

QWACs

A Path Forward?

Concerns & Compromise

Article 45

The goals of article 45 are noble.

- 'Right to know' / Access to trustworthy information
- Ensure gatekeepers act fairly and responsibly
- Ensure critical infrastructure for EU citizens is well-secured

Articles 12, 13 & 14 of the GDPR

Digital Markets Act

NIS2 Directive

But these goals are already covered by mature EU initiatives.

Regulation is hard.

- GDPR, the DMA and NIS2 are incredibly complex and evolving regulatory systems.
- They have gone through extensive debate, revision and compromise.
- If they are insufficient, the problem will not be solved within a single article in eiDAS2

Compromises


- A **right** to know is not an **obligation** to know.
 - Users must be free to choose how they engage with the web

- EU standards should be a foundation, not a ceiling.
 - The EU has the right to set baseline standards for securing the web.
 - Companies should be able to go above and beyond those standards

Opportunities

Trustworthy Indicators

- Legal identity is not especially meaningful to users.
- Knowing a business is accredited and licensed for a particular purpose is impactful.

“The operator of this website is supervised by Federal Financial Supervisory Authority of ”

“This website is operated by the  government”

Banking. Pharmacy / Healthcare. Government / Administration.


Trust is a valuable commodity

If we can get this right


- We help users navigate the web, safely and securely.
- We can unlock new markets and new opportunities.
- We can bring the trust enjoyed by our society to a global stage.

Challenges & Solutions

Challenge: Engagement

 **Safari is using an encrypted connection to www.us-cert.gov.**
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.us-cert.gov.

DigiCert Global Root CA
GeoTrust RSA CA 2018
www.dhs.gov

 **www.dhs.gov**
Issued by: GeoTrust RSA CA 2018
Expires: Saturday, October 17, 2020 at 8:00:00 AM Eastern Daylight Time
This certificate is valid

Trust

When using this certificate: Use System Defaults ?

Secure Sockets Layer (SSL) no value specified
X.509 Basic Policy no value specified

Details

Subject Name

Country or Region US
State/Province District Of Columbia
Locality Washington
Organization Department of Homeland Security
Common Name www.dhs.gov


Issuer Name

Country or Region US
Organization DigiCert Inc
Organizational Unit www.digicert.com

