Hvordan bli en QTSP?

Qualified Trust Service Provider

John Erik Setsaas
Signicat AS

SIGNICAT

Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice.

This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.

Hvorfor QTSP?

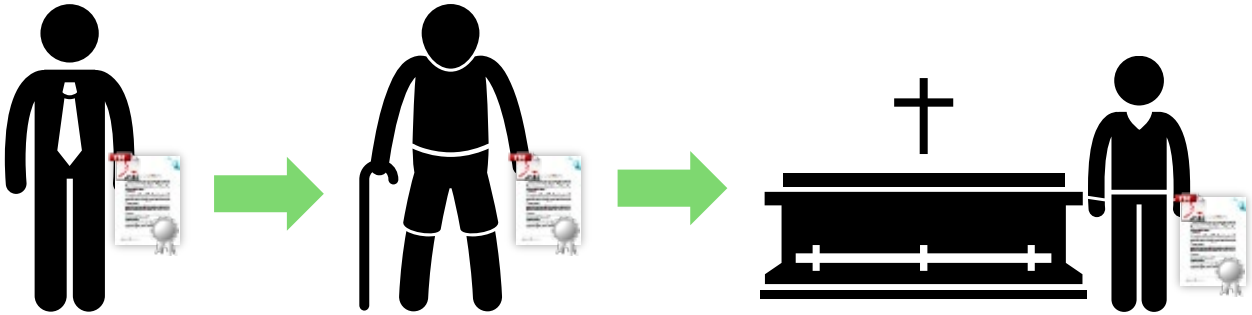
Hvorfor QTSP?

- Signicats kundebase – Regulerte bransjer
  - Høye krav til tillit
- Kvalitetsstempel – EU Trustmark
  - Forenkler kvalifisering av tilbud (tilsvarende ISO27001)

- TSP – Trust Service Provider
  - "Du kan stole på at vi gjør det vi sier vi skal gjøre"
- QTSP – Qualified Trust Service Provider
  - "Vi kan dokumentere at vi gjør det vi sier vi skal gjøre"
  - Auditor + NKOM

Hvorfor QTSA?

- Qualified Time Stamping Authority
- Time Stamping
- Preservering av signature og segl



Verifying the signature in 5, 50 or 500 years

Veien til QTSP

Krav

As managing director of Signicat AS (further referred to as Signicat) I hereby declare that our organization complies with the requirements laid down in:

- ETSI EN 319401 v2.1.1 "General Policy Requirements for Trust Service Providers"
- ETSI EN 319421 v1.1.1 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- Regulation (EU) No 910/2014 (eIDAS) of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, chapter III Trust Services.

Organisasjonsstruktur

Rutiner

Intern audit

Prosesser

Risikovurdering

Kontrakter

Risikohåndtering

Ekstern audit

Policyer

Dokumentasjon

Avtaler

Teknologi

Veien til QTSP

Audit

NKOM

... eller kanskje sånn?

SIGNICAT

basefarm

utimaco®

PrimeKey

bsi.

Justervesenet

Juridisk rådgivning

Økonomisk rådgivning

Nasjonal kommunikasjons-myndighet

Oversikt over kravene fra eIDAS

eIDAS

- 5 Data processing agreement
- 13 Liability and burden of proof
- 15 Accessibility
- 19 Security requirements
  - Risk management – ITIL/ISO27005
  - Notification of security board – ITIL/ISO27005
- 20 Conformity assessment

SIGNICAT

eIDAS

- 24 Requirements
  - Inform supervisory body
  - Employ qualified staff and subcontractors with necessary expertise
  - Financial resources for liability
  - Precise terms and conditions
  - Trustworthy systems (NPR-CEN-TS-419261-2015-v122-20180123_1836)
  - Measures against forgery and theft
  - Logs and audits
  - Termination plan
  - Lawful processing of personal data

SIGNICAT

eIDAS

- 42 QTSA
  - Binding time to data in a way that changes can be detected
  - Based on accurate time source
  - Signed using AES

