Toward Assured Trusted Time Stamping

Polar Humenn
Gregoritz Lewandowski
Dan Zhou

Center for Systems Assurance
Syracuse University

polar@syr.edu
grlewand@syr.edu
dan@cse.fau.edu

Why do we need assured trusted time?

- Legal non-repudiation of timely interactions
  - Phone calls
  - Monetary transactions
- Electronic notaries
- Assured instrumentation
  - Navigation
  - Secure and trusted operations

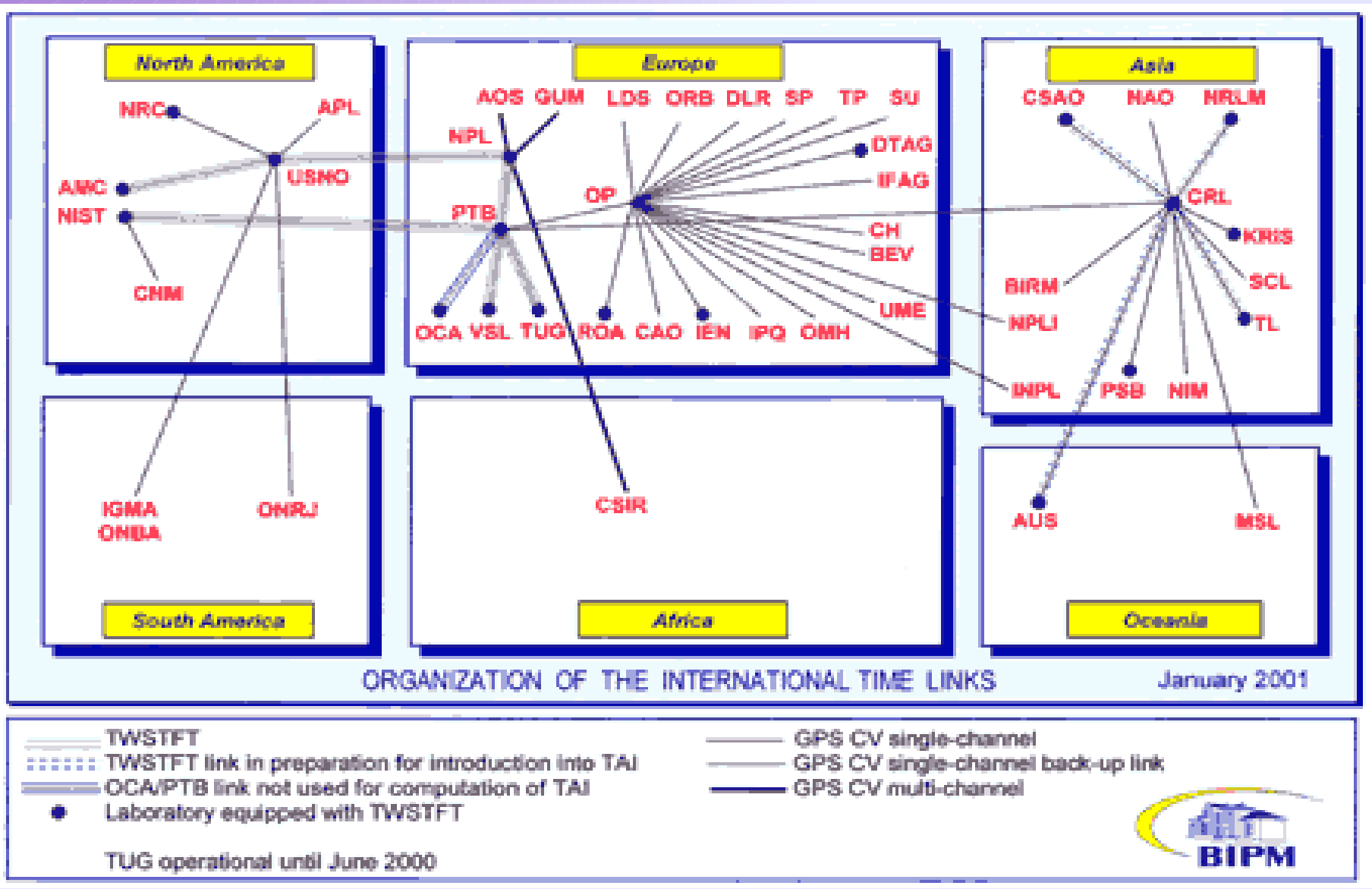
Presentation Agenda

- The time standards
- Oscillators and clocks
- Meeting the time standards
- Formal model of assured time stamping
- Formal properties

What are the time standards?