Hide Certificate OK

Certificate

General Details Certification Path

 **Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.ssl2buy.com

Issued by: RapidSSL RSA CA 2018

Valid from 11-03-2020 **to** 11-03-2022

Issuer Statement

OK

Certificate Viewer: *.reddit.com

General **Details**

Certificate Hierarchy

- DigiCert Global Root CA
 - DigiCert TLS RSA SHA256 2020 CA1
 - *.reddit.com**

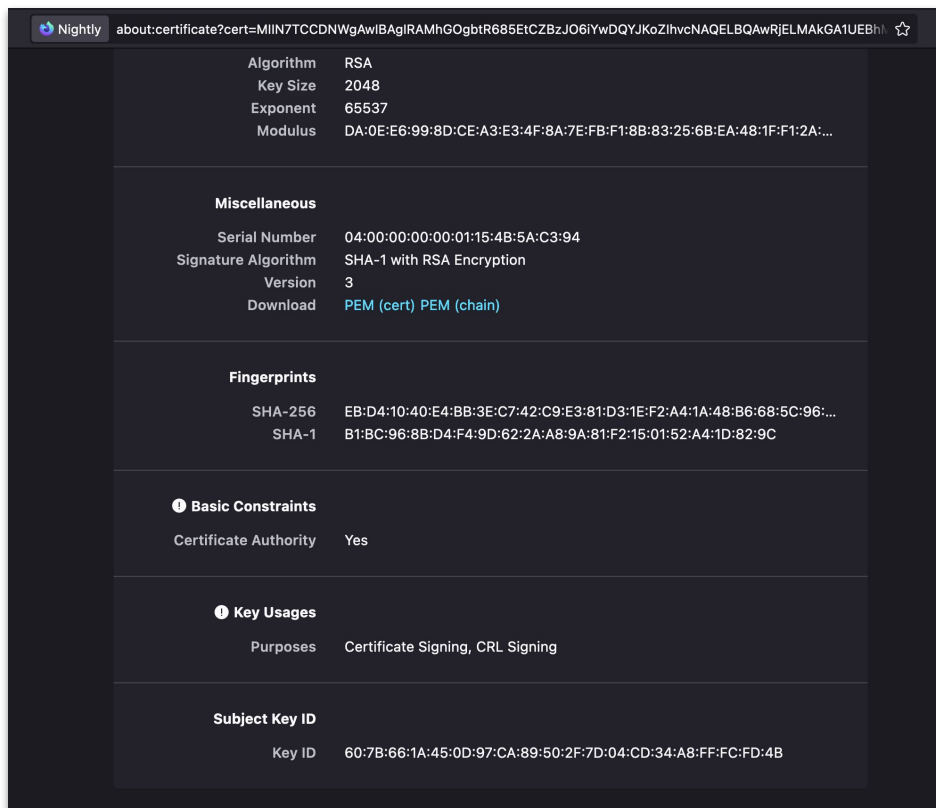
Certificate Fields

- *.reddit.com
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before

Field Value

Export...

Challenge: Engagement



The screenshot shows a browser's certificate details page in dark mode. The address bar shows a URL starting with 'about:certificate?cert=MIIN7TCCDNWgAwIBAgIRAMhGOgbr685EtCZBzJO6YwDQYJKoZIhvcNAQELBQAwRjEjMAkGA1UEBhI...'. The page is divided into several sections:

- Algorithm:** RSA
- Key Size:** 2048
- Exponent:** 65537
- Modulus:** DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:...

Miscellaneous

- Serial Number:** 04:00:00:00:00:01:15:4B:5A:C3:94
- Signature Algorithm:** SHA-1 with RSA Encryption
- Version:** 3
- Download:** [PEM \(cert\)](#) [PEM \(chain\)](#)

Fingerprints

- SHA-256:** EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:...
- SHA-1:** B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

Basic Constraints

- Certificate Authority:** Yes

Key Usages

- Purposes:** Certificate Signing, CRL Signing

Subject Key ID

- Key ID:** 60:7B:66:1A:45:0D:97:CA:89:50:2F:7D:04:CD:34:A8:FF:FC:FD:4B

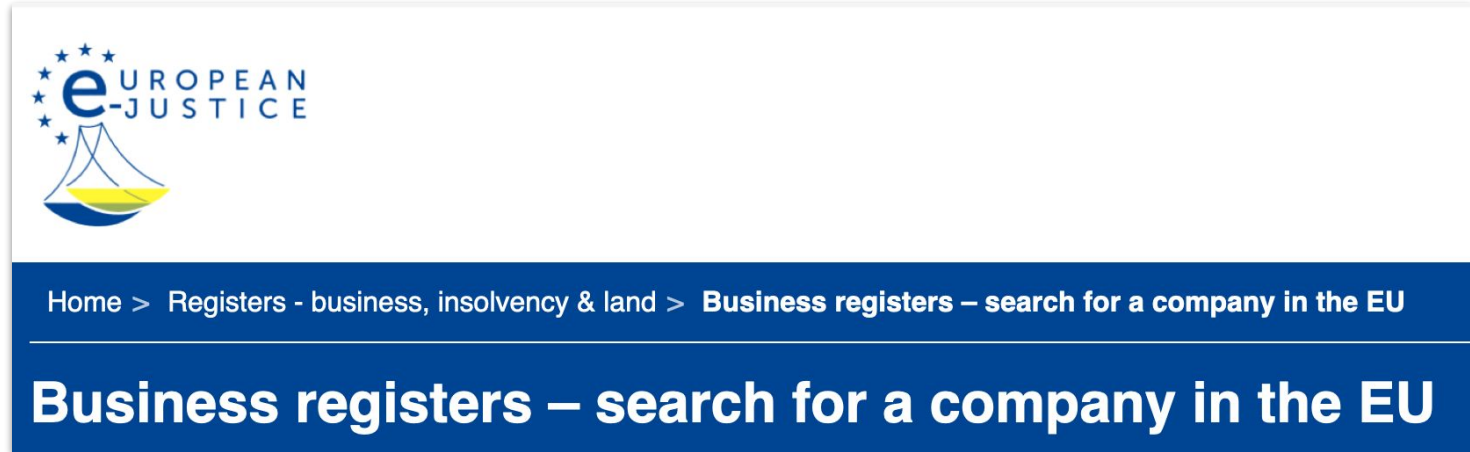
- Copy / Paste
- Dark Mode
- PEM Downloads
- Clickable Links

Challenge Engagement

User Responses:

- I don't use that feature
- No, I use Adobe Acrobat
- ...

