CEF Digital
Connecting Europe

CEF eSignature pilot on ntQWACs

DIGIT
Directorate-General
for Informatics

DG Connect
Directorate-General for Communications
Networks, Content and Technology

Table of Contents

1 Introduction

2 How the ntQWAC Pilot Works

3 Demo

1

Introduction

Explanation on QWACs

QWAC as set out in the eIDAS Regulation

WAC makes it possible to authenticate a website and links it to the person it is issued to (eIDAS Art.3(38))*

QWAC is a WAC that is issued by a QTSP and meets Annex IV requirements (eIDAS Art.3(39), Art.45(1))

As long as these requirements are fulfilled, QWAC can be technically packaged with other security elements using "any method or technology"

Certificat

Général | Détails | Chemin d'ac

Informations su

Ce certificat est conçu

- Garantit l'identité d'un ordinateur distant
- Garantit votre identité auprès d'un ordinateur distant
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

* Consultez la déclaration de l'autorité de certification pour plu

Délivré à : nt-qwac.novina.solutions

Délivré par Let's Encrypt Authority X3

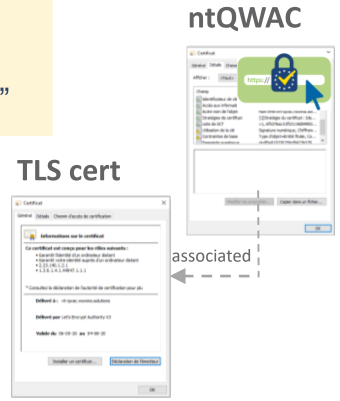
Valide du 06-05-20 **au** 04-08-20

One-certificate approach: tlsQWAC

A single certificate that is **both** a TLS certificate (e.g. DV/OV/EV) and an eIDAS QWAC

Two layers / flavours of authentication & linking of

- Website (domain name)
- Website "owner" identification information
- a TLS public/private key pair used to establish a secure connection to the website (domain name)



Certificat

Général | Détails | Chemin d'accès de certification

Informations sur le certificat

Ce certificat est conçu pour les rôles suivants :

- Garantit l'identité d'un ordinateur distant
- Garantit votre identité auprès d'un ordinateur distant
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

* Consultez la déclaration de l'autorité de certification pour plu

Délivré à : nt-qwac.novina.solutions

Délivré par Let's Encrypt Authority X3

Valide du 06-05-20 **au** 04-08-20

Certificat

Général | Détails | Chemin

Afficher : <Tout>

Champ	
Identificateur de clé	
Accès aux informati	
Autre nom de l'objet	Nom DNS=nt-qwac.novina.sol...
Stratégies de certificat	[1]Stratégie du certificat : Ide...
Liste de SCT	v1, [illegible]...
Utilisation de la clé	Signature numérique, Chiffrem...
Contraintes de base	Type d'objet=Entité finale, Co...
Empreinte numérique	[illegible]

https://
Installer un certificat...
Déclaration de l'émetteur
Modifier les propriétés...
Copier dans un fichier...
OK

Two-certificate approach: TLS cert & ntQWAC

A nonTLS attestation certifying the identity of the "operator" of a website (domain name) and making it possible to authenticate this website (domain name) as being associated to a TLS certificate (DV/OV/EV) used to establish a secure connection to the website (domain name)

ntWACs are currently already existing e.g. in the context of the provision of "verified valuations and valuation ranking" services