SIGNICAT

eIDAS

- 5 Data processing agreement
- 13 Liability and burden of proof
- 15 Accessibility
- 19 Security requirements
  - Risk management – ITIL/ISO27005
  - Notification of security board – ITIL/ISO27005
- 20 Conformity assessment

eIDAS

- 24 Requirements
  - Inform supervisory body
  - Employ qualified staff and subcontractors with necessary expertise
  - Financial resources for liability
  - Precise terms and conditions
  - Trustworthy systems (NPR-CEN-TS-419261-2015-v122-20180123_1836)
  - Measures against forgery and theft
  - Logs and audits
  - Termination plan
  - Lawful processing of personal data

eIDAS

- 42 QTSA
  - Binding time to data in a way that changes can be detected
  - Based on accurate time source
  - Signed using AES

Oversikt over kravene fra ETSI 319 421 – Time Stamping

ETSI 319 421 - TSA

- 6.1 Risk assessment
- 6.2 Trust service practice statement
  - Specify
    - » Algorithms
    - » Accuracy of time
    - » Limitations of use
    - » Subscriber's obligations
    - » Verification procedures
    - » Legal requirements
- 6.3 Terms and conditions (ETSI 319 401)
- 6.4 Information security policy (ETSI 319 401)

SIGNICAT

ETSI 319 421 - TSA

- 7.6 Cryptographic controls
  - Protection of signing keys
  - Secure cryptographic device (HSM)
  - Trustworthy systems (ISO/IEC 15408)
  - Requirements from (ISO/IEC 19790)
  - TSU key generation (ETSI 319 312)
  - TSU private key protection (ISO/IEC 15408)
  - Backup of private key
  - TSU public key certificate (ETSI 319 411-1)
  - Rekeying
  - End of TSU life cycle

SIGNICAT

ETSI 319 421 - TSA

- 7.10 Network security
  - Secure zone
  - Remove/disable all unused accounts
  - Restrict to trusted roles
- 7.11 Incident management
- 7.12 Collection of evidence
  - Clock events
- 7.13 Business continuity management
  - Disaster recovery plan
  - Notifications
  - Key compromise handling

SIGNICAT

ETSI 319 421 - TSA

- 6.5 TSA Obligations
  - Subscriber obligations
    - » Verify the time stamp
    - » Take into account any limitations
  - Terms and conditions
- 7 TSA management and operation
  - Legal entity
  - System for quality and information security
  - Sufficient and competent personnel
  - Personnel security (ETSI 319 401)
  - Internal organization (ETSI 319 401)
  - Asset management (ETSI 319 401)

SIGNICAT

ETSI 319 421 - TSA

- 7.7 Time stamping
  - Profile (ETSI 319 422)
  - Time according to UTC(k)
    - » Accuracy < 1s
    - » Threat protection
    - » Leap second management
    - » If outdated – Stop service
  - Certificate validity
- 7.8 Physical and environmental
  - Access control etc (ISO 319 401)
  - Physical access control
  - Authorized personnel

SIGNICAT

ETSI 319 421 - TSA

- 7.14 Termination plan
- 7.15 Compliance
- 8 Additional (eIDAS)
  - Certificate – EUTL
  - QTSA vs TSA – Separate service end-points and policy OID
- Liability

SIGNICAT

ETSI 319 421 - TSA

- 6.1 Risk assessment
- 6.2 Trust service practice statement
  - Specify
    - » Algorithms
    - » Accuracy of time
    - » Limitations of use
    - » Subscriber's obligations
    - » Verification procedures
    - » Legal requirements
- 6.3 Terms and conditions (ETSI 319 401)
- 6.4 Information security policy (ETSI 319 401)

ETSI 319 421 - TSA

- 6.5 TSA Obligations
  - Subscriber obligations
    - » Verify the time stamp
    - » Take into account any limitations
  - Terms and conditions
- 7 TSA management and operation
  - Legal entity
  - System for quality and information security
  - Sufficient and competent personnel
  - Personnel security (ETSI 319 401)
  - Internal organization (ETSI 319 401)
  - Asset management (ETSI 319 401)