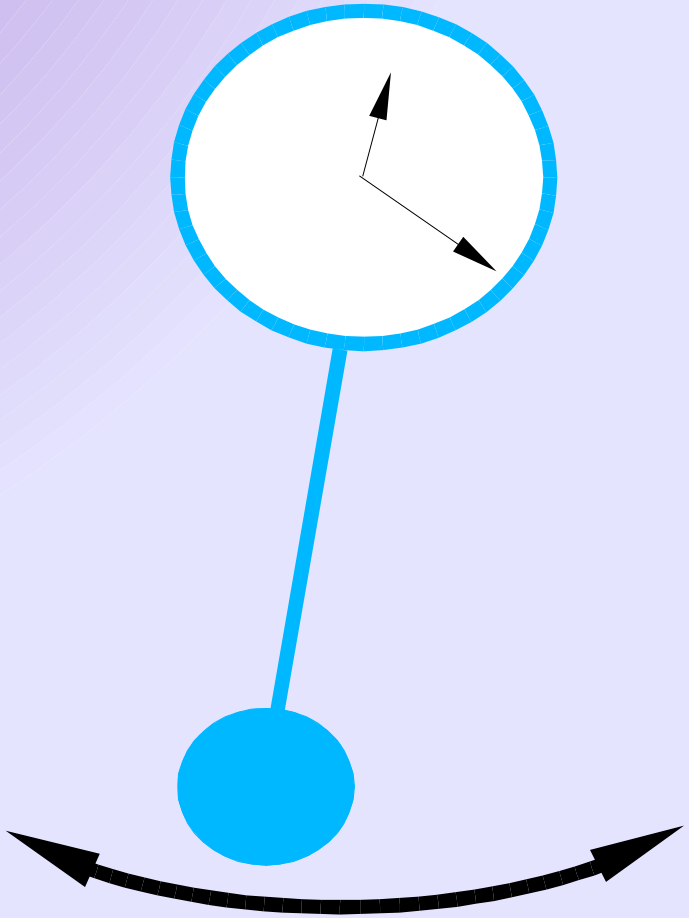
- Time representation comes in many forms.
- Time is the quintessential global standard.
- Several standards exist:
  - TAI (International Atomic Time)
  - UT1 (Universal Astronomical Time)
  - UTC (Universal Coordinated Time)

International Atomic Time

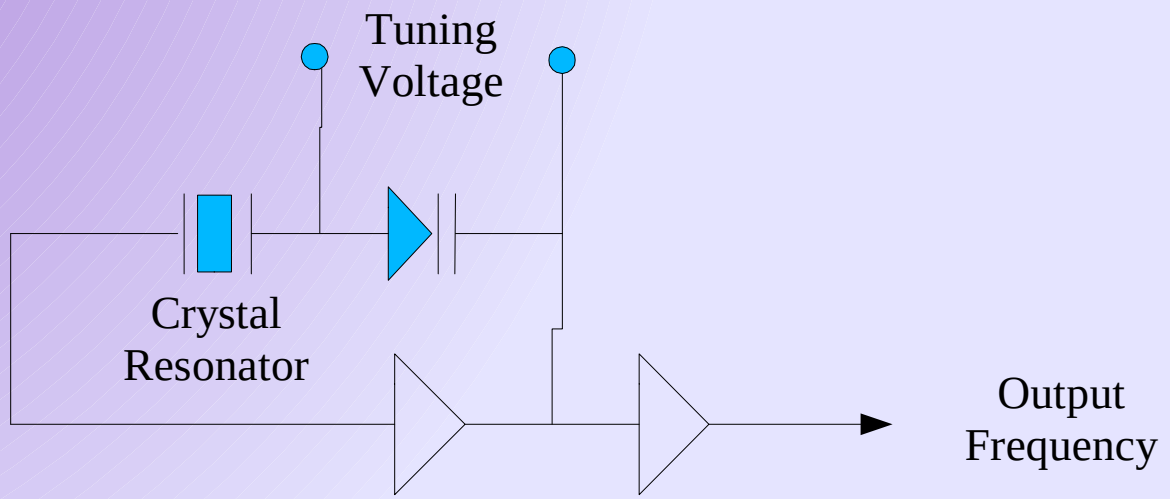


What is a clock?

- A Clock is an oscillator and a counter.



