GUIDE TO CHOOSE THE RIGHT PKI VENDOR FOR EU TRUST SERVICE PROVIDERS

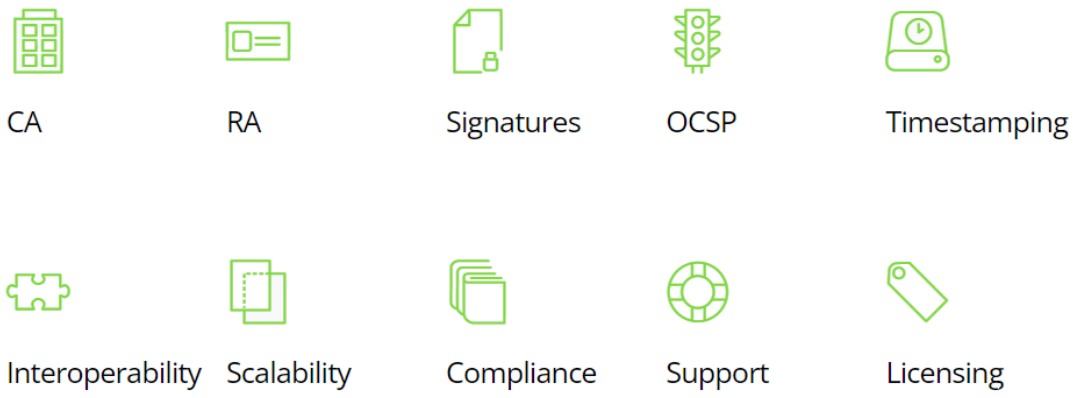
In today's rapidly evolving digital landscape, trust and security are more critical than ever. According to a 2023 study by the European Union Agency for Cybersecurity (ENISA), Cyberattacks targeting digital trust services increased by 35% in the past year alone, highlighting the urgent need for robust security frameworks.

Cyberattacks targeting digital trust services increased by 35% in the past year alone – Enisa

Trust Service Providers (TSPs) play a pivotal role in fostering trust and confidence in the digital ecosystem by delivering a wide range of trust services to individuals, businesses, and governments. At the heart of these services lies Public Key Infrastructure (PKI), a foundational framework for managing digital certificates and cryptographic keys.

This checklist is designed to assist companies aspiring to become European Trust Service Providers or those that are already TSPs in evaluating and selecting the right PKI software. By following our comprehensive checklist, TSPs can make informed decisions, ensuring they choose a PKI solution that empowers them to deliver reliable, secure, and compliant trust services to their clients.

This checklist is organized into 10 distinct areas for comprehensive coverage:



Which services do Trust Service Providers typically select?

Before focusing on the checklist, lets first summarize the list of digital trust services a European Trust Service Provider might go for. These services are group in two categories **Qualified** or **Non-Qualified** trust services.

Qualified certificates are issued in accordance with the Electronic Identification, Authentication and Trust Services (eIDAS) regulation in the European Union, providing a higher level of assurance for electronic signatures, seals, and authentication.

Qualified	Advanced / Non-Qualified
1. **QCert** for ESign Qualified certificate for electronic signature 2. **QCert** for ESeal Qualified certificate for electronic seal 3. **QWAC** Qualified certificate for website authentication 4. **QVal** for QESign Qualifie1d validation service for qualified electronic signature 5. **QVal** for QESeal Qualified validation service for qualified electronic seal 6. **QPres** for QESign Qualified preservation service for qualified electronic signature 7. **QPres** for QESeal Qualified preservation service for qualified electronic seal 8. **QTimestamp** Qualified time stamp 9. **QeRDS** Qualified electronic registrered delivery service	1. Certificate for electronic signature 2. Certificate for electronic seal 3. Certificate for website authentication 4. Validation service for electronic signature 5. Generation service for electronic signature 6. Preservation service for electronic signature 7. Validation service for electronic seal 8. Generation service for electronic seal 9. Preservation service for electronic seal 10. Time stamp service 11. Electronic registrered delivery service 12. Non-regulatory, nationally defined trust service

In essence, these services are focusing on two main groups:

- Certificate issuance, requiring:
  - CA
  - RA
  - OCSP

- Digital signature creation or verification, requiring:
  - Signing
  - Verification
  - Timestamping
  - Preservation

Let us delve deeper into each of these requirements to elucidate specific criteria.

