

Elektronische Zeitstempeldienste in Österreich

DDipl.-Ing. Gernot Schmied, MSc
Ing. Wolfgang Fabics
majordomo@iktech.net

E-Government Conference 2006
Linz, 1. Juni 2006

- Zertifikat (*sic!*), das von einem Zertifizierungsdiensteanbieter ausgestellt wird
- mehrere Varianten von *Data Verification Certificates (DVCs)*, z.B.:
 - ***Certification/Proof of Claim of Existence of Data***
Bestätigung, daß das Vorhandensein eines *bestimmten Datums* zu einem *bestimmten Zeitpunkt behauptet* wurde
 - ***Certification/Proof of Existence of Data***
Bestätigung, daß ein *bestimmtes Datum* zu einem *bestimmten Zeitpunkt tatsächlich vorhanden* war
 - ***Certification/Proof of Claim of Possession of Data***
Bestätigung, daß *eine bestimmte Person* den Besitz eines *bestimmten Datums* zu einem *bestimmten Zeitpunkt behauptet* hat
 - ***Certification/Proof of Possession of Data***
Bestätigung, daß *eine bestimmte Person* ein *bestimmtes Datum* zu einem *bestimmten Zeitpunkt tatsächlich besessen* hat
- Die österreichische Gesetzgebung stellt nur auf den unverbindlichsten Fall, nämlich „*Certification/Proof of Claim of Existence of Data*“ ab → RFC 3161

- Bestätigung des Vorhandenseins eines bestimmten Datums („Dokuments“) zu einem bestimmten Zeitpunkt – vgl. § 2 Z 12 SigG
- „*Proof of Existence*“? nein, leider nur ein „*Proof of Claim of Existence*“ (eine Authentifizierung des Benutzers ist ja nicht vorgeschrieben)
- zuverlässige eindeutige Verknüpfung des Zeitstempels mit dem gestempelten Dokument
- Glaubwürdigkeit aufgrund Zeitstempelung durch vertrauenswürdigen (!) Dritten (*Time-Stamping Authority, TSA*)
- Richtigkeit und Genauigkeit der Zeitangabe durch Verwendung zuverlässiger Zeitquellen (z.B. Atomuhr, DCF-77, GPS, NTP)
- ggf. erhöhte Vertrauenswürdigkeit aufgrund technischer & betrieblicher Vorkehrungen („sicherer Zeitstempeldienst“ gem. § 10 SigG)

Wer bräuchte Zeitstempeldienste?

- öffentliche Auftraggeber

„Bei elektronisch übermittelten Angeboten ist der Eingang mittels Zeitstempel im Sinne des § 2 Z 12 SigG festzuhalten.“ (ehem. § 87 Abs 1 BVergG 2002, jetzt §§ 119 Abs 1 & 265 Abs 1 BVergG 2006 sowie § 6 E-Procurement-V)

- Notare bzw. die Notariatskammer

- Führung des Urkundenarchivs sowie des Testaments-, Treuhand- & Teilzeitnutzungsregisters auf elektronischer Basis
- Führung des Zeitstempelregisters (§ 140g NO)

- Wirtschaftstreuhänder, Rechtsanwälte, Ziviltechniker (*jaja, das BRÄG*)...

- verbindliche Dokumentation von Dokumentenständen
- treuhändische Archivierung von elektronischen Dokumenten der Klienten

- Organisationen, die der (internen oder externen) Revision unterliegen (*Haben Sie schon an die Zeitstempelung von Dienstanweisungen gedacht?*)