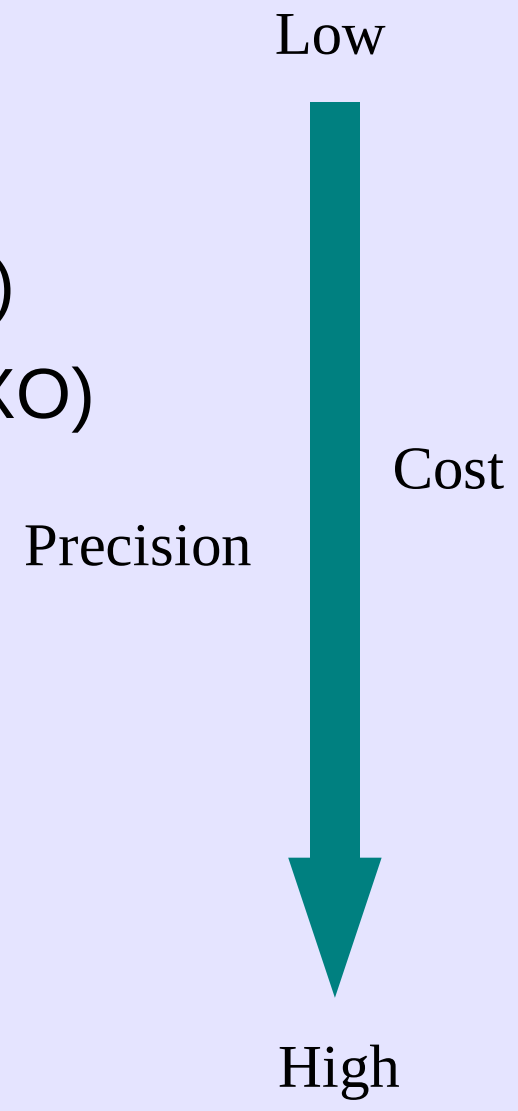
Quartz Oscillator



- Base frequency of crystal is manufactured
  - Size, Mass, Purity
- Frequency is altered by
  - Tuning: Input Voltage
  - Environment: Aging, Temperature, Humidity

Oscillators

- Quartz Oscillators
  - Temperature Compensated (TCXO)
  - Microcomputer Compensated (MCXO)
  - Oven Controlled (OCXO)
- Atomic Oscillators
  - Rubidium
  - Cesium
  - Maser (Hydrogen)



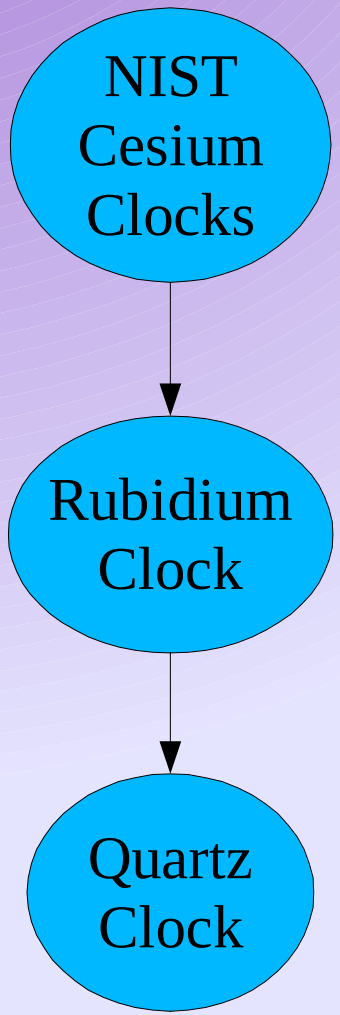
Who maintains the standards?

- Globally
  - Bureau International des Poids de Mesures (BIPM)
- USA
  - National Institute for Standards and Technology (NIST).
  - NIST maintains
    - Ensemble of Cesium oscillators
    - UTC reference