Certificate Authority (CA) Functionality

A Certificate Authority (CA) serves as the cornerstone of a Trust Service Provider (TSP), enabling the issuance of crucial digital identities in the form of digital certificates. TSPs have the flexibility to either establish their own Root CA or opt to have subordinate CAs issued by external TSPs, ensuring a robust framework for digital trust and identity management.

Check List

1. **Certificate Templates:** Can the CA software support customizable certificate templates to accommodate different use cases and certificate policies?

2. **Certificate Revocation Management:** Does the software offer robust mechanisms for managing certificate revocation, including Certificate Revocation Lists (CRLs) & Online Certificate Status Protocol (OCSP)?

3. **Hierarchical CA Support:** Is the CA software capable of managing hierarchical CA structures for delegation of certificate issuance and management responsibilities?

4. **Certificate Types:** Can the CA support different types of certificates such as:
    - SSL/TLS
    - Document Signing
    - Qualified Certificates (eIDAS Compliant)
    - Email Signing & Encryption
    - Code Signing
    - Time Stamping

Registration Authority (RA) Features

A Registration Authority (RA) complements the Certificate Authority (CA) in the operations of a Trust Service Provider (TSP), facilitating seamless enrolment, validation, and management of digital certificates. As an essential component of the TSP ecosystem, the RA interfaces with users and systems, verifying identity credentials and ensuring compliance with certificate issuance policies. Whether integrated within the TSP infrastructure or outsourced to specialized providers, the RA plays a pivotal role in upholding the integrity and reliability of digital identities within the trust framework.

Check List

1. **Authentication Methods:** Does the RA software support multiple authentication methods, such as username/password, two-factor authentication (2FA), or client certificates?

2. **Audit Trails:** Can the RA software generate comprehensive audit trails and logs for all certificate-related activities, including enrolment, validation, and revocation?

3. **Self-Service Enrolment:** Is there support for self-service certificate enrolment capabilities, allowing users to request and manage their certificates through a user-friendly interface?

4. **Vetting Workflow:** Does the RA software support vetting life cycle for requested certificates avoiding wrong certificate issuance?

5. **Certificate Issuance:** Does the RA software allow certificate issuance using multiple options i.e.
    - Manual submission of CSR/PKCS#10
    - Certify eys generated in Crypto/USB tokens
    - Cerify keys generated on the server

OCSP Support

In the realm of Trust Service Providers (TSPs), the Online Certificate Status Protocol (OCSP) serves as a critical mechanism for real-time verification of digital certificate validity. Operating in tandem with the Certificate Authority (CA), the OCSP responder promptly responds to certificate status queries, ensuring the authenticity and integrity of digital transactions. As an indispensable component of the TSP infrastructure, OCSP plays a vital role in maintaining the trustworthiness of digital certificates, bolstering the security posture of the digital ecosystem.

Check List

1. **High Availability:** Does the OCSP responder software provide built-in high availability and failover capabilities to ensure continuous availability of certificate status checking services?

2. **Load Balancing:** Can the OCSP responder be configured for load balancing across multiple servers to distribute incoming certificate status queries evenly?

3. **Performance Monitoring:** Does the OCSP responder offer performance monitoring and reporting features to track response times, throughput, and server health metrics? Checkout our blog on 7 OCSP challenges and how to overcome them.

Timestamping Functionality

Timestamping stands as a cornerstone function within the operations of a Trust Service Provider (TSP), enabling the generation of trusted timestamps that authenticate the temporal integrity of digital data. By affixing precise timestamps to electronic documents, transactions, and records, TSPs provide irrefutable proof of data existence and integrity at specific points in time. Integral to regulatory compliance, legal admissibility, and data integrity assurance, timestamping services offered by TSPs serve as a cornerstone of trust in the digital realm, facilitating secure and reliable interactions across diverse domains.

Check List

1. **Client Authentication:** Can the timestamping service support multiple authentication options like Basic and CMS Authentication?

2. **NTP support:** Other than machine time, can the timestamp use its time source from a single or multiple secure NTP servers?

3. **Auditability:** Can the timestamping service generate audit logs and reports to demonstrate compliance with regulatory requirements and audit trail integrity?

4. **High Availability:** Does the Timestamp software provide built-in high availability and failover capabilities to ensure continuous availability?

5. **Client Management & Reporting:** Can the timestamp service handle client management, quota management and reporting of timestamp requests across multiple timestamp servers?