* "authentication" meaning the transmission of the website operator's identity

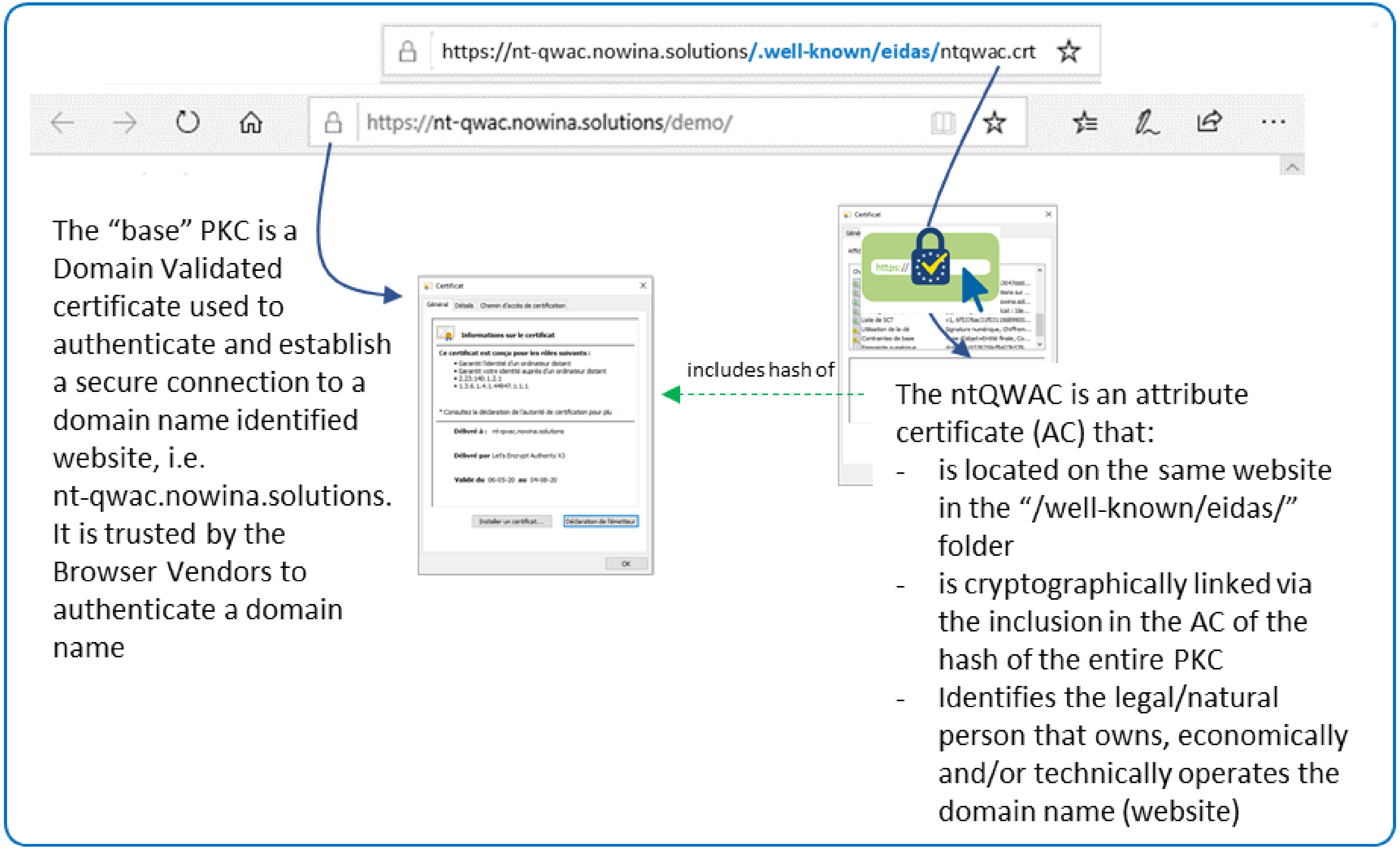
2

How the ntQWAC Pilot works

The Two Certificate approach and its attributes

Two-certificate approach

An ntQWAC **attribute certificate** associated to a base **PKC TLS certificate** (e.g. DV)


https://nt-qwac.nowina.solutions/.well-known/eidas/ntqwac.crt
https://nt-qwac.nowina.solutions/demo/
https://
Certificat
Général
Détails
Chemin d'accès de certification
Installer un certificat...
Déclaration de l'émetteur
OK
includes hash of

Informations sur le certificat

Ce certificat est conçu pour les rôles suivants :
- Garantit l'identité d'un ordinateur distant
- Garantit votre identité auprès d'un ordinateur distant
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

* Consultez la déclaration de l'autorité de certification pour plu

Délivré à : nt-qwac.nowina.solutions

Délivré par Let's Encrypt Authority X3

Valide du 06-05-20 au 04-08-20

The "base" PKC is a Domain Validated certificate used to authenticate and establish a secure connection to a domain name identified website, i.e. nt-qwac.nowina.solutions. It is trusted by the Browser Vendors to authenticate a domain name

The ntQWAC is an attribute certificate (AC) that:

- is located on the same website in the "/well-known/eidas/" folder
- is cryptographically linked via the inclusion in the AC of the hash of the entire PKC
- Identifies the legal/natural person that owns, economically and/or technically operates the domain name (website)

ntQWAC is implemented as RFC 5755 attribute certificate

RFC 5755: An Internet Attribute Certificate Profile for Authorization

The standard can be used as is, without any other change then defining new ntQWAC attributes

- Acinfo
  - Version
  - Holder (baseCertificate ID, objectDisgestInfo)
  - Issuer (DN)
  - Signature algorithm identifier
  - Serial Number
  - AC validity period (NotBefore, NotAfter)
  - Attributes (sequence of attributes)
  - IssuerUniqueID
  - Extensions
    - AKI
    - AIA (ocsp, id-ad-caIssuer)
    - CRLDP
    - QcStatement (QcCompliance, QcType 3)
    - Optional: CP, SAN, IAN, BC
- Signature Algorithm
- Signature Value