Traceability

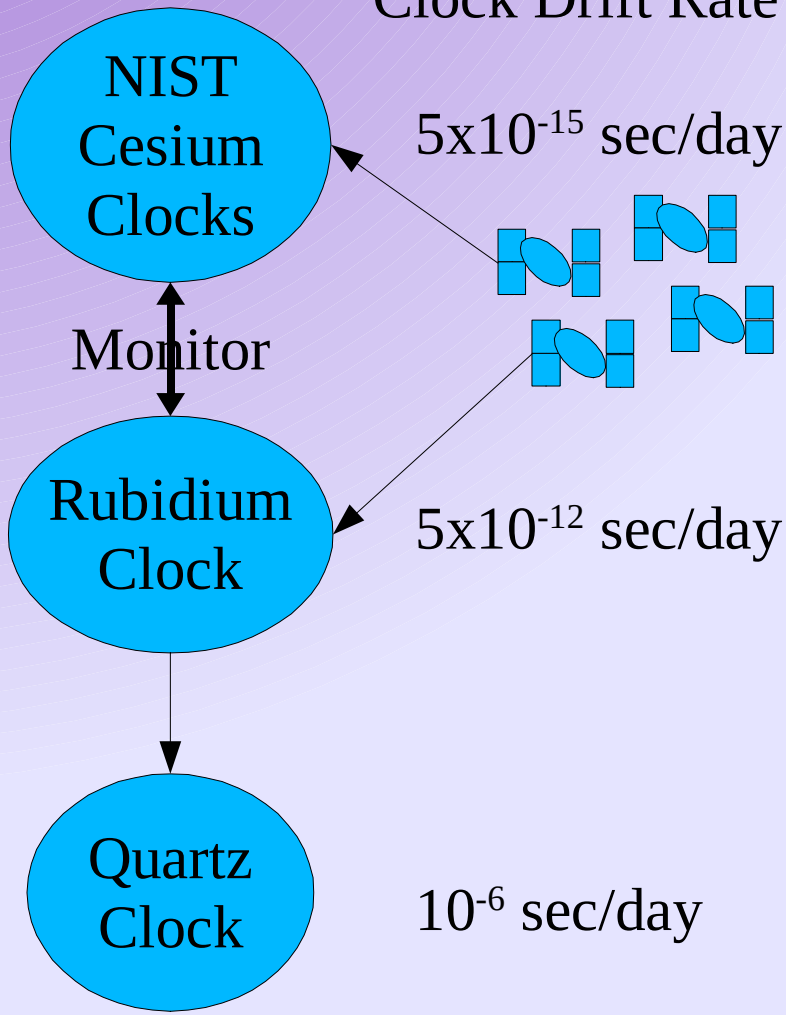
- Data from the Device Under Test (DUT) is compared (traced) to a reference (standard) oscillator of greater performance.
- Traceability (ISO Guide 25)
  - The property of the result of a measurement or the value of a standard whereby it can be related to stated references, usually national or international standards, through an unbroken chain of comparisons all having stated uncertainties.

Traceability



	Clock Drift Rate	Calibration Error NTP
NIST Cesium Clocks	5×10^{-15} sec/day	10^{-6} s
Rubidium Clock	5×10^{-12} sec/day	10^{-6} s
Quartz Clock	10^{-6} sec/day	2×10^{-6} s