Digital Signing and Verification Tools

Within the arsenal of a Trust Service Provider (TSP), digital signing and verification tools stand as pillars of integrity and authenticity in the digital realm. Empowering users to affix legally binding electronic signatures to documents, transactions, and communications, these tools ensure the irrefutable identification and validation of signatories. Seamlessly integrated into TSP workflows, digital signing and verification tools uphold the highest standards of cryptographic security, enabling the verification of signatures and the integrity of digitally signed data with utmost precision and reliability. As guardians of trust in the digital landscape, TSPs leverage these tools to instil confidence in electronic interactions, fostering a secure and transparent environment for digital transactions and communications.

Check List

1. **Advanced Signature Formats:** Does the signing software support advanced signature formats such as:
    - XAdES
    - PAdES
    - ASic
    - CAdES
2. **Multi-Signature Support:** Can the signing software handle multi-signature scenarios where multiple signatories contribute to a single digitally signed document or transaction?
3. **Cross-Certification:** Is the verification tool capable of validating cross-certificates and certificate chains to establish trust relationships between different PKI domains and hierarchies?

Interoperability and Integration

Interoperability and Integration are pivotal aspects addressed within the checklist, encompassing the seamless interaction and compatibility of Trust Service Provider (TSP) systems with diverse environments. This section delves into the capacity of TSP software to effectively interface with third-party applications, middleware, and identity management systems through standard APIs (e.g., RESTful APIs, SOAP APIs). By ensuring smooth interoperability, TSPs can streamline processes, enhance efficiency, and facilitate the exchange of trusted information across disparate platforms. Moreover, the checklist scrutinizes the integration capabilities of TSP software with LDAP directories, Active Directory, or other directory services for seamless user authentication, attribute lookup, and certificate enrollment. Robust interoperability and integration mechanisms empower TSPs to seamlessly integrate trust services into existing infrastructures, fostering a cohesive and interconnected digital ecosystem.

Check List

1. **Standard APIs:** Does the PKI software offer standard APIs (e.g., RESTful APIs, SOAP APIs) for seamless integration with third-party applications, middleware, and identity management systems?

2. **Directory Integration:** Can the PKI software integrate with LDAP directories, Active Directory, or other directory services for user authentication, attribute lookup, and certificate enrollment?

3. **Federated Identity Support:** Does the PKI software support federated identity protocols such as SAML, OpenID Connect, or OAuth for single sign-on (SSO) and cross-domain authentication scenarios?

Scalability and Performance

Scalability and performance form the bedrock of operations for a Trust Service Provider (TSP), ensuring seamless handling of increasing workloads and maintaining optimal service levels for Production, Staging and DR. By harnessing scalable infrastructure and finely-tuned performance mechanisms, TSPs accommodate growing demands without compromising on efficiency or reliability.

Check List

1. **Horizontal Scalability:** Is the PKI software designed for horizontal scalability, allowing organizations to add additional servers or nodes to the PKI infrastructure to handle increased load and user demand?

2. **Performance Tuning:** Does the software provide performance tuning options and configuration settings to optimize resource utilization, throughput, and response times for critical PKI operations?

3. **Capacity Planning:** Can the PKI software generate performance metrics and capacity planning reports to help organizations forecast future demand and scale their infrastructure accordingly?

Security and Compliance

Security and compliance serve as non-negotiable cornerstones within the operations of a Trust Service Provider (TSP), safeguarding sensitive data and ensuring adherence to regulatory requirements. Through rigorous security protocols, TSPs mitigate risks and protect against unauthorized access, data breaches, and cyber threats. By adhering to industry regulations and standards, TSPs demonstrate commitment to data privacy, integrity, and trust, fostering confidence among users and stakeholders. With a proactive approach to security and compliance, TSPs uphold the highest standards of reliability and integrity in the digital realm.

Check List

1. **ISMS Certification:** Does the PKI vendor hold active ISO 27001 certification?

2. **Security Compliance:** Is the PKI software built by a company which knows industry standards like: ETSI, FIPS 140-2, Common Criteria?

3. **Key Management:** Does the software offer robust key management capabilities, including key generation, storage, backup, and rotation, to protect sensitive cryptographic keys and materials?

4. **Regulatory Compliance:** Can the PKI software generate demonstrate adherence to regulatory requirements, industry standards, and best practices such as:

    - **eIDAS Regulation (EU) No 910/2014:** The eIDAS Regulation establishes a legal framework for electronic identification, authentication, and trust services within the European Union (EU).
    - **ETSI EN 319 421:** This Technical requirements and procedures for the creation, verification, and archival of electronic timestamps.
    - **RFC 3161:** RFC 3161 is an Internet Engineering Task Force (IETF) standard that defines the Time-Stamp Protocol (TSP) for requesting and receiving trusted timestamps over the internet.
    - **ETSI EN 319 412-1:** Electronic Signatures and Infrastructures (ESI); Certificate Profiles
    - **RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP)**

- **ETSI EN 319 122-1:** Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
- **ETSI EN 319 132-1:** Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
- **ETSI EN 319 142-1:** Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- **ETSI EN 319 162-2:** Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers

To see the full list of EU standards checkout Electronic Signatures and Trust Infrastructures Activities.