Hash of the entire base TLS certificate

9 attributes in the pilot

- Domain Name Beneficiary (Economical Operator)
- DNB Legal representative
- Domain Name Owner
- Domain Name Technical Operator
- Type of relationship between DNB/DNO/DNT
- DNB Main Activity Description
- GDPR compliance attestation reference
- (Trading) Insurance coverage attestation
- Valuation ranking

AC issuer may not be a “CA” but an AC signer

Clause 5.4 The AC issuer MUST be directly trusted as an AC issuer (by configuration or otherwise)

→ EU MS TL

The Attributes that were included in the Pilot

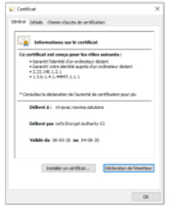
Attribute	Description
id-ntqwac 1	**DNB identification** conveying the name, registration identifier and address details of the **person** who is the business beneficiary of the domain name.
id-ntqwac 2	**DNB legal representative** identification conveying the name and registration identifier of the **person** who is the business beneficiary of the domain name.
id-ntqwac 3	**DNO identification** conveying the name, registration identifier and address details of the **person** who is the domain name owner (DNO).
id-ntqwac 4	**DNT identification** conveying the name, registration identifier and address details of the **person** who technically operates the domain name.
id-ntqwac 5	An expression of the **relationship(s) between the 3 parties**: DNB, DNO, DNT. It may also be used to avoid repetition of DNB, DNO, and DNT when they are the same person.
id-ntqwac 6	**DNB Main Activity Description** attribute provides information on the main (business) activity(ies) run by the DBU through the website domain name(s).
id-ntqwac 7	An attestation of the verification of GDPR compliance or at least of the “Protection of personal data”, together with the identification of the territory, in which the consumer personal data is exclusively stored.
id-ntqwac 8	An attestation of a trading insurance guarantee or coverage.
id-ntqwac 9	A valuation ranking attribute.

Disclaimer regarding the attributes

- Included for **illustration** purposes
- Showing how rich it can be, how much **added value** it can bring
- Making ntQWAC issuance closer to “real” **business value**
- More than just issuing “**security**” certificates for the sake of issuing “security” certificates

Illustration of the attributes

TLS cert


Certificat
Général
Détails
Chemin d'accès de certification
Installer un certificat...
Déclaration de l'émetteur
OK

Informations sur le certificat

Ce certificat est conçu pour les rôles suivants :

- Garantit l'identité d'un ordinateur distant
- Garantit votre identité auprès d'un ordinateur distant
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

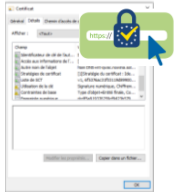
* Consultez la déclaration de l'autorité de certification pour plu

Délivré à : nt-qwac.nowina.solutions

Délivré par Let's Encrypt Authority X3

Valide du 06-05-20 **au** 04-08-20

ntQWAC



Afficher : <Tout>

Champ	Valeur
Identificateur de clé de l'aut...	[illegible]
Accès aux informations de l'...	[illegible]
Autre nom de l'objet	Nom DNS=nt-qwac.nowina.sol...
Stratégies du certificat	[1]Stratégie du certificat : Ide...
Liste de SCT	v1, [illegible]
Utilisation de la clé	Signature numérique, Chiffrem...
Contraintes de base	Type d'objet=Entité finale, Ca...
Empreinte numérique	[illegible]

DV certificate

[…]
SubjectDN
  CN = nowina.lu
[…]
AltName
  DNS=nowina.lu
  DNS=www.nowina.lu
[…]
Issuer
  Let's Encrypt, US

