TicketBAI 1.0 Signature Policy

Version date: 19/12/2019

CONTENTS

1 INTRODUCTION

1.1 Purpose of the document

This TicketBAI Signature Policy (hereinafter referred to as the Policy) set out the criteria established by the Provincial Governments of Araba-Álava, Bizkaia and Gipuzkoa and by the Basque Government with regard to the electronic signing of TicketBAI files.

The definition, structure and technical requirements of the TicketBAI file are set out in the document entitled "Functional and Technical Specifications of the TicketBAI system". In short: a TicketBAI file contains the data of a single invoice issued in XML format. This includes data specific to that invoice and other control data (invoice chaining, invoice issuing device, the developer, etc.).

This signature policy must be available in readable format, so that it can be used in specific contexts to ensure compliance with the requirements on creating and validating e-signatures.

1.2 References

In drafting this policy, the following technical specifications have been used:

- ETSI EN 319 132-1 V1.1.1 (2016-04) XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

- ETSI EN 319 132-2 V1.1.1 (2016-04) XAdES digital signatures; Part 2: Extended XAdES signatures.

- EN 319 102-1 V1.1.1 (2016-05) Procedures for Creation and Validation of AdES Digital Signatures.

- ETSI TS 119 312 V1.3.1 (2019-02) Cryptographic Suites.

The basic legislation applying to this policy is as follows:

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

- Digital signature Act (Ley 59/2003), of 19 December 2003.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Personal Data Protection and Digital Rights Assurance Act (*Ley Orgánica* 3/2018) of 5 December 2018.

- Public Sector Procurement Act (Act 40/2015) of 1 October 2015.

- Information Society Promotion Act (Act 56/ 2007)

- Royal Decree 3/2010, of 8 January 2010, governing the National Security Framework for eGovernment

- Royal Decree 4/2010, of 8 January 2010, governing the National Interoperability Framework in the area of eGovernment.

2 SCOPE OF THE TICKETBAI FILE SIGNATURE POLICY

This policy sets out the general conditions for signing XML files to TicketBAI specifications.

It will be valid from the date of its publication until such time as an update is published.

The signature policy will be identified with a unique identifier, http://ticketbai.eus/politicafirma. This identification must obligatorily be included in the electronic signature, using the corresponding field to identify the framework policy and version, with the general and specific conditions of application for its validation.

2.1 Agents involved

The agents involved in the process of creating and validating electronic signatures are:

- Signatory: natural or legal person or entity without legal personality that possesses a device for creating a signature and which signs a TicketBAI file.
- Verifier: entity (natural or legal person), which validates or verifies an electronic signature based on the conditions required by a specific signature policy.
- Trust service provider: natural or legal person issuing electronic certificates or providing other services relating to the electronic signature.
- Policy Issuer: organisation responsible for creating and managing this document, by which the signatory and verifier must be governed in the processes of creating and validating electronic signatures.

2.2 Formats accepted for the signature

XAdES (XML AdvancedElectronicSignatures) format, as per technical specification ETSI EN 319 132-1 V1.1.1. For later versions of the standard, changes in the syntax will be analysed and any adaptation of the profile to the new version of standard will be approved by means of an addendum to the policy.

Throughout this document the prefixes ds: and xades: will be used to refer to elements defined in the XMLDSig and XAdES standards, respectively.

Of the different **XAdES** profiles (forms), at least the basic form with added information on the signature policy (i.e. **XAdES-EPES**) must be generated.

2.3 Creating the electronic signature

It is advisable to implement the creation of the electronic signature using cryptographic libraries or existing products.

The signature need not include TimeStamping provided by TSA services at the time of signature.

2.4 Verification of the electronic signature

The verifier can use any standardised method to verify the signature created in accordance with this Policy. The minimum conditions that must be fulfilled to validate the signature shall be as follows:

1. Guarantee of signature integrity validity.

2. Validity of certificates at time of signing.

3. Signing certificate issued under a specific Certification Practice Statement, available in a public repository.

4. The issuer of the signing certificate must be on the list of qualified trust service providers (QTSPs). This list can be found at https://webgate.ec.europa.eu/tl-browser/#/.

2.5 Management of the Signature policy

The provincial governments of Araba/Alava, Bizkaia and Gipuzkoa, and the Basque Government are responsible for maintenance, update, publication and dissemination of this document.

Updated versions of this policy will be published at http://ticketbai.eus/politicafirma.

3 ELECTRONIC SIGNATURE VALIDATION POLICY

This section sets out the conditions that must be taken into consideration by the signatory, in the process of creating an electronic signature, and by the verifier, in the process of validating the signature.

3.1 Validity period

This Policy is valid from its publication until such time as a new updated version is published. A transition period may be provided, in which the two versions are equally valid, to allow the platforms of the different agents involved in the TicketBAI project to be adapted to the specifications of the new version. This transitory period must be indicated in the new version, after which time only the updated version will be valid.

3.2 Common rules

The common rules for the agents involved in the electronic signature (i.e. the signatory and verifier) constitute a mandatory field which must appear in any Signature Policy. These rules establish the different responsibilities of the person or entity creating the signature and the person or entity verifying the signature, establishing the minimum requirements that must be presented. Requirements for the signatory must be signed and requirements for the verifier unsigned.

3.3 Signatory rules

The signatory shall be responsible for ensuring that the file to be signed does not contain dynamic content that might alter the result of the signature over time. If the file to be signed has not been created by the signatory, the signatory must ensure that there is no dynamic content within the file (e.g. macros).

XAdES format: only **XAdESenveloped** signatures will be accepted. XAdESenveloping or XAdESdetached will not be permitted.