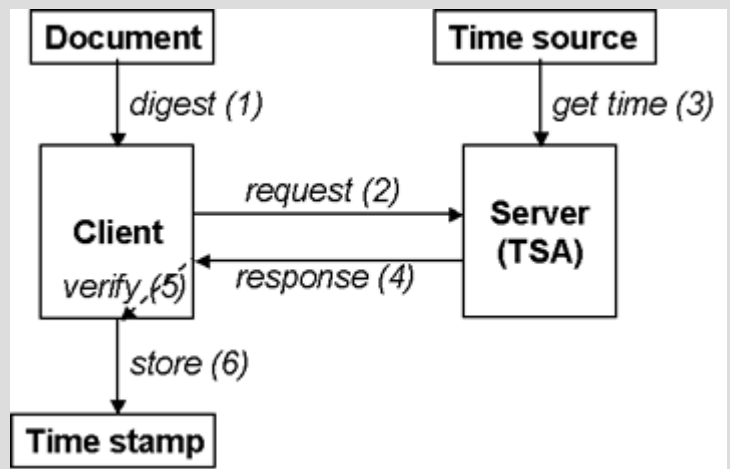
- jeder, für den die offizielle Bestätigung eines Dokumentenstandes von (z.B. urheberrechtlicher) Bedeutung ist

- verwendet X.509-Mechanismen zur Identifikation der TSA
- verwendet eine „*trustworthy source of time*“, was immer das sein mag
- liefert aber **keine** Bestätigung darüber,
 - **was** mit dem Dokument zur bestätigten Zeit passiert ist (Versand, Empfang, Änderung, Druck, Unterschrift...)
 - **wer** den Zeitstempel angefordert hat (d.h. in wessen Besitz sich das Dokument zur bestätigten Zeit befunden hat)
- definiert in erster Linie ein **Protokoll**, das für Zeitstempeldienste verwendet werden kann, nicht notwendigerweise den **Dienst** selbst
- setzt auf weiteren RFCs auf bzw. wird durch diese ergänzt, z.B.
 - RFC 3029 „*Internet X.509 PKI: Data Validation & Certification Server Protocols*“
 - RFC 2459 „*Internet X.509 PKI: Certificate and CRL Profile*“
 - RFC 2510 „*Internet X.509 PKI: Certificate Management Protocols*“
 - RFC 3628 „*Policy Requirements for Time-Stamping Authorities (TSAs)*“
 - RFC 2246 „*The TLS Protocol Version 1.0*“

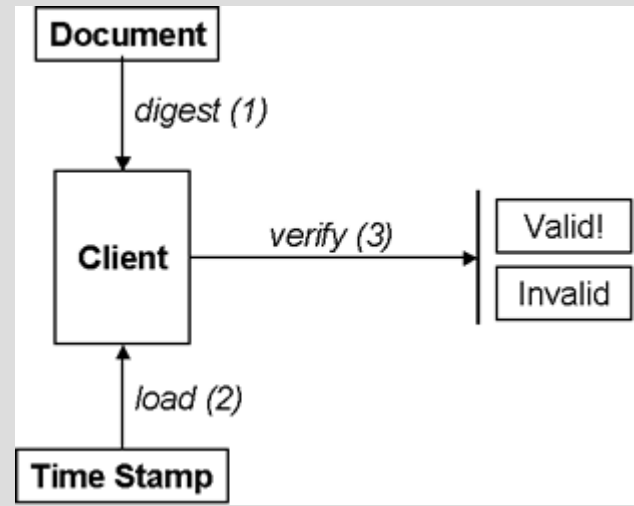
- RFC 3161 spezifiziert ein Applikationsprotokoll, das wahlweise in andere Applikationsprotokolle eingebettet oder über Protokolle unterer Schichten transportiert werden kann.
- TSP via E-Mail
 - MIME-Types „*application/timestamp-query*“ & „*application/timestamp-reply*“
 - Dateinamen sollten der 8+3-Notation gehorchen (*.tsq, *.tsr)
 - Problem: Wie unterscheide ich den Zeitstempel von *Datei1.doc* und *Datei1.pdf*?
- TSP via FBP (*File-Based Protocol*),
 - nur Dateien werden ausgetauscht (*.tsq, *.tsr).
 - FTP drängt sich auf, aber RCP, SCP et al. sind genauso möglich.
- TSP via HTTP/HTTPS
 - MIME-Types wie bei E-Mail, ansonsten normale HTTP(S) requests & replies
- TSP via SBP (*Socket-Based Protocol*)
 - via Socket (z.B. Unix oder TCP), *well-known number 318*
 - erteilt direkte TSR oder Referenz für spätere Abholung (*Polling*)