Traceability

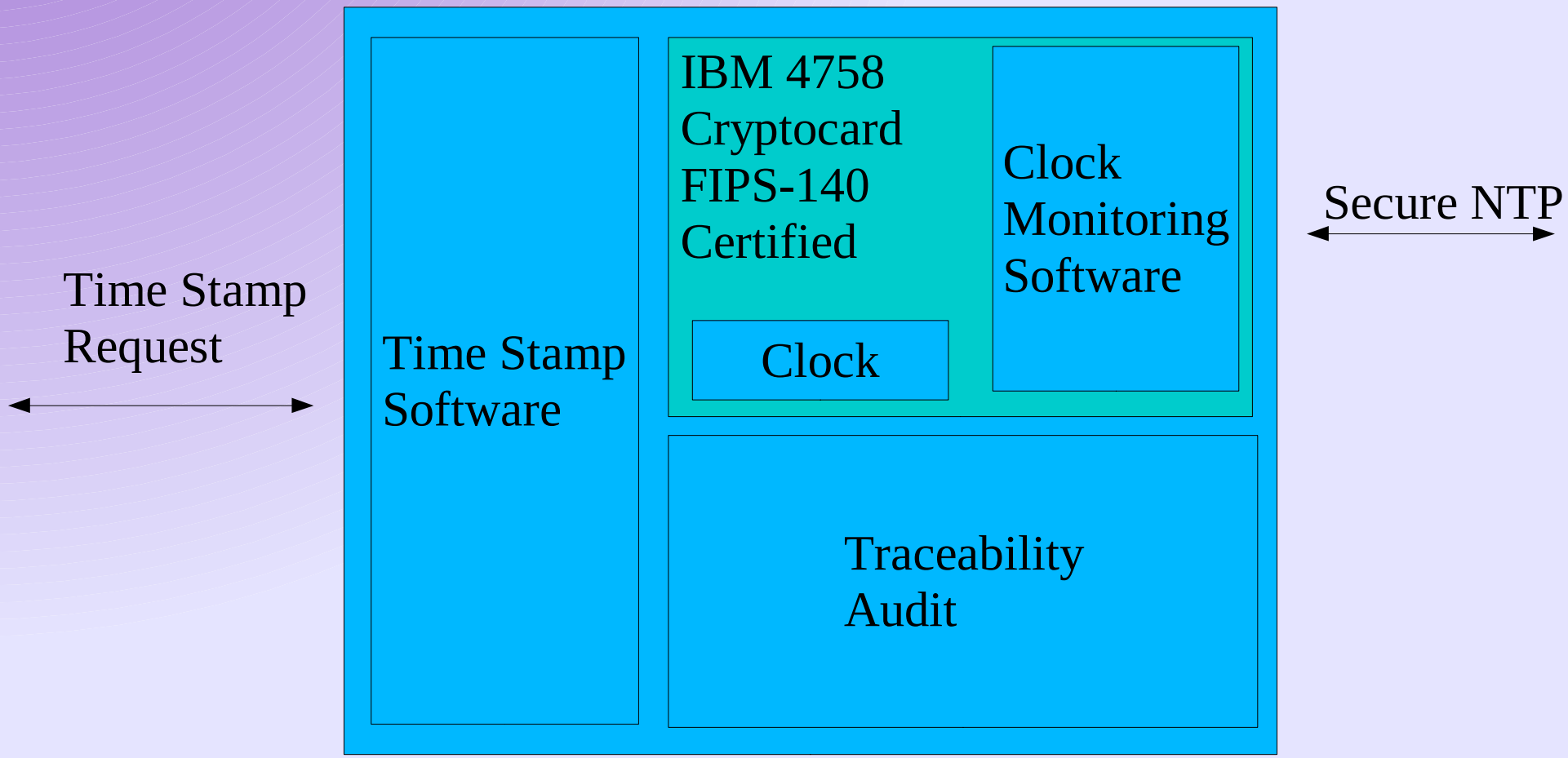


	Clock Drift Rate	Calibration Error GPS/NTP
NIST Cesium Clocks	$5x10^{-15}$ sec/day	
		10^{-13} s
Rubidium Clock	$5x10^{-12}$ sec/day	
		10^{-6} s
Quartz Clock	10^{-6} sec/day	
		10^{-6} s

