signing
- Firmware signing
- Antivirus signature file signing
- Financial transaction signing
- Insurance claim signing
- Digital media signing



TRUSTED TIMESTAMPS FOR DIGITAL SIGNATURES

Extend the validity of certificates even after they expire. [Talk to an IdenTrust PKI expert for help >>](#)



hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769

Europe, Middle East, Africa: +44 1440 714 850

Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108

For more global phone numbers click here

© 2021 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

2021-08-05-iams-identrust-time-stamping-service-ds-en PLT-06125

Part of ASSA ABLOY