The signatory must provide, at minimum, the information contained in the following mandatory tags in the SignedProperties field (which contains a series of properties signed jointly on generation of the XMLDsig signature):

- SigningTime: specifies the time at which the signatory performs the signing process.
- SigningCertificatev2: contains references to the certificates and security algorithms used in each certificate. This element must be signed to prevent against possible substitution of the certificate.
- SignaturePolicyIdentifier: identifies the signature policy on which the process of generating the electronic signature is based, and must include the following contents, in the elements into which it is subdivided:
    - An explicit reference to this signature policy document, in the xades:SigPolicyId element. For this purpose, it must show the OID of the specific version of the signature policy or the URL where it can be found.

- ○ The digital fingerprint of the corresponding signature policy document and the algorithm used, in the <xades:SigPolicyHash> element. This allows the verifier, by calculating this value, to check that the signature has been generated in accordance with the same signature policy as the policy that will be used for validation.

The remaining tags that can be added in the SignedProperties field will be considered optional:

- SignatureProductionPlacev2: defines the geographical location where the document has been signed.
- SignerRolev2: defines the person's role in the electronic signature. If used, it must contain one of the following values in the ClaimedRoles field:
  - ○ “supplier”, “issuer” or “egilea”: when the document is signed by the issuer.
  - ○ “customer”, “receptor” or “hartzailea”: when the document is signed by the recipient.
  - ○ “thirdparty”, “tercero” or “hirugarrena”: when the document is signed by a person or entity other than the issuer or recipient.
- CommitmentTypeIndication: defines the signatory's action with regard to the signed document (approves, reports, receives, certifies, etc.).
- AllDataObjectsTimeStamp: contains a time stamp, calculated before the signature is generated, on all the ds:Reference elements.
- IndividualDataObjectsTimeStamp: contains a time stamp, calculated before the signature is generated, on some of the ds:Reference elements.

  The CounterSignature tag can be included in the UnsignedProperties field and will be considered optional. The following signatures, either in series or in parallel, will be added as indicated by the XAdES standard, in accordance with document EN 319 102-1.

3.4 Verifier rules

The basic advanced electronic signature format does not include any validation information apart from the signing certificate. The verifier can use the following attributes to check compliance with the requirements of the signature policy under which the signature has been generated:

- Signing Time: only used in verifying electronic signatures to check the status of the certificates on the given date, since time references can only be assured by means of a time stamp (especially in the case of signatures on client devices).

- SigningCertificatev2: used to check and verify the certificate status (and, where applicable, the certification chain) on the date on which the signature is generated, where the certificate has not expired and it is possible to access the verification data (CRL, OCSP) or where the PSC offers a historical certificate status validation service.

- SignaturePolicyIdentifier: it is necessary to check that the signature policy used to generate the signature is the same as that which must be used for a given service.

There is a waiting time —known as a grace or caution period— to check the revocation status of a certificate. The verifier can wait for this time to validate the signature or do it at that time and revalidate it later. The reason is that there may be a short delay between the time the signatory initiates revocation of a certificate and the time the information on the revocation status of the certificate is distributed to the corresponding information points. It is recommended that this period, i.e. the time that elapses from signing, should be at least equal to the maximum time permitted for complete CRL refresh or the maximum certificate status update time in the OCSP service. These times may vary depending on the Certification Service Provider.

3.5 Algorithm usage rules

Any of the RSA-based algorithms accepted in ETSI TS 119 312 V1.3.1. may be used. The following is required at minimum:

- The key size must be strictly greater than 1024.

- SHA256 or higher versions.

4 TICKETBAI ARCHITECTURE REQUIREMENTS

4.1 Certificates accepted

The TicketBAI solution requires use of one of the following certificates:

Device certificate: provides a unique identity for each device. It is installed and associated with the device from which the invoices are issued.

Certificate of natural person or entity representative: allows the identity of the natural or legal person, respectively, to be accredited.

Company stamp: this is a technical certificate which may be used in automated mode by an application, or by a group of people from the same department or work team. This certificate can be compared to the common use of rubber stamps in a company's real-world operations.

Self-Employed Worker's Certificate: non-qualified certificate, issued by natural persons who declare business activities as self-employed workers. Its function is to guarantee the VAT Registration Number of the person applying for the certificate.

4.2 Signature restrictions depending on the architecture

4.2.1 Client-based signature architectures

These are solutions in which the software creating the signature is located on the device from which the invoicing application is accessed, e.g. a desktop application with no Internet access:.

Where another device is accessed remotely to create the signature, the solution is referred to as “server-based signature architecture”.

There are no restrictions on certificates for this type of architecture. Signatures can be created with the following: **device certificate, natural person certificate, entity representative certificate, company stamp or self-employed worker's certificate**.

4.2.2 Server-based signature architectures

These are solutions in which the software creating the signature is located on a device other than that from which the invoicing application is accessed. Thus, the client device remotely accesses another device to make the signature.

Complementarily, solutions in which invoices are issued in automated processes (batches) are considered to be “server-based signature architectures”.

Signatures can be created with the following: **natural person certificate, entity representative certificate, company stamp or self-employed worker's certificate**.

In these cases, signing with a device certificate is not permitted.

4.2.3 Architectures offering the possibility of client and server-based signing

Distributed architectures can choose between making the signature on the client or on the server, provided the restrictions applying to each one are respected.

For example, in a web-based application:

- A client-based signature would be made on the device with the browser installed from which the application is accessed. In this case, the restrictions on client-based signature architectures apply.

- A server-based signature would be made on the remote server accessed by the browser. In this case, the restrictions on server-based signature architectures apply.

The same architecture cannot make signatures on the client and server simultaneously. Only one of the available architectures must be chosen.