MOBILE-ID
Anytime, Anywhere

TRUSTED HUB

TSA Appliance

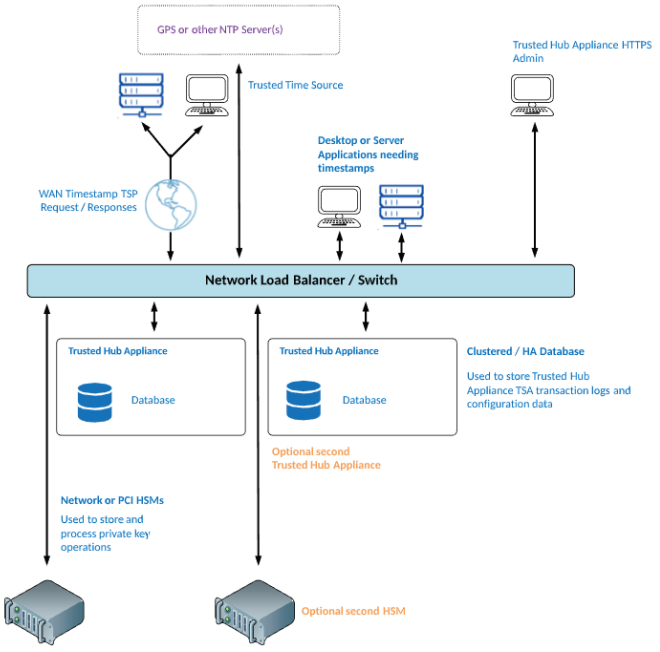
RFC 3161 and Authenticode timestamps

The Trusted Hub TSA Appliance provides independent and irrefutable proof of time for business transactions, e-documents and digital signatures. It can be used to create legal weight evidence that business transactions occurred at a defined moment in time, it can be used to notarize documents and data that they have not been altered since that date/time. It can also independently prove when a digital signature was applied or was accepted so that its validity can be verified even after the expiry or later revocation of a signer's certificate.

Trusted Hub TSA Appliance complies with the IETF RFC 3161 and RFC 5816 specifications and satisfies ETSI TS 101 861 and TS 102 023 requirements for TSA services and supports Microsoft Authenticode. It meets all requirements for an internal enterprise TSA or to power world-class commercial TSA services to multiple third parties. The underlying technology for Trusted Hub TSA Appliance is Mobile-ID™'s well-proven Trusted Hub Appliance, which provides a range of trust services from digital signing, centralized signature verification and certificate validation, notarization/archiving and key management services, all from the same CWA 14167-1 certified product.

Trusted Hub TSA Appliance can be installed in minutes and quickly configured to offer effective timestamp services for a wide variety of needs. It provides very high throughput even using long-length keys and certificates and whilst providing detailed logging for later management analysis.

All timestamp requests and responses are stored in secure sequenced transaction logs. These provide good information for commercial accountability purposes and to meet any legislative or regulatory requirements for timestamp preservation as well as providing effective evidence for normal dispute resolution processes and for any technical issue resolution.



Configuration Options

PCI(e) HSMs can be used with dedicated windows or Linux servers Networked HSMs can be used with Virtualized servers to meet high availability requirements use two Trusted Hub TSA Appliances.

Why use Trusted Hub TSA Appliance

- A highly effective, flexible Time Stamp Authority server designed for use as an Enterprise TSA or as a high volume commercial service TSA
- Supports RFC 3161 TSP and Microsoft Authenticode timestamp protocols
- Can be deployed as a dedicated TSA server or a run with multiple virtualized TSAs within a single server, each with its own TSA signing key and certificate
- Provides very effective timestamp service management with detailed transaction logs with viewing, searching, reporting and archiving options
- Optionally monitors NTP time sources to check TSA server time drift and alert operations staff to time issues and if necessary stop the service
- Optionally controls access by SSL client certificates or allowed or denied IP addresses to ensure that only subscribing users access the service
- Supports strong signing algorithms: RSA 2048 to 8192 bits, ECDSA 256 to 521 bits
- Supports all common hash algorithms including SHA-256/384/512
- Supports FIPS 140-2 and CC EAL4+ HSMs
- Is easy to install, configure and manage using secure web-browser management screens
- Meets the CWA 14167-1 requirements for trustworthy systems including strong role-based access controls for administrators, optional dual controls, detailed and secure transactional, system event & operator activity logging
- Records and archives issued timestamps if required for legislative or regulatory demands or simply as evidence to simplify dispute resolution processes

Key Features

Accountability: Timestamp requestors can be authenticated and specific reports can be produced based on requestor activity within a defined date range for commercial purposes. Trusted Hub TSA Appliance provides detailed reports on authorized usage and also records the timestamp tokens issued.