- Der TStClient erstellt aus dem zu stempelnden Dokument einen Hashwert.
- Der Hashwert wird mit Zusatzinformation versehen und formatiert (*Timestamp Query, TSQ*).
- Die TSQ wird an die TSA übermittelt (HTTP[S], E-Mail, FBP, SBP).
- Die TSA prüft die TSQ und erstellt (falls alles damit OK ist) eine TStInfo.
- Die TSA signiert die TStInfo und formatiert sie (*Timestamp Reply, TSR*)...
agiert somit als Signator bzgl. TStInfo
- Die TSR wird an den Client zurückgesandt.
- Der TStClient kann nun
 - die Signatur der TSA prüfen,
 - den Inhalt von TStInfo auslesen (Datum/Uhrzeit, Genauigkeit, Policy usw.) und
 - aufgrund des mitsignierten Hashwertes den eindeutigen Zusammenhang mit dem ursprünglichen Dokument herstellen.
 - Voilà, der „Zeitstempel“ kann „angebracht“ werden.

Ausstellen des Zeitstempels:



Verifizierung des Zeitstempels:



Quelle: <http://security.polito.it>



- Die Wüste Gobi ist dagegen ein Blumenmeer:

Name des Dienstes	Dienstanbieter	sicherer ZSD
A-CERT Timestamp	ARGE DATEN Österreichische Gesellschaft für Datenschutz	nein
E-Control Timestamping Service	Energie-Control Österreichische Gesellschaft für die Regulierung in der Elektrizitäts- und Erdgaswirtschaft mit beschränkter Haftung	nein
Trodat Seal	Trosoft Entwicklungs- und Vertriebs-GmbH	nein
XiCrypt Time Stamping Services	XiCrypt Internetsicherheitslösungen GmbH	nein

- Es gibt (noch?) keine sicheren Zeitstempeldienste. Woran das wohl liegt?
- Der (geplantermaßen sichere) ZSD des BEV besteht seit 1. November 2004 als Pilotbetrieb. Eine Meldung bei der TKC scheint nicht auf, die weitere Entwicklung ist unklar.

Voraussetzungen für Anbieter

- Anzeige der Dienstaufnahme bei der TKC:

„Auch ein reiner "Zeitstempeldiensteanbieter" ist nach den Begriffsbestimmungen des § 2 Z 10 und 11 als Zertifizierungsdiensteanbieter zu qualifizieren und unterliegt daher der Aufsicht.“ (aus den ErlRV zum SigG)
- Bekanntgabe des Sicherheits- & Zertifizierungskonzepts

„Die bereitgestellten Zeitstempeldienste sind im Sicherheits- und im Zertifizierungskonzept zu beschreiben.“ (aus den ErlRV zum SigG)
- Was beaufsichtigt die TKC hier?
 - Gibt sie die Zertifikate für den Zertifizierungsdiensteanbieter aus (§13 Abs 3 SigG)?

Nein, nicht hier. Für die ZSD verwenden alle Anbieter eigene Zertifikate. Für nicht sichere ZSD ist mehr auch weder technisch noch rechtlich nötig.
 - Sorgt sie für die Einhaltung von Qualitätsstandards (§13 Abs 2 Z1 SigG)?

„Die technische Sachkunde ist insbesondere bei der Bestätigungsstelle (oder den Bestätigungsstellen) nach § 19 konzentriert.“ (ErlRV) – Für nicht sichere ZSD ist die Begutachtung durch die Bestätigungsstelle(n) jedoch gar nicht erforderlich.
 - Übt sie die Aufsicht über die Bestätigungsstelle(n) (§ 13 Abs 2 Z4 SigG) aus?

Nur für sichere ZSD relevant, allerdings ohne Rechtsanspruch der Nutzer und ohne Weisungsbefugnis der TKC gegenüber den Bestätigungsstellen.