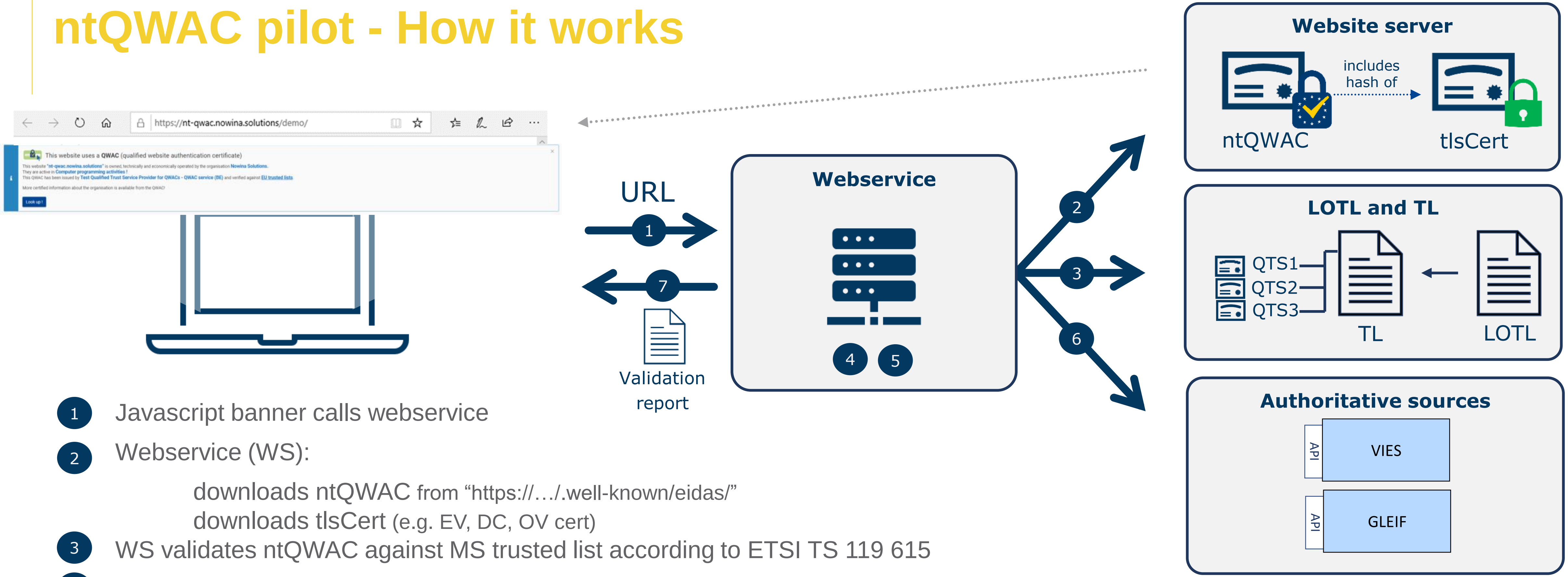
ntQWAC meets Annex IV requirements (eIDAS Art.3(39), Art.45(1))

Annex IV.a) → Acinfo/Extensions/QcCompliance, QcType 3
Annex IV.b) → Acinfo/Issuer (Distinguished Name)
Annex IV.c) & d) → Acinfo/Attributes with regards to the domain name certified in the crypto referenced base TLS certificate

1. DNB
2. DNB legal representative
3. DNO
4. DNT
5. DNB/DNO/DNT relationships
6. DNB Main Activity(ies) Description
7. GDPR compliance
8. (Trading) Insurance guarantee
9. Valuation ranking

Annex IV.e) → Acinfo/Holder (baseCertificate ID, objectDisgestInfo) i.e. as certified in the crypto referenced base TLScertificate
Annex IV.f) → Acinfo/AC validity period (NotBefore, NotAfter)
Annex IV.g) → Acinfo/Serial Number
Annex IV.h) → (Signature Algorithm &) Signature Value
Annex IV.i) → Acinfo/Extensions/AIA (id-ad-caIssuer)
Annex IV.j) → Acinfo/Extensions/CRLDP & AIA (ocsp)

ntQWAC pilot - How it works



https://nt-qwac.nowina.solutions/demo/

This website uses a **QWAC** (qualified website authentication certificate)

This website "nt-qwac.nowina.solutions" is owned, technically and economically operated by the organisation Nowina Solutions.
They are active in Computer programming activities !
This QWAC has been issued by Test Qualified Trust Service Provider for QWACs - QWAC service (BE) and verified against EU trusted lists

More certified information about the organisation is available from the QWAC!

1 Javascript banner calls webservice

2 Webservice (WS):

downloads ntQWAC from “https://…/.well-known/eidas/”
downloads tlsCert (e.g. EV, DC, OV cert)

3 WS validates ntQWAC against MS trusted list according to ETSI TS 119 615

4 WS verifies ntQWAC and tlsCert cryptographic relationship

5 WS processes ntQWAC attributes to produce structured ntQWAC validation report

6 WS performs additional checks against authoritative sources (e.g. VAT against VIES, LEI against GLEIF)

7 Javascript receives back the validation report

8. ntQWAC validation report is displayed into three tabs (Summary; ntQWAC Validation; TLS validation)

Webservice could be run by a TSP and the ntQWAC validation report signed/sealed

3

Demo

https://nt-qwac.nowina.solutions/demo/