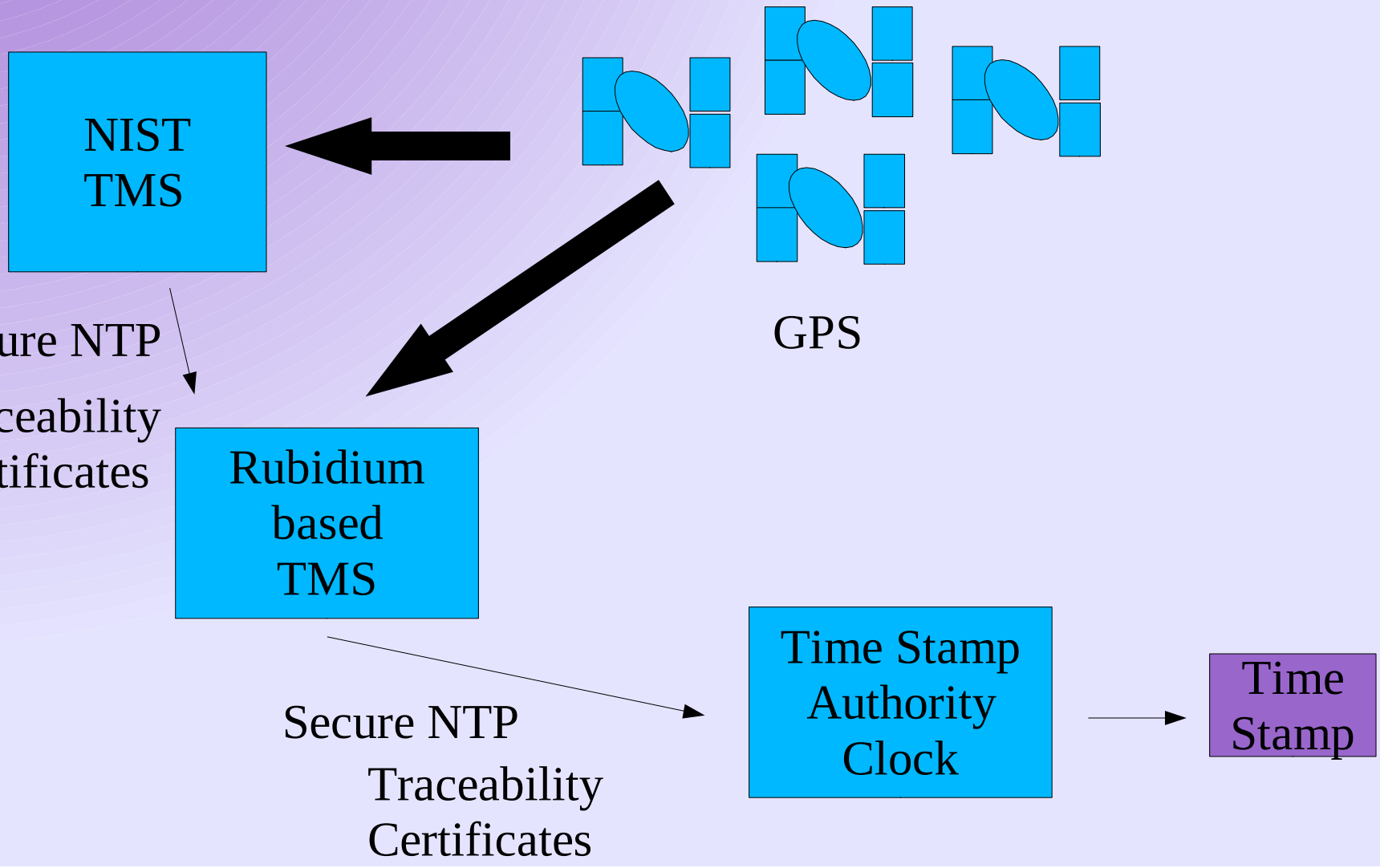
Secure Time Measurement Service

- Proprietary protocol based on NTP
- Issues Traceability Attribute Certificates (TAC)
  - Time of measurement and certification
  - Time offset of lower clock from upper clock
  - NTP path propagation delay (uncertainty)
  - Validity period, digital signature

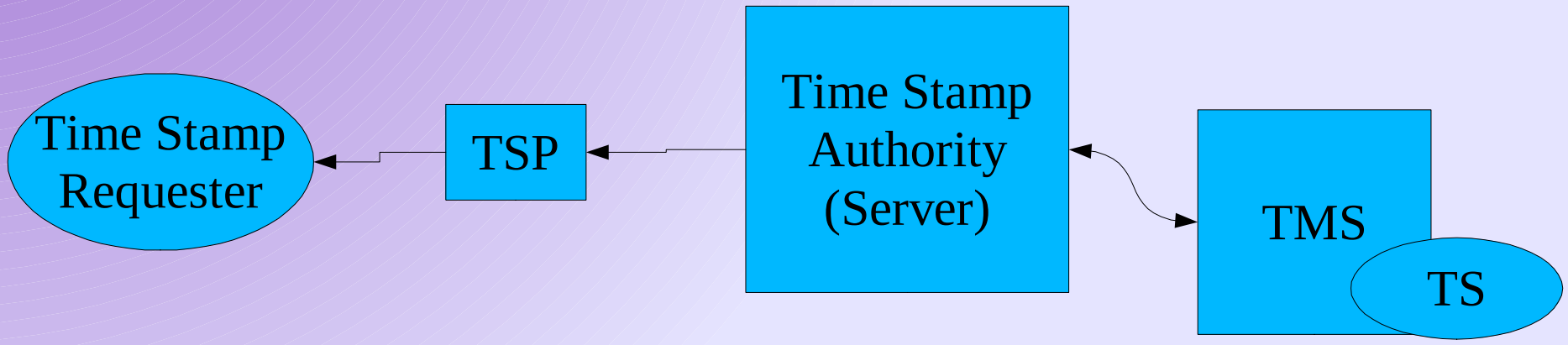
Anatomy of a Trustworthy Time Stamp Authority