Support and Maintenance

Support and maintenance constitute essential pillars of service delivery for a Trust Service Provider (TSP), ensuring continuous operation and user satisfaction. With dedicated support teams and proactive maintenance schedules, TSPs promptly address user inquiries, troubleshoot issues, and deliver timely updates and patches. By offering round-the-clock assistance and comprehensive documentation, TSPs empower users to maximize the value of trust services while minimizing disruptions and downtime. Through ongoing support and maintenance efforts, TSPs uphold their commitment to service excellence and user-centricity, fostering long-term partnerships built on trust and reliability.

Check List

1. **24/7 Support:** Can the PKI vendor provide round-the-clock technical support and assistance for critical issues, outages, or emergencies?

2. **Knowledge Base and Documentation:** To help users troubleshoot common issues and perform routine maintenance tasks does the vendor provide:
    - Installation & Admin Guides
    - Product Training

3. **Software Updates and Patch Management:** Does the vendor offer regular software updates, security patches, and bug fixes to address vulnerabilities, performance improvements, and feature enhancements?

Cost and Licensing

In the process of procuring PKI software, assessing the cost and licensing model is paramount for Trust Service Providers (TSPs). Beyond the initial purchase price, TSPs must consider the total cost of ownership (TCO), encompassing deployment, maintenance, and support expenses. Evaluating different licensing options, such as perpetual licenses or subscription-based models, allows TSPs to align with budgetary constraints and operational needs. Scalability pricing is also a critical factor, ensuring that licensing costs evolve in tandem with the growth of the TSP's infrastructure and user base. By carefully examining cost and licensing considerations, TSPs can make strategic decisions that optimize value and support the long-term success of their trust service offerings.

Check List

1. **Total Cost of Ownership (TCO):** Have all costs associated with purchasing, deploying, configuring, maintaining, and supporting the PKI software been factored into the TCO analysis?

2. **Licensing Flexibility:** Are there flexible licensing options available, such as perpetual licenses, subscription-based models, or usage-based pricing, to accommodate different budgetary constraints and deployment scenarios?

3. **Scalability Pricing:** Does the pricing model align with the scalability requirements of the organization, allowing for incremental growth and expansion of the PKI infrastructure without significant cost overheads?

What should be the Vendor Assessment and Selection Process?

The Vendor Assessment and Selection Process for choosing the right PKI vendor for EU Trust Service Providers (TSPs) is a multi-step approach aimed at evaluating vendors based on various criteria and selecting the most suitable partner. Here's a suggested process. A TSP can customize this as per their own needs:

1. Define Requirement
2. Market Research
3. RFI
4. RFP
5. Vendor Demos
6. Technical Evaluation
7. Security Assessment
8. Vendor Reputation
9. Contract Negotiation
10. Support

1 – Define Requirements: Begin by defining the specific requirements and objectives of your TSP. Consider factors such as technical capabilities, security requirements, compliance needs, scalability, budget constraints, and timeline for implementation.

2 - Market Research: Conduct thorough market research to identify potential PKI vendors that meet your requirements. Utilize online resources, industry reports, analyst evaluations, and peer recommendations to create a list of candidate vendors.

3 – Request for Information (RFI): Send out RFIs to the shortlisted vendors to gather detailed information about their PKI solutions, including technical specifications, security features, pricing models, customer references, and implementation timelines. Use the responses to assess vendors' alignment with your requirements and narrow down the list further.

4 – Request for Proposal (RFP): Based on the RFI responses, select a subset of vendors and invite them to submit formal proposals outlining their PKI solutions in greater detail. The RFP should include specific questions about architecture, deployment options, customization capabilities, support services, and pricing structures. Evaluate the proposals against your criteria and identify vendors that best meet your needs.

5 – Vendor Demos and Presentations: Schedule demos or presentations with the shortlisted vendors to see their PKI solutions in action. Request live demonstrations of key features, user interfaces, and administrative functionalities. Use this opportunity to ask questions, clarify doubts, and assess the vendor's responsiveness and expertise.

