# Takto má vypadat výchozí šablona XML souboru

<?xml version="1.0" encoding="UTF-8"?>

<AutorizovanaDigitalizaceDokumentu

xmlns="http://www.example.org/autorizovana-digitalizace"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.example.org/autorizovana-digitalizace autorizovana-digitalizace.xsd"

ID="AD-2025-000123">

<!-- === 1) Metadata (sem vložíte svůj blok DigitalizacniDolozka) === -->

<Metadata>

<!-- sem přijde:

<DigitalizacniDolozka>

<ID>…</ID>

<DatumDigitalizace>…</DatumDigitalizace>

<Operator>…</Operator>

<PocetStran>…</PocetStran>

<Format>…</Format>

<DocumentHash Algorithm="SHA-256">…</DocumentHash>

</DigitalizacniDolozka>

-->

</Metadata>

<!-- === 2) Obsah dokumentu (odkazy na skeny / embedded PDF nebo OCR) === -->

<Content>

<!-- příklad odkazu na PDF -->

<!-- <DocumentReference URI="documents/page1.pdf"/> -->

<!-- nebo embedded Base64 -->

<!-- <DocumentData encoding="base64">JVBERi0xLj…</DocumentData> -->

</Content>

<!-- === 3) Šablona pro podpis (XAdES-BES) – vložíte sem před </AutorizovanaDigitalizaceDokumentu> === -->

<!--

<ds:Signature Id="SIG-AD-2025-000123">

<ds:SignedInfo>… reference na "" a #SignedProps …</ds:SignedInfo>

<ds:SignatureValue/>

<ds:KeyInfo>…</ds:KeyInfo>

<xades:QualifyingProperties Target="#SIG-AD-2025-000123">

<xades:SignedProperties Id="SignedProps">…</xades:SignedProperties>

</xades:QualifyingProperties>

</ds:Signature>

-->

</AutorizovanaDigitalizaceDokumentu>

# 1 - Naskenovat v 300DPI do PDF/A (nekomprimovaný formát)

# 2 - Další krok je vytvořit tzv. digitalizační doložku – nejdřív ale získat otisk (hash) našeho PDF.

**sha256sum /cesta/k/vasemu.pdf**

– výstupem je SHA-256 hash, který pak vložíte do XML metadat (element <DocumentHash>).

# 3- V dalším kroku vytvoříte XML metadatový blok („doložku autorizované digitalizace“), ve kterém:

- uvedete identifikátor digitalizace (např. AD-2025-000123),

- čas a datum digitalizace,

- identifikaci operátora či pracoviště,

- počet stran (z PDF),

- formát (PDF/A nebo PDF),

- a právě ten SHA-256 hash, který jste získali příkazem sha256sum.

Například:

<DigitalizacniDolozka>

<ID>AD-2025-000123</ID>

<DatumDigitalizace>2025-06-18T10:42:00+02:00</DatumDigitalizace>

<Operator>Jan Novák, Městský úřad Praha</Operator>

<PocetStran>3</PocetStran>

<Format>PDF/A-2a</Format>

<DocumentHash Algorithm="SHA-256">

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

</DocumentHash>

</DigitalizacniDolozka>

Tento XML blok pak bude součástí dokumentu, který následně podepíšete.

# 4 - Dalším krokem je naplnit sekci <Content> odkazy na vaše naskenované PDF (nebo jednotlivé stránky) a případně OCR textem, aby bylo jasné, co všechno se bude podepisovat.

Rozhodněte se, zda budete obsah ukládat externě nebo embedovat

**Externě:** budete mít jeden (nebo víc) PDF souborů ve složce documents/

**Embedovat:** celý PDF (nebo stránky) vložíte jako Base64 do XML

Upravte blok <Content> ve vaší šabloně takto:

<Content>

<!-- 1) Všechny PDF soubory -->

<DocumentReference URI="documents/foo.pdf"/>

<DocumentReference URI="documents/bar.pdf"/>

<!-- 2) OCR text pro jednotlivé stránky,

přičemž atribut file ukazuje, z kterého PDF stránka pochází -->

<Page file="documents/foo.pdf" number="1">

<Text>…OCR foo.pdf, strana 1…</Text>

</Page>

<Page file="documents/foo.pdf" number="2">

<Text>…OCR foo.pdf, strana 2…</Text>

</Page>

<Page file="documents/foo.pdf" number="3">

<Text>…OCR foo.pdf, strana 3…</Text>

</Page>

<Page file="documents/bar.pdf" number="1">

<Text>…OCR bar.pdf, strana 1…</Text>

</Page>

<Page file="documents/bar.pdf" number="2">

<Text>…OCR bar.pdf, strana 2…</Text>

</Page>

<Page file="documents/bar.pdf" number="3">

<Text>…OCR bar.pdf, strana 3…</Text>

</Page>

</Content>

Nebo pokud chcete **embedovat:**

<Content>

<DocumentData encoding="base64">

JVBERi0xLjQKJ…(celé vaše PDF v Base64)…==

</DocumentData>

<Text>… OCR výstup …</Text>

</Content>

Poznámka k referencím

Pokud použijete DocumentReference, pak se element <ds:Reference URI="documents/vase-dokument.pdf"> ve vaší podpisové šabloně postará o výpočet a ověření hashe toho externího PDF.

Pokud embedujete Base64, referencujte prvek <DocumentData> jeho vlastní ID (např. URI="#Data-1").

Po vložení těchto elementů už máte v XML kompletní datový obsah, na který budete následně aplikovat podpis (šablonu <ds:Signature>).

# 5 - Vložení šablony podpisu (XAdES-BES)

Do XML, těsně před </AutorizovanaDigitalizaceDokumentu>, přidejte prázdnou XAdES-BES šablonu <ds:Signature>, která obsahuje:

* Reference na celý dokument (URI="", enveloped transform)
* Reference na SignedProperties (pro kvalifikované vlastnosti)
* Prázdné uzly pro DigestValue, SignatureValue a certifikát
* Blok <xades:QualifyingProperties> s SigningTime a SigningCertificate

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"

Id="SIG-AD-2025-000123">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<!-- 1) podepisujeme celý XML dokument -->

<ds:Reference URI="">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue/>

</ds:Reference>

<!-- 2) podepisujeme i SignedProperties -->

<ds:Reference URI="#SignedProps"

Type="http://uri.etsi.org/01903#SignedProperties">

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue/>

</ds:Reference>

</ds:SignedInfo>

<!-- 3) míst pro podpisovou hodnotu -->

<ds:SignatureValue/>

<!-- 4) KeyInfo – sem doplní xmlsec váš certifikát -->

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate/>

</ds:X509Data>

</ds:KeyInfo>

<!-- 5) XAdES vlastnosti -->

<xades:QualifyingProperties Target="#SIG-AD-2025-000123">

<xades:SignedProperties Id="SignedProps">

<xades:SignedSignatureProperties>

<xades:SigningTime/>

<xades:SigningCertificate>

<xades:Cert>

<xades:CertDigest>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue/>

</xades:CertDigest>

<xades:IssuerSerial>

<ds:X509IssuerName/>

<ds:X509SerialNumber/>

</xades:IssuerSerial>

</xades:Cert>

</xades:SigningCertificate>

</xades:SignedSignatureProperties>

</xades:SignedProperties>

</xades:QualifyingProperties>

</ds:Signature>

**Poznámky:**

* Id="SIG-AD-2025-000123" musí odpovídat atributu ID="AD-2025-000123" ve vašem root elementu.
* Prázdné elementy (<ds:DigestValue/>, <ds:SignatureValue/>, <ds:X509Certificate/>, <xades:SigningTime/> apod.) xmlsec1 při podpisu vyplní.
* Tento blok společně s vloženými odkazy na <DocumentReference> a <DigitalizacniDolozka> v XML zajistí XAdES-BES podpis.

# 6 - Teď, když máš v unsigned-xades.xml vloženou XAdES-BES šablonu, následuje skutečné podepsání:

Ulož si upravený XML pod jménem třeba **unsigned-xades.xml**.

Spusť xmlsec1 (jako root nebo uživatel s přístupem k privátnímu klíči):

xmlsec1 sign \

--privkey-pem /home/webdata/www/brambor.net/developlitex.brambor.net/certifikaty/osobniNemec/priv.pem,/home/webdata/www/brambor.net/developlitex.brambor.net/certifikaty/osobniNemec/cert.pem \

--id-attr:ID AutorizovanaDigitalizaceDokumentu \

--node-xpath "/\*[local-name()='AutorizovanaDigitalizaceDokumentu']" \

--output signed.xml \

unsigned-xades.xml

Co se stane:

* xmlsec1 najde <ds:Signature> šablonu, spočítá všechny DigestValue,
* doplní <xades:SigningTime> a údaje o certifikátu,
* vypočte a vloží <ds:SignatureValue>,
* výsledek uloží do signed.xml.