ETSI 319 421 - TSA

- 7.6 Cryptographic controls
  - Protection of signing keys
  - Secure cryptographic device (HSM)
  - Trustworthy systems (ISO/IEC 15408)
  - Requirements from (ISO/IEC 19790)
  - TSU key generation (ETSI 319 312)
  - TSU private key protection (ISO/IEC 15408)
  - Backup of private key
  - TSU public key certificate (ETSI 319 411-1)
  - Rekeying
  - End of TSU life cycle

ETSI 319 421 - TSA

- 7.7 Time stamping
  - Profile (ETSI 319 422)
  - Time according to UTC(k)
    - » Accuracy < 1s
    - » Threat protection
    - » Leap second management
    - » If outdated – Stop service
  - Certificate validity
- 7.8 Physical and environmental
  - Access control etc (ISO 319 401)
  - Physical access control
  - Authorized personnel

ETSI 319 421 - TSA

- 7.10 Network security
  - Secure zone
  - Remove/disable all unused accounts
  - Restrict to trusted roles
- 7.11 Incident management
- 7.12 Collection of evidence
  - Clock events
- 7.13 Business continuity management
  - Disaster recovery plan
  - Notifications
  - Key compromise handling

ETSI 319 421 - TSA

- 7.14 Termination plan
- 7.15 Compliance
- 8 Additional (eIDAS)
  - Certificate – EUTL
  - QTSA vs TSA – Separate service end-points and policy OID
- Liability

Oversikt over kravene fra ESI 319 401 – Generelt for QTSP

ETSI 319 401

- 5. Risk assessment
- 6.1 Trust service practice (TSP) statement
  - Set of policies and practices
  - Procedures used to address the requirements
  - Identity obligations of all external organizations
  - Make available to subscribers and relying parties
  - Management body with overall responsibility
  - Implement all practices
  - Review process for the implementation
  - Notification of changes to practices
  - Provision for termination services

SIGNICAT

ETSI 319 401

- 6.2 Terms and conditions
  - Available to all subscribers and relying parties
  - Trust policy
  - Limitations of use
  - Subscribers obligations
  - Information for subscribers and relying parties
  - Retention of logs
  - Limitations of liability and use of service
  - Applicable legal system
  - Procedures for complaints and settlements
  - Conformance assessment scheme
  - TSP contact information
  - Undertaking regarding availability

SIGNICAT

ETSI 319 401

- 6.3 Information security policy
  - Information security policy approved by management
  - Communication of changes
  - Documented, implemented, maintained
  - Responsibility for conformance with procedures
  - Planned reviews

SIGNICAT

ETSI 319 401

- 7.1 Internal organization
  - Reliability
  - Trust service practices
  - Financial resources for liability
  - Financial stability
  - Procedures and policies for handling complaints and disputes
  - Documented agreement, including subcontracting
  - Segregation of duties

SIGNICAT

ETSI 319 401

- 7.2 Human resources
  - Employees and contractors support the trustworthiness of the TSP
  - Staff shall have required training (formal or acquired)
  - Disciplinary actions for violations
  - Security roles and responsibilities clearly identified
  - Clear job descriptions
  - Procedures shall be followed
  - Management processes
  - Free of conflict of interest
  - Trusted roles
    - Security officers, System administrators, System operators, System auditors
    - Formally appointed
    - Least privilege principle
    - Also for contractors and suppliers

SIGNICAT

ETSI 319 401

- 7.3 Asset management – media handling
- 7.4 Access control
  - Limited to authorized roles
  - Firewalls
  - Administration of user access (incl removal)
  - Restriction of access to information and systems
  - Authentication (two-factor)
  - Accountability of employees
  - Protection of sensitive data
- 7.5 Cryptographic controls
  - Appropriate security controls for protection of key materials