Proven Technology: Trusted Hub TSA Appliance uses the well proven Trusted Hub Appliance to deliver the underlying platform features such as optional dual controls, secure web-based management screens, event logging, trust anchor management, key and certificate management, secure logging and reporting as well as support for HSMs.

Interoperability: Trusted Hub TSA Appliance has been designed to work with a variety of timestamp clients, including Mobile-ID™ PDF Sign&Seal, PDF Signer Server, XML Signer Server, File Signer Server and third party products including Adobe® Acrobat®.

High-Availability: Trusted Hub TSA Appliance can be easily implemented as a highly available service to meet demanding service level agreement needs. Multiple servers can work in parallel using standard load-balancing techniques and a resilient secondary site can also be established. Network HSMs, system platforms and database management systems can be used as required to meet availability requirements.

Flexible Trust Model: Timestamp server's keys can be self-certified, or a delegated certificate can be issued by an built-in CA module or external CA.

TSA Management: Trusted Hub TSA Appliance has been designed to provide management services for back-end TSA servers. In this capacity it authenticates end-user requests and records all transactions for report generation and billing purposes. The interaction with back-end TSA appliances is invisible to end-users.

TSA Proxy: Mobile-ID™ can optionally provide a local TSA proxy to enable end user or server systems to use a centralized requestor on behalf of the organization. A client SSL certificate is used to allow the requests to be authenticated by the Trusted Hub TSA Appliance.

Maximum Security: Timestamp services can be provided over SSL/TLS with client authentication, Operator access is also controlled with client certificates. Keys can be managed inside a secure FIPS approved HSM. Logs are tamper-evident. Dual control over operator actions is a supported option.

Multiple Instances: A single installation of Trusted Hub TSA Appliance can run multiple TSA profiles each with their time stamping policy and with unique signing keys (e.g. for internal and external communities).

High Performance: Trusted Hub TSA Appliance has been designed for high throughput and can be used in a load-balanced configuration.

Test Tools: TSA Crusher is licensed separately to check TSA performance. TSA Monitor provides continuous Timestamp Server availability monitoring.

This screenshot shows the detail from just one of the management screens, in this case the transaction log viewer for the Timestamp Service.

As can be seen there are sophisticated options for filtering and searching as well as English language detail screens for the viewing the Timestamp protocol request and response messages and the TSA certificate.

TSA Service > Transactions Log Viewer

Showing page 1 of 163

Order by: Log ID | Descending | Current | Go

|< | < | > | >|

Clear Search | Search | Customise Columns | Export Logs | Verify Integrity

Log ID	Response Status	Request Time	Response Time	Policy ID	Request/Response	Subject name of SSL Client Cert	TSA Certificate	Forwarded To	SSL Cert	IP Address	Error Code
141142	granted (0)	2012-04-13 18:29:49.656	2012-04-13 18:29:49.656	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141141	granted (0)	2012-04-13 18:03:31.343	2012-04-13 18:03:31.343	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141140	granted (0)	2012-04-13 18:01:17.656	2012-04-13 18:01:17.656	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141139	granted (0)	2012-04-13 17:49:47.218	2012-04-13 17:49:47.218	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141138	granted (0)	2012-04-13 17:49:32.703	2012-04-13 17:49:32.703	1.1.1.1.1	View	-	View	-	-	188.81.238.21	-
141137	granted (0)	2012-04-13 17:47:49.562	2012-04-13 17:47:49.562	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141136	granted (0)	2012-04-13 17:46:11.765	2012-04-13 17:46:11.765	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-

Trusted Hub TSA Appliance Standards Compliance:

Timestamp standards:	RFC 3161 ETSI TS 101 861 and TS 102 023, Supports RFC3161 TSP and Microsoft Authenticode protocols
Algorithms and keys:	RSA 1024/2048/4096/8192, ECDSA 256/384/521, SHA-1/256/384/512, RIPEMD
PKI standards:	PKCS#10, PKCS#7, PKCS#11, SSL/TLS
For use with:	Code Signing, Timestamped ETSI PAdES/XAdES/CAdES signatures, Document timestamps, LTANS/ERS Archiving
Platforms:	Windows Server 2016/2012 R2/2012/2008 R2, Linux (RedHat, CentOS, SuSe, others), Solaris
Databases:	SQL Server 2016/2014/2012, Oracle 12c/11gR2/11g, PostgreSQL 9/8, MySQL (Percona & Oracle), Azure SQL
HSM support:	PKCS#11 or CAPI/CNG compliant HSMs, smartcards or tokens, Gemalto/SafeNet, Thales, Utimaco, Cloud HSMs including Azure Key Vault, Amazon AWS Cloud HSM