# 7 - Ověř podpis (volitelné, ale doporučené):

xmlsec1 verify \

--pubkey-cert-pem /home/webdata/www/brambor.net/developlitex.brambor.net/certifikaty/osobniNemec/cert.pem \

signed.xml

Po tomto kroku máš hotové XAdES-BES podepsané XML. Dál přidat kvalifikované časové razítko (XAdES-T)

# 8 - Dalším krokem je vygenerovat a vložit XAdES-T – tedy kvalifikované časové razítko – do elementu <UnsignedProperties>. Postup:

Vygenerujte RFC-3161 timestamp request z hodnoty <ds:SignatureValue>:

# 1. Extrahujte SignatureValue (base64) a dekódujte do binárky

xmlstarlet sel -N ds="http://www.w3.org/2000/09/xmldsig#" \

-t -v "//ds:SignatureValue" unsigned-xades.xml \

| base64 -d > sig.bin

# 2. Pošlete na TSA (PostSignum Q-TSA)

curl -s \

-H "Content-Type: application/timestamp-query" \

--data-binary @sig.bin \

http://qtsa.postsignum.cz/TSS/TSS \

> ts.tsr

Převrťte odpověď na base64:

base64 ts.tsr > ts.b64

Vložte do XML blok <UnsignedProperties> těsně za <xades:QualifyingProperties>:

<xades:UnsignedProperties>

<xades:UnsignedSignatureProperties>

<xades:SignatureTimeStamp Id="TS-AD-2025-000123">

<ds:CanonicalizationMethod

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<xades:EncapsulatedTimeStamp>

<!-- sem zkopírujte obsah ts.b64 -->

MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglg...

</xades:EncapsulatedTimeStamp>

</xades:SignatureTimeStamp>

</xades:UnsignedSignatureProperties>

</xades:UnsignedProperties>

Teď máte v <ds:Signature> kromě SignedProperties i UnsignedProperties s kvalifikovaným časovým razítkem (XAdES-T).

# 9 - Vytvoření adresářové struktury

Ve vašem pracovním adresáři (např. balicek/) vytvořte tyto složky:

balicek/

├─ META-INF/

│ ├─ manifest.xml

│ └─ signatures.xml

├─ documents/

│ └─ vaše-pdf-soubory…

└─ metadata.xml

**Přesun PDF do složky documents/**

Teď do složky documents/ zkopíruj (nebo přesun) všechny své naskenované PDF

**Vytvoření metadata.xml**

Do kořenového adresáře (vedle složek META-INF/ a documents/) vytvoř soubor metadata.xml, je to přesně ten XML podepsaný soubor který jsme na začátku generovali.

**Vytvoření manifestu (manifest.xml) v META-INF/**

V souboru META-INF/manifest.xml vyjmenuješ všechny soubory, které chceš dát do ADOC balíku:

Každý PDF soubor v documents/

Soubor metadata.xml:

Pro každý uvedeš element <Reference> s URI, DigestMethod a vypočteným DigestValue (SHA-256).

Příklad META-INF/manifest.xml

<?xml version="1.0" encoding="UTF-8"?>

<Manifest xmlns="http://www.example.org/adoc">

<!-- 1) všechny dokumenty -->

<Reference URI="documents/foo.pdf">

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>…hash foo.pdf…</DigestValue>

</Reference>

<Reference URI="documents/bar.pdf">

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>…hash bar.pdf…</DigestValue>

</Reference>

<!-- 2) podepsané metadata -->

<Reference URI="metadata.xml">

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>…hash metadata.xml…</DigestValue>

</Reference>

</Manifest>

Pro rychlý výpočet hashů můžeš použít například v shellu:

sha256sum documents/foo.pdf | awk '{print $1}'

sha256sum metadata.xml | awk '{print $1}'

**Podepsání manifestu (XAdES-LTA)**

Nyní podepíšeme META-INF/manifest.xml a vytvoříme META-INF/**signatures.xml**, který bude obsahovat XAdES podpis manifestu. Tento podpis je detached (není „enveloped“ uvnitř manifestu), a pro dlouhodobou archivaci (LTA) se doporučuje připojit i časové razítko – ale pro základní XAdES-T postačí:

Vložte do manifestu šablonu <ds:Signature>

Podobně jako jste to dělal v metadata.xml, ale s Type=http://www.w3.org/2000/09/xmldsig#Manifest a referencí právě na manifest stesso:

<!-- na konec META-INF/manifest.xml přidejte: -->

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

Id="SIG-MANIFEST-AD-2025-000123">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI=""

Type="http://www.w3.org/2000/09/xmldsig#Manifest">

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue/>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue/>

<ds:KeyInfo>

<ds:X509Data><ds:X509Certificate/></ds:X509Data>

</ds:KeyInfo>

</ds:Signature>

Podepište manifest pomocí xmlsec1

Spustíte příkaz (jako předtím):

xmlsec1 sign \

--privkey-pem /home/webdata/www/brambor.net/developlitex.brambor.net/certifikaty/osobniNemec/priv.pem,/home/webdata/www.brambor.net/developlitex.brambor.net/certifikaty/osobniNemec/cert.pem \

--id-attr:ID Manifest \

--output META-INF/signatures.xml \

META-INF/manifest.xml

* --id-attr:ID Manifest říká, že atribut Id na <Manifest> je typu ID.
* --output META-INF/signatures.xml uloží podepsaný blok do nového souboru.

# Pro přidání kvalifikovaného časového razítka (XAdES-T) k podpisu manifestu (META-INF/manifest.xml → META-INF/signatures.xml) postupujte takto:

**1. Extrahujte <ds:SignatureValue> ze signatures.xml**

xmlstarlet sel -N ds="http://www.w3.org/2000/09/xmldsig#" \

-t -v "//ds:SignatureValue" META-INF/signatures.xml \

| base64 -d > manifest-sig.bin

Tím máte v manifest-sig.bin čistá podepsaná data (binárně).

**2. Odešlete požadavek na RFC3161 TSA**

curl -s \

-H "Content-Type: application/timestamp-query" \

--data-binary @manifest-sig.bin \

http://qtsa.postsignum.cz/TSS/TSS \

> manifest-tsr.bin

Odpověď (TSR) je v manifest-tsr.bin.

**3. Převraťte odpověď na Base64**

base64 manifest-tsr.bin > manifest-ts.b64

V souboru manifest-ts.b64 je řetězec, který vložíte do XML.

**4. Vložte <xades:UnsignedProperties> do META-INF/signatures.xml**

Otevřete META-INF/signatures.xml a těsně za koncovku <ds:KeyInfo>…</ds:KeyInfo> (a před </ds:Signature>) doplňte:

<xades:UnsignedProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">

<xades:UnsignedSignatureProperties>

<xades:SignatureTimeStamp Id="TS-MANIFEST-AD-2025-000123">

<ds:CanonicalizationMethod

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<xades:EncapsulatedTimeStamp>

<!-- sem vložte celý obsah manifest-ts.b64 -->

MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglghkgBZQMEAgEFAD...

</xades:EncapsulatedTimeStamp>

</xades:SignatureTimeStamp>

</xades:UnsignedSignatureProperties>

</xades:UnsignedProperties>

Id timestampu (např. TS-MANIFEST-…) je libovolné, jen unikátní v rámci podpisu.

Nezapomeňte přidat namespace xmlns:xades (pokud už tam není).

Po uložení má META-INF/signatures.xml kompletní XAdES-T podpis manifestu. Nyní je celý balík připraven k archivaci či předání úřadům.

# Vytvoření konečného ADOC balíku

V kořenovém adresáři (tam, kde máš META-INF/, documents/ a metadata.xml) spusť:

zip -r vyslednyBalik.adoc META-INF documents metadata.xml

* -r rekurzivně přidá složky i soubory
* **vyslednyBalik.adoc** je výstupní ZIP-archiv (můžeš dát i příponu .zip, ale .adoc se v praxi používá)
* META-INF obsahuje manifest.xml + signatures.xml
* documents obsahuje všechny PDF soubory
* metadata.xml je tvoje podepsané autorizované XML
* Hotový vyslednyBalik.adoc je kompletní kontejner autorizované digitalizace, připravený k odevzdání úřadu.