Bemerkenswertes (I)

■ § 10 SigG:

„[...] Für sichere Zeitstempeldienste sind technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen und den Anforderungen des § 18 entsprechen.“

■ § 18 SigG:

„Technische Komponenten und Verfahren für sichere Signaturen“

■ Möchte das SigG sichere Zeitstempel tatsächlich an sichere Signaturen binden? Aus den ErlRV zum SigG:

„Sichere Zeitstempeldienste [...] dürfen nur mit geeigneten technischen Komponenten und Verfahren im Sinn des § 18 erstellt werden.“

■ Das wäre problematisch, denn:

- Die Anzeige des signierten Inhalts ist nicht möglich/sinnvoll (§ 18 Abs 2 SigG)
- Die Eingabe von Autorisierungscode ist nicht möglich/sinnvoll (§ 4 Abs 2 SigV)
- Die Personenbindung ist nicht möglich/sinnvoll (§ 2 Z 2 & 3 SigG)

■ Allerdings scheint die SigV nicht wirklich Notiz davon zu nehmen, zumindest ist kein *expliziter* Verweis darauf zu entnehmen.

■ § 14 Abs 2 SigV:

„Die bescheinigte Zeitangabe (Datum und Uhrzeit) hat sich nach Mitteleuropäischer Zeit (MEZ) unter Beachtung der Sommerzeit zu richten; andere Zeitzonen sind ausdrücklich anzugeben [.]“

■ RFC 3161:

„X.690 | ISO/IEC 8825-1 provides the following restrictions for a DER-encoding. The encoding MUST terminate with a "Z" (which means "Zulu" time).“

■ Zum Glück bindet das BEV per Verordnung das, was in Österreich unter MEZ verstanden wird, an die UTC:

„Die Impulsfolge hat der vom Bureau International de l'Heure (BIH) festgelegten koordinierten Weltzeit (UTC) und der Mitteleuropäischen Zeit (MEZ § 1 Zeitzählungsgesetz, BGBl. Nr. 78 / 1976) zu entsprechen.“

■ Brilliant ist die Bestimmung der SigV dennoch nicht. Die Umrechnung von UTC in Lokalzeit sollte – wie im Internet üblich & sinnvoll – auch in der Rechtsnormung den Endsystemen vorbehalten bleiben.

■ § 14 Abs 2 SigV:

„[...] Die Abweichung von der tatsächlichen Zeit darf beim Anbieter des Zeitstempeldienstes höchstens eine Minute betragen.“

■ Was in einer einzigen Minute alles passieren kann:

- 22:38:01 Ein Zeitstempel für ein Dokument wird angefordert.
- 22:38:03 Der Zeitstempel langt ein, Zeitangabe 21:39:02.67 UTC
- 22:38:08 „Oh, das hab‘ ich ja noch vergessen!“
→ Ein Absatz wird aus dem Dokument gelöscht.
- 22:38:09 *Die TSA synchronisiert mit ihrer Referenzuhr!*
bisherige Zeit 21:39:08.21 UTC, neue Zeit 21:38:09.43 UTC
- 22:38:38 Das Dokument wird gespeichert und ein neuer Zeitstempel angefordert.
- 22:38:40 Der Zeitstempel langt ein, Zeitangabe 21:38:39.01 UTC

■ Welches ist nun das letztgültige Dokument? Wurde der Absatz hinzugefügt oder entfernt? Wie beweise ich das im Streitfall?

Es gibt keine rechtlichen Bestimmungen über den *Betrieb* einer TSA, z.B.