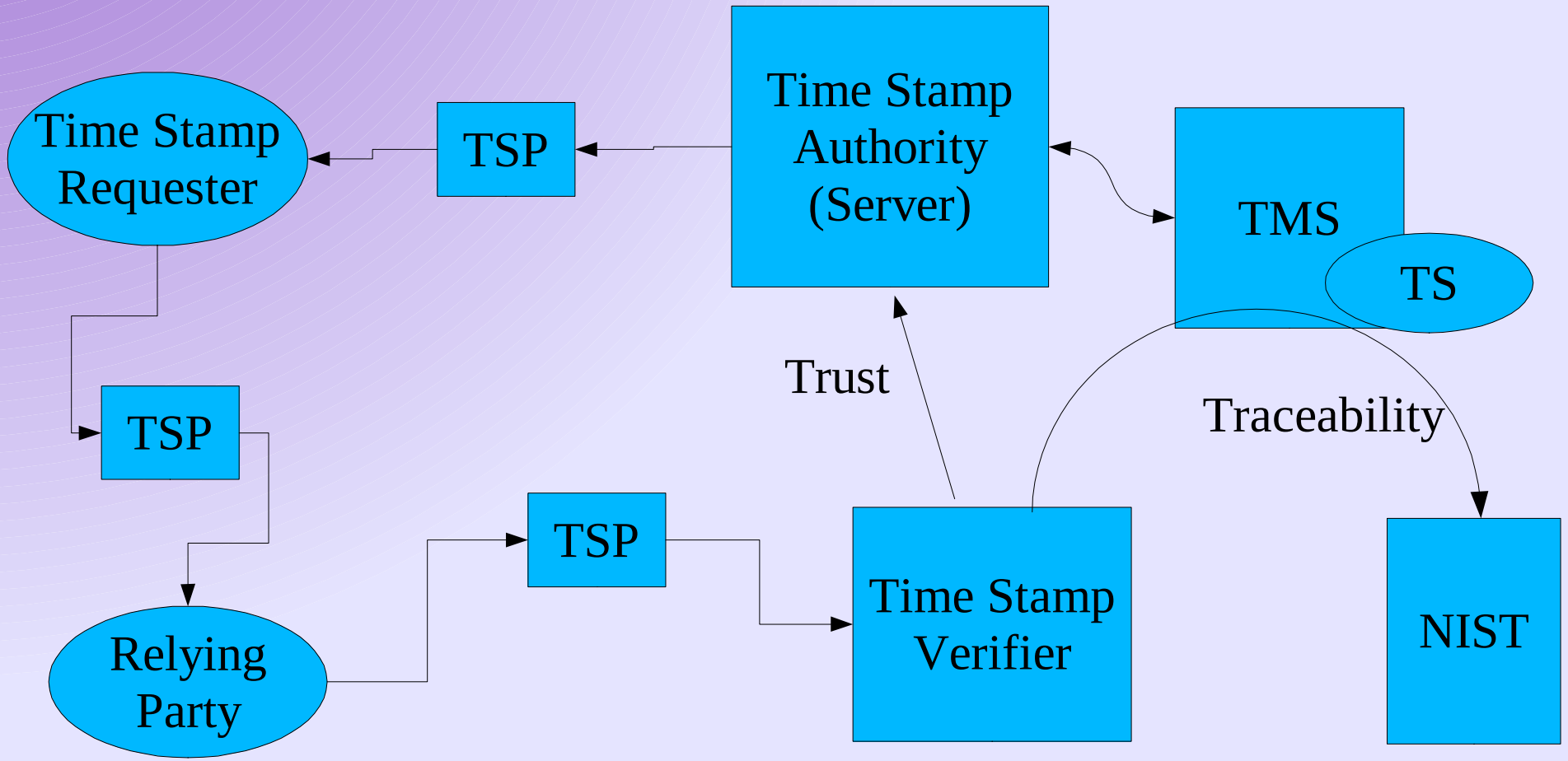
Clock Auditing
Establishing Traceability