SIGNICAT

ETSI 319 401

- 7.6 Physical security
  - Physical access control w/limited access
  - Controls to avoid loss, damage, theft or compromise
  - Controls to limit interruption of business services
  - Critical components in protected environments
    - Security perimeters
    - Alarms

SIGNICAT

ETSI 319 401

- 7.7 Operation security
  - Use trustworthy systems (ISO27002:2013)
  - Protected against modifications
  - Analyzes of security requirements
  - Change control procedures
  - Protection against viruses, malicious and unauthorized software
  - Media to be protected from theft, damage and unauthorized access
  - Media to be protected from deterioration
  - Procedures for all roles
  - Security patches
    - Applied within reasonable time
    - Does not introduce instabilities
    - Documentation in case of not implementing

SIGNICAT

ETSI 319 401

- 7.8 Network security
  - Segmentation – functional, logical, physical
  - Restrict access between segments
    - Regular review
  - Critical TSP systems in secure zone(s)
  - Dedicated administration network
  - Secure channels
  - Redundancy for administration access
  - Regular vulnerability scans
  - Regular penetration tests

SIGNICAT

ETSI 319 401

- 7.9 Incident handling
  - System monitoring
  - Do not expose sensitive data
  - Abnormal activities shall cause alarms
  - Monitoring – Start/stop of logging functions, utilization of services
  - Trusted personnel to follow up on alarms
  - Procedures for notification
    - Relying parties – Supervisory body
    - Loss of integrity
  - Regular review of audit logs
  - Vulnerability issues to be addressed (within 48 hours)
  - Incident reporting – Minimize damage (within 24 hours)

SIGNICAT

ETSI 319 401

- 7.10 Collection of evidence
  - Log retention
  - Sensitive
  - Archived according to business processes
  - Shall be made available in case of legal proceedings
  - Time source synchronization
  - Backup and held according to requirements
  - Integrity of the logs

SIGNICAT

ETSI 319 401

- 7.11 Business continuity
  - Plan for disaster recovery
- 7.12 Termination plan
  - Minimize the damage in case of termination of business
    - Notification
    - Transfer of obligations to other parties
    - Exporting of information
  - Financial agreements – cover cost of the above
- 7.13 compliance
  - Legal requirements
  - Accessible to persons with disabilities
  - Data processing agreement (95/46/EC)

SIGNICAT

SIGNICAT

ETSI 319 401

- 5. Risk assessment
- 6.1 Trust service practice (TSP) statement
  - Set of policies and practices
  - Procedures used to address the requirements
  - Identity obligations of all external organizations
  - Make available to subscribers and relying parties
  - Management body with overall responsibility
  - Implement all practices
  - Review process for the implementation
  - Notification of changes to practices
  - Provision for termination services

ETSI 319 401

- 6.2 Terms and conditions
  - Available to all subscribers and relying parties
  - Trust policy
  - Limitations of use
  - Subscribers obligations
  - Information for subscribers and relying parties
  - Retention of logs
  - Limitations of liability and use of service
  - Applicable legal system
  - Procedures for complaints and settlements
  - Conformance assessment scheme
  - TSP contact information
  - Undertaking regarding availability

ETSI 319 401

- 6.3 Information security policy
  - Information security policy approved by management
  - Communication of changes
  - Documented, implemented, maintained
  - Responsibility for conformance with procedures
  - Planned reviews

ETSI 319 401

- 7.1 Internal organization
  - Reliability
  - Trust service practices
  - Financial resources for liability
  - Financial stability
  - Procedures and policies for handling complaints and disputes
  - Documented agreement, including subcontracting
  - Segregation of duties

ETSI 319 401

- 7.2 Human resources
  - Employees and contractors support the trustworthiness of the TSP
  - Staff shall have required training (formal or acquired)
  - Disciplinary actions for violations
  - Security roles and responsibilities clearly identified
  - Clear job descriptions
  - Procedures shall be followed
  - Management processes
  - Free of conflict of interest
  - Trusted roles
    - » Security officers, System administrators, System operators, System auditors
    - » Formally appointed
    - » Least privilege principle
    - » Also for contractors and suppliers