- Welche Services werden überhaupt angeboten und welchen Bedingungen müssen sie genügen? Reicht das Sicherheits- & Zertifizierungskonzept dazu tatsächlich aus?
- Welche und wieviele Zeitnormale sind zu verwenden, damit die Zeitquelle der TSA als „*trustworthy*“ gelten kann?
- Welche Zeitsysteme sind überhaupt geeignet? UTC via DCF-77, NTP-Zeit und GPS-Zeit sind nicht dasselbe! Stichworte: *Schaltsekunden*, *Langzeitarchivierung* (*rechtlich* ≤ 30 Jahre, *technisch* ≥ 100 Jahre)
- Wie sind die Zeitquellen der TSA zu konfigurieren und zu betreiben? Stichworte: *skewing* vs. *stepping*, *Kompensation des Zeitsystems*
- Wie sind die erteilten Zeitstempel zu archivieren? Wie können sie von jedermann (!) überprüft werden? Stichworte: *Veröffentlichung*, *Hash Trees*

■ OpenTSA (<http://www.opentsa.org>)

- *OpenSSL Timestamp Patch*: Benützt die etablierte Infrastruktur von OpenSSL und fügt den Befehl „ts“ hinzu, mit dem die ZSD-Funktionen ausgeführt werden können.
- *Apache Timestamp Module*: Setzt auf dem *OpenSSL Timestamp Patch* auf und bietet einen kompletten ZSD-Server via Apache (HTTP & HTTPS). Die erzeugten Zeitstempel können über MySQL oder FireBird Datenbank-Backends archiviert werden.
- *Timestamp Client „tsget“*: einfach zu bedienendes CLI-Programm, das TSA Queries abschicken sowie TSA Replies entgegennehmen kann:

```
$ tsget -h http://localhost:8080/tsa request.tsq
```

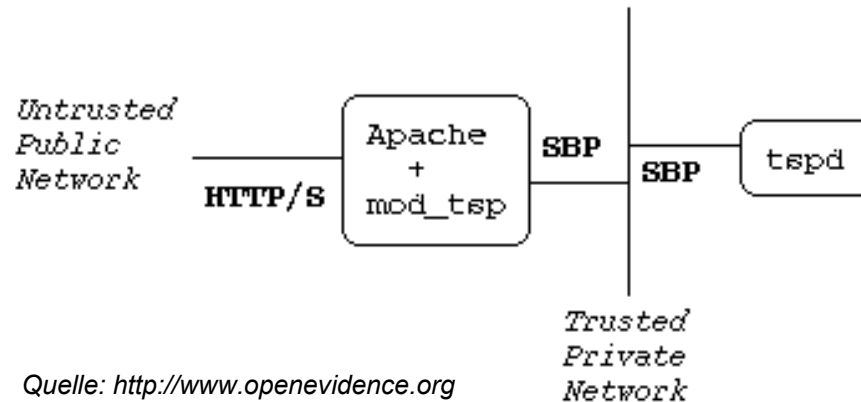
- Ohne *tsget* geht das auch, allerdings etwas umständlicher, z.B. mit dem HTTP(S) Client Tool *curl*:

```
$ openssl ts -query -data letter -cert | tee request.tsq | \  
curl -s -S -H 'Content-Type: application/timestamp-query' \  
--data-binary @- http://localhost:8080/tsa -o response.tsr
```

Quelle für CLI Snippets: <http://www.opentsa.org>

■ OpenEvidence (<http://www.openevidence.org>)

- Bietet einen Timestamp Daemon (*tspd*) gem. RFC 3161, der über das Socket Based Protocol (SBP) angesprochen werden kann.
- Zusatz: *mod_tsp*, ein Apache-Modul, das über SBP mit dem *tspd* kommuniziert und TSA-Funktionalität über HTTP und HTTPS zur Verfügung stellt.



- OpenEvidence bietet aber noch viel mehr, nämlich ein komplettes *Notary Service* einschließlich Dokumenten-Archivierung und –Verifizierung. *Schau'n Sie sich das an!*

kommerzielle Lösungen

- Davon gibt es zuhauf... bitte einfach <http://www.google.at> befragen und die Kreditkarte gut festhalten.



Rakkarsoft L.L.C.



■ „*Tempus edax rerum.*“

Marcus Porcius Cato

A propos: Was halten Sie eigentlich von PGP?

<http://www.itconsult.co.uk/stamper.htm>

Wir freuen uns auf die Diskussion mit Ihnen!