Challenge: Understanding



The image shows the header of the European e-Justice portal. It features the logo for 'eUROPEAN -JUSTICE' with a stylized sailboat icon. Below the logo is a navigation breadcrumb: 'Home > Registers - business, insolvency & land > Business registers – search for a company in the EU'. The main title 'Business registers – search for a company in the EU' is displayed in large white text on a dark blue background.

eUROPEAN
-JUSTICE

Home > Registers - business, insolvency & land > **Business registers – search for a company in the EU**

Business registers – search for a company in the EU

Challenge: Understanding

1-50 of 182 results for search inquiries

[Expand all](#) | [Collapse all](#)

ENTRUST S.R.L. - Italy



ENTRUST SERVICE S.R.L. - Italy



ENTRUST S.R.L., IN LIQUIDAZIONE - Italy



ENTRUST 2 - France



Registered office: 20 rue Chevreul, Nantes, France

Registration number: 838372084

Company type: Société par Actions Simplifiée 

Business Register ID: 4401 

EUID: FR4401.838372084

ENTRUST ARMOR GROUP - France



Challenge: Understanding

1-50 of 62 results for search inquiries

[Expand all](#) | [Collapse all](#)

NATWEST MARKETS N.V. - France



NATWEST SL - Spain



NATWEST s.r.o. - Slovakia



NatWest Markets (secondary name) - Netherlands



NATWEST MARKETS N.V. - Ireland



NATWEST MARKETS PLC - Ireland



NatWest Wertpapierhandels GmbH - Germany



BANCO NATWEST ESPAÑA SA - Spain



Challenge: Consistency

← Connection security for www.quovadisglobal.com

🔒 You are securely connected to this site.

Certificate issued to:

DigiCert, Inc.
Lehi
Utah, US

Verified by: DigiCert Inc

More information



Safari is using an encrypted connection to www.quovadisglobal.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.quovadisglobal.com.

DigiCert Inc has identified www.quovadisglobal.com as being owned by DigiCert, Inc. in Lehi, Utah, US.