6 – Technical Evaluation: Conduct a technical evaluation of the PKI solutions offered by the remaining vendors. Assess factors such as interoperability, integration capabilities, scalability, performance, and compliance with industry standards and regulations. Consider conducting a proof of concept (POC) or pilot project to validate the vendor's claims in a real-world environment.

7 – Security and Compliance Assessment: Evaluate the security measures implemented by each vendor to protect sensitive data, secure communication channels, and ensure compliance with relevant regulations (e.g., eIDAS, GDPR). Review the vendor's certifications, audit reports, and security practices to assess their commitment to data protection and risk mitigation.

8 – Vendor Reputation and References: Research the reputation and track record of each vendor in the industry. Seek feedback from existing customers or references provided by the vendor to gain insights into their experience with the PKI solution, vendor support, and overall satisfaction.

9 – Contract Negotiation and Final Selection: Once you've thoroughly evaluated each vendor, engage in contract negotiations with the preferred vendor. Discuss pricing, licensing terms, service level agreements (SLAs), implementation timelines, and any customization or additional requirements. After reaching mutually acceptable terms, finalize the contract and select the vendor as your PKI solution provider.

10 – Post-Selection Support: After selecting a PKI vendor, establish clear communication channels and expectations for ongoing support, maintenance, and collaboration. Work closely with the vendor to ensure a smooth implementation process, comprehensive training for staff members, and timely resolution of any issues or concerns that may arise.

By following this structured Vendor Assessment and Selection Process, EU Trust Service Providers can make informed decisions and choose a PKI vendor that aligns with their requirements, budget, and long-term strategic objectives.

Rating

Here's a rating system you can use for evaluating each checklist point. Rating system ranges from 1 to 5, where 1 represents poor performance and 5 represents excellent performance.

Certificate Authority (CA) Functionality	
Certificate Templates	
Certificate Revocation Management	
Hierarchical CA Support	
Certificate Types	
Registration Authority (RA) Features	
Authentication Methods	
Audit Trails	
Self-Service Enrolment	
Vetting Workflow	
Certificate Issuance	
OCSP Support	
High Availability	
Load Balancing	
Performance Monitoring	
Timestamping Functionality	
Client Authentication	
NTP Support	
Auditability	
High Availability	
Client Management & Reporting	
Digital Signing and Verification Tools	
Advanced Signature Formats	

Multi-Signature Support	
Cross-Certification	
Interoperability and Integration	
Standard APIs	
Directory Integration	
Federated Identity Support	
Scalability and Performance	
Horizontal Scalability	
Performance Tuning	
Capacity Planning	
Security and Compliance	
ISMS Certification	
Security Compliance	
Key Management	
Regulatory Compliance	
Support and Maintenance	
24/7 Support	
Knowledge Base and Documentation	
Software Updates and Patch Management	
Cost and Licensing	
Total Cost of Ownership (TCO)	
Licensing Flexibility	
Scalability Pricing	

How to use the Rating System

1. Rate each criterion on a scale from 1 (Poor) to 5 (Excellent).
2. Summarize the scores to get an overall picture of how well each PKI vendor meets your needs.
3. Compare vendors based on their total scores and individual criterion ratings to make an informed decision.

This structured rating system will help you evaluate and compare PKI vendors effectively, ensuring you choose the best fit for your Trust Service Provider requirements.

Summary

As you embark on the journey of selecting the perfect PKI software for your Trust Service Provider organization, remember that the ultimate goal is to build trust, security, and reliability in the digital ecosystem. While our checklist provides a comprehensive framework for evaluating PKI solutions, we understand that the decision-making process can be complex.

That's why we invite you to explore **Khatim Trust Suite**, our flagship PKI software solution designed specifically for Trust Service Providers like you. With Khatim Trust Suite, you'll have access to a suite of robust, scalable, and interoperable PKI tools that empower you to deliver a wide range of trust services to your clients with confidence.

Khatim Trust Suite comprises of:

- Khatim PKI Server
- Khatim RA Server
- Khatim OCSP Server
- Khatim Timestamp Server
- Khatim Sign & Verification Server
- KhatimDoc

From its advanced CA functionality and seamless integration capabilities to its stringent security and compliance features, Khatim Trust Suite is

engineered to meet the diverse needs and challenges of modern Trust Service Provider. Whether you're issuing digital certificates, managing certificate lifecycle, or providing timestamping and signing services, Khatim Trust Suite has you covered.

Trust in Khatim Trust Suite. Trust in the future!