Model of the System
Time Stamping

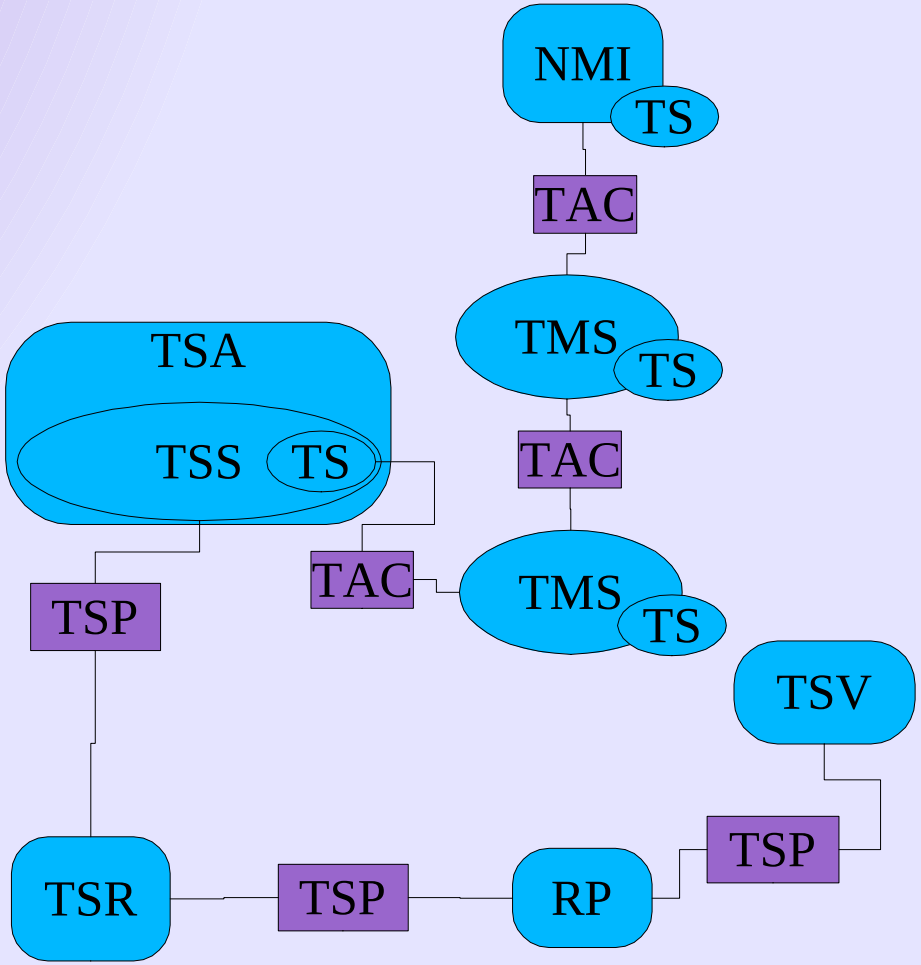


Model of the System
Assured Trusted Time Stamping



Trusted Time Stamp Model

- TSA - Time Stamp Authority
- TSS - Time Stamp Server
- TS - Time Source
- TSR - Time Stamp Requester
- TMS - Time Measurement System
- TSV - Time Stamp Verifier
- NMI - National Metrology Institute
- TAC - Traceability Attribute Certificate
- TSP - Time Stamp
- RP - Relying Party



Formal Uncertainty Properties

- Trust
- Trustworthiness
- Integrity
- Assurance
- Relaxation of trustworthiness

Trust

- A trusts B wrt uncertainty e only if
  - B is trustworthy wrt u
  - e <= u
- A can trust B only if B is trustworthy to an acceptable degree.

Trustworthiness

- A is trustworthy wrt uncertainty e if
  - A has integrity wrt uncertainty q,
  - A has assurance wrt uncertainty r
  - max(q,r) <= e
- A can only be as trustworthy as its the maximum of its uncertainty on its integrity and its assurance.

Integrity

- A has integrity wrt uncertainty e if
  - B **certifies** A has integrity wrt uncertainty e
  - B is trustworthy wrt uncertainty u
  - u <= e
- A has integrity relative to the authority vouching for its integrity.

Assurance

- A has assurance wrt uncertainty e if
  - A uses B with uncertainty d
  - B is trustworthy wrt uncertainty u
  - d + u <= e
- A has assurance of the same degree of its parts plus some error pertaining to the dependence relationship.

Relaxation of Trustworthiness

- A is trustworthy wrt uncertainty e if
  - A is trustworthy wrt uncertainty u
  - u <= e
- A can be arbitrarily more trustworthy than we acknowledge.

Conclusion

- A Relying Party (RP) can trust a Time Stamp (TSP) only if
  - TSP is trustworthy wrt X
    - depends upon the chain of uncertainties about the clocks behind the TSA as well as the TSA itself.
      - $\max(U_{TSA}, U_{TMS1}+...+U_{TMSn}) <= X$
      - X is acceptable to the RP

Experimental Implementation

- Equipment, all IBM 4758 enabled.
  - Secure Rubidium Master Clock with GPS
  - Secure Time Stamp Server
  - Proprietary Secure NTP with TMS at NIST
- CORBA Based Time Stamp Service (TSS)
  - Issues Enhanced RFC 3161 Time Stamps
  - Adiron ORBAsec SL3 Secure ORB (Java)
- Web Server Demonstration Client
  - Asks CORBA TSS for time stamps

Work In Progress

- Implementation
  - Investigate Delays for different Time Stamp Services
- Looking at the "after the fact" notion of time accuracy certification.
  - Uncertainty of a time stamp can be reduced with subsequent TACs.
- Exploration of the trustworthiness metrics with respect to assurance.