Show Certificate OK



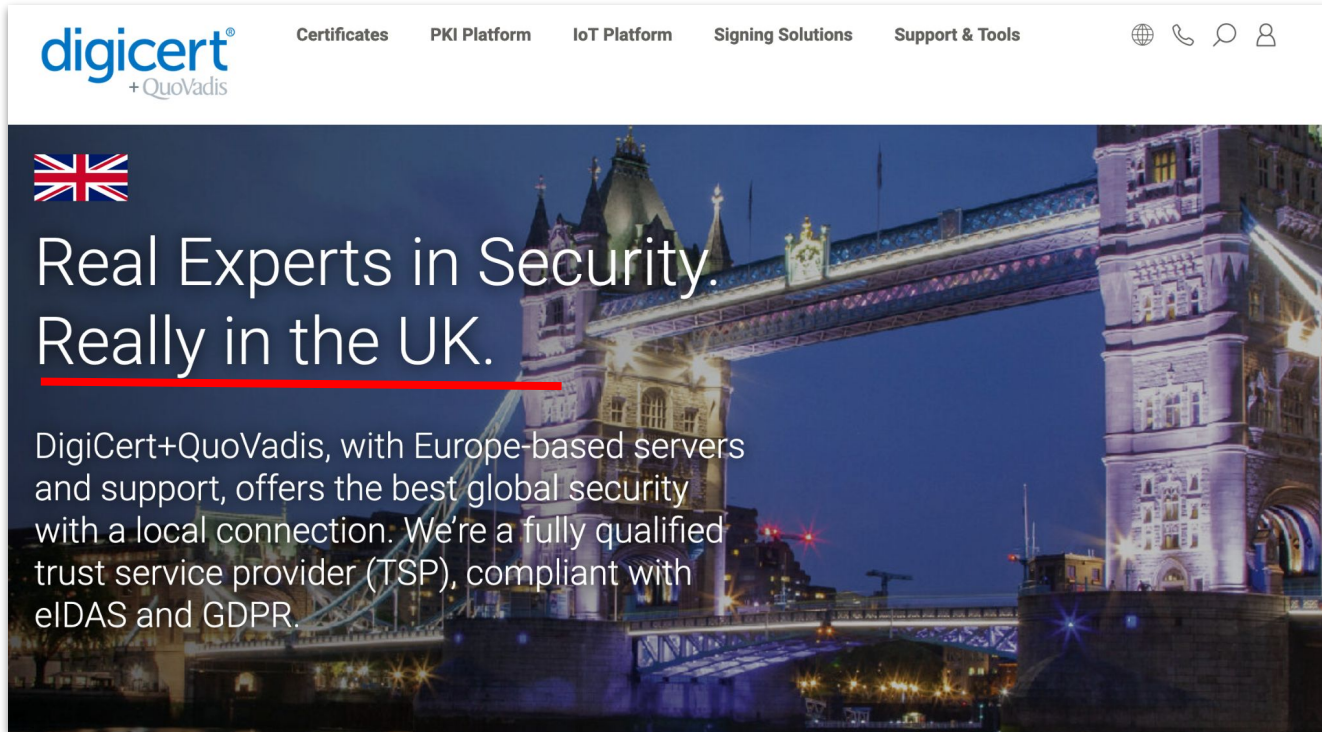
← Security ×

quovadisglobal.com


🔒 Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. [Learn more](#)

📄 Certificate is valid 🔗
Issued to: DigiCert, Inc. [US]

Challenge: Consistency



The screenshot shows the top navigation bar of the DigiCert+QuoVadis website. The logo is on the left, followed by menu items: Certificates, PKI Platform, IoT Platform, Signing Solutions, and Support & Tools. On the right, there are icons for a globe, a telephone, a speech bubble, and a user profile.

 Real Experts in Security.
Really in the UK.

DigiCert+QuoVadis, with Europe-based servers and support, offers the best global security with a local connection. We're a fully qualified trust service provider (TSP), compliant with eIDAS and GDPR.

Challenge: Consistency

Homepage DigiCert + QuoVadis × +

https://www.quovadisglobal.com/uk/

Connection security for www.quovadisglobal.com

You are securely connected to this site.

Certificate issued to:
DigiCert, Inc.
Lehi
Utah, US

Verified by: DigiCert Inc

More information

UKI Platform IoT Platform
ns Support & Tools

Real Experts in Security.
Really in the UK.

DigiCert+QuoVadis, with Europe-based servers and support, offers the best global security with a local connection. We're a fully qualified

Certificate issued to:
DigiCert, Inc.
Lehi
Utah, US

Solutions?

- Regulation & standards are very blunt instruments. Flexibility is essential.
- Embrace User Choice
 - User's should have low-friction ways to engage with - or dismiss - identity information.
 - Accessibility
- Education
 - Engage with users
- Science!
 - European Academia is an underutilised resource.

Challenge: Deployment

- Ultimately website operators have to choose to deploy this technology
- Certificate management and disaster recovery is already a headache
- Major Websites have complex custom architectures, with very little incentive to overhaul them.
- Fragile designs which magnify the impact of interruptions are problematic.

Solution: pQWACs

- Mozilla has developed a technical proposal which has several attractive features
- It provides the authentic information about ownership that users need to see
- It is very simple for operators, just an additional certificate placed on the web server in .well-known.

Solution: pQWACs

- If it expires or is misconfigured - regular TLS still works and the website remains available - without the EU trust mark.
- It adds to the security of DV certificates without replacing them. Websites can use all existing best practices and automated methods.
- **The QTSP issuing the QWAC does NOT need to be in the root store.**
Widening the market and reducing the compliance burden.

Solution: pQWACs

- The solution is compliant with eIDAS Annex IV:
 - It contains the legal identity or natural person
 - Their domain names
 - The validity period
 - The advanced electronic signature / seal of the qualified trust service provider.
- The solution supports existing management and revocation methods (OCSP, CRLite, certificate transparency, etc)

Solution: pQWACS

Portable Qualified Website Authentication Certificates (pQWACs)

Table of Contents

Abstract	2
1. Introduction	2
2. Overview and Rationale	2
2.1. Compatibility with TLS and WebPKI Practices	3
2.2. Incremental Deployment	3
2.3. Smooth Degradation	3
2.4. Extensibility	4
3. pQWAC Certificate Profile	4
4. Endorsement Document	4
4.1. Processing the Endorsement Document	5
5. Delivery Methods	5
5.1. TLS Extension	5
5.2. HTTP Header	6
5.3. Alternative Delivery Mechanisms	6
6. Browser Processing	6
6.1. Root Store Management	6
6.2. Connection Establishment	6
6.3. Top-level Page Load	7
6.3. Semantics	7

Solution: pQWACs

- But we don't have all the answers...
- We want to engage with QTSPs, supervisory bodies, ENISA, website operators.
- We're working with stakeholders at ETSI and other technical bodies.
- We've already received valuable input from EnTrust, ANSSI, LuxTrust, HARICA and more

Let's talk!