ETSI 319 401

- 7.3 Asset management – media handling
- 7.4 Access control
  - Limited to authorized roles
  - Firewalls
  - Administration of user access (incl removal)
  - Restriction of access to information and systems
  - Authentication (two-factor)
  - Accountability of employees
  - Protection of sensitive data
- 7.5 Cryptographic controls
  - Appropriate security controls for protection of key materials

ETSI 319 401

- 7.6 Physical security
  - Physical access control w/limited access
  - Controls to avoid loss, damage, theft or compromise
  - Controls to limit interruption of business services
  - Critical components in protected environments
    - » Security perimeters
    - » Alarms

ETSI 319 401

- 7.7 Operation security
  - Use trustworthy systems (ISO27002:2013)
  - Protected against modifications
  - Analyzes of security requirements
  - Change control procedures
  - Protection against viruses, malicious and unauthorized software
  - Media to be protected from theft, damage and unauthorized access
  - Media to be protected from deterioration
  - Procedures for all roles
  - Security patches
    - » Applied within reasonable time
    - » Does not introduce instabilities
    - » Documentation in case of not implementing

ETSI 319 401

- 7.8 Network security
  - Segmentation – functional, logical, physical
  - Restrict access between segments
    - » Regular review
  - Critical TSP systems in secure zone(s)
  - Dedicated administration network
  - Secure channels
  - Redundancy for administration access
  - Regular vulnerability scans
  - Regular penetration tests

ETSI 319 401

- 7.9 Incident handling
  - System monitoring
  - Do not expose sensitive data
  - Abnormal activities shall cause alarms
  - Monitoring – Start/stop of logging functions, utilization of services
  - Trusted personnel to follow up on alarms
  - Procedures for notification
    - » Relying parties – Supervisory body
    - » Loss of integrity
  - Regular review of audit logs
  - Vulnerability issues to be addressed (within 48 hours)
  - Incident reporting – Minimize damage (within 24 hours)

ETSI 319 401

- 7.10 Collection of evidence
  - Log retention
  - Sensitive
  - Archived according to business processes
  - Shall be made available in case of legal proceedings
  - Time source synchronization
  - Backup and held according to requirements
  - Integrity of the logs

ETSI 319 401

- 7.11 Business continuity
  - Plan for disaster recovery
- 7.12 Termination plan
  - Minimize the damage in case of termination of business
    - » Notification
    - » Transfer of obligations to other parties
    - » Exporting of information
  - Financial agreements – cover cost of the above
- 7.13 compliance
  - Legal requirements
  - Accessible to persons with disabilities
  - Data processing agreement (95/46/EC)

Erfaringer

ISO27001 var en fordel

Styringssystemet for informasjonssikkerhet
er helt nødvendig

Kravene til en QTSP er mye større og mer krevende

Etabler QTSP-organisasjonen så tidlig som mulig

Slik at denne både får et eierskap til prosessen og blir en drivkraft i denne

Ta rådet/formaningen om å forankre prosessen hos ledelsen, på største alvor

QTSP påvirker og involverer
store deler av organisasjonen

Kreves stort momentum for å gjennomføre

Ikke gå ut fra at underleverandører har relevant kompetanse

Tett dialog om leveranser

Tilpasning til nytt direktiv

Ting (prosedyrer, maskinvare, programvare) som er godkjent under gamle krav kan kreve utvidelser for fungere under det nye regelverket

Ta kravet om å bygge opp intern kompetanse alvorlig

Analysere hvert krav svært nøye

Trenger (bred) felles intern forståelse for oppfyllelse av hvert krav

Pinlig nøyaktig dokumentasjon av implementasjon

Auditor er en ekstremt nyttig resurs

Spørsmål

John Erik Setsaas

VP of Identity and Innovation

jsetsaas

john.erik.setsaas@signicat.com